President Obama, who once believed in the Fourth Amendment, is the President who is now scooping up all of your records illegally. Then he feigns concern and says: Oh, we need to pass this new bill. He could stop it now. Why won't someone ask the President: Why do you continue? Why won't you stop this program now? The President has every ability to do it. We have every ability to keep our Nation safe. I intend to protect the Constitution.

The PRESIDING OFFICER. The Senator's time has expired.

RECESS

The PRESIDING OFFICER. Under the previous order, the Senate stands in recess subject to the call of the Chair.

Thereupon, the Senate, at 5:11 p.m., recessed subject to the call of the Chair and reassembled at 6:14 p.m. when called to order by the Presiding Officer (Mr. WICKER).

USA FREEDOM ACT OF 2015—MOTION TO PROCEED—Continued

The PRESIDING OFFICER. The majority leader.

Mr. MCCONNELL. Mr. President, before the recess, I tried to get a short-term extension of three provisions that will expire at midnight tonight: section 215, business records; section 206, roving wiretap authority; and the ''lone wolf'' provision. Unfortunately, those efforts were unsuccessful.

''Lone wolf'' and roving wiretap are not—I repeat, not—the subject of controversy with the House bill. So I would propose that we extend at least the ''lone wolf'' and the roving wiretap authorities while we continue to litigate the differing views on section 215. More specifically, I would propose that we extend those two provisions—''lone wolf'' and roving wiretaps—for up to 2 weeks.

UNANIMOUS CONSENT REQUEST

Mr. President, having said that, I ask unanimous consent that the Senate proceed to the immediate consideration of a bill, which is at the desk, to extend the expiring provisions relating to ''lone wolf'' and roving wiretaps for 2 weeks, and that the bill be read a third time and passed, and the motion to reconsider be considered made and laid upon the table with no intervening action or debate.

The PRESIDING OFFICER. Is there objection?

The Senator from Kentucky.

Mr. PAUL. Mr. President, reserving the right to object, one of the promises that was given when the PATRIOT Act was originally passed was that, in exchange for allowing a less than constitutional standard, we would only use the actions against——

The PRESIDING OFFICER. Is there objection?

Mr. PAUL. Terrorists and against foreigners. We found that 99 percent of the time, section 213 is used for domestic crime. I believe that no section of the PATRIOT Act should be passed unless our targets are terrorists—not Americans.

Mr. CORNYN. Mr. President, regular order.

The PRESIDING OFFICER. The Senator from Kentucky——

Mr. COTTON. Regular order.

Mr. PAUL. I object.

The PRESIDING OFFICER. Objection is heard.

Mr. MCCONNELL. Mr. President, last week, I proposed giving the Intelligence Committee the time it would need to work toward the kind of bipartisan legislative compromise Americans deserve—a compromise that would preserve important counterterrorism tools necessary to protect American lives. That effort was blocked.

Just now, I proposed an even narrower extension that would have only extended some of the least controversial—least controversial—but still critical tools to ensure they do not lapse as Senators work toward a more comprehensive legislative outcome. But even that very narrow offer was blocked. I think it should be worrying for our country because the nature of the threat we face is very serious. It is aggressive, it is sophisticated, it is geographically dispersed, and it is not—not—going away.

As the LA Times reported, ''the Obama administration has dramatically stepped up warnings of potential terrorist attacks on American soil after several years of relative calm.'' The paper reported that this is occurring in the wake of ''FBI arrests of at least 30 Americans on terrorism-related charges this year in an array of 'lone wolf' plots.''

So these aren't theoretical threats. They are not theoretical threats. They are with us every day. We have to face up to them. We shouldn't be disarming unilaterally as our enemies grow more sophisticated and aggressive, and we certainly should not be doing so based on a campaign of demagoguery and disinformation launched in the wake of the unlawful actions of Edward Snowden, who was last seen in Russia.

The opponents of this program have not been able to provide any—any—examples of the NSA abusing the authorities provided under section 215. And the record will show that, in fact, there has not been one documented instance of abuse of it.

I think it is also important to remember that the contents of calls are not captured. That is the general view, but it is an incorrect one. I will say it again: The contents of calls are not captured. I say this to the American people: If you have been told that, that is not correct. That is what I mean about a campaign of disinformation. The only things in question are the number dialed, the number from which the call was made, the length of the call, and the date. That is it. That is it. Detailed oversight procedures have been put in place, too, in order to protect the privacy of Americans.

Now, I believe this is a program that strikes a critical balance between privacy on the one hand and national security on the other. That doesn't mean the Senate still shouldn't have the opportunity to make some changes to it. That is precisely the outcome I had been hoping to facilitate by seeking several short-term extensions. And considering all that has come to light about the House-passed bill in recent weeks, I believe this was more than reasonable.

The administration's inability to answer even the most basic questions about the alternate bulk data system it would have to build under that legislation is, to say the least, pretty troubling—pretty troubling. And that is not just my view. That is the view of many in this body, including colleagues who have been favorably predisposed to the House bill.

In particular, I know Senators from both parties have been disturbed by the administration's continuing inability to guarantee whether the new system would work as well as the current one or whether there would even be any data available to analyze. While the administration has let it be known that this nonexistent system could only be built in time if telephone providers cooperated in building it, providers have made it abundantly clear that they are not going to commit to retaining the data. They are not going to commit to retaining the data for any period of time unless legally required to do so, and there is no such requirement in the House-passed bill—none at all.

Here is how one provider put it: ''[We are] not prepared to commit to voluntarily retain documents for any particular period of time pursuant to the proposed USA Freedom Act if not required by law''—if not required by law.

Now, these are just a few of the reasons I thought it prudent to try to give the Senate more space to advance better legislation through committee consideration and regular order, with input from both sides. But, my colleagues, it is now clear that will not be possible in the face of a determined opposition from those who simply wish to end the counterterrorism program altogether. No time to try to improve the House-passed bill will be allowed because some would like to end the program altogether.

So this is where we find ourselves. This is the reality. So it essentially leaves us with two options. Option one is to allow the program to expire altogether without attempting to replace it. That would mean disarming completely and arbitrarily, based on a campaign of disinformation, in the face of growing, aggressive, and sophisticated threats—growing, aggressive, and sophisticated threats. That is a totally unacceptable outcome—a completely and totally unacceptable outcome. So we won't be doing that.

So we are left with option two, the House-passed bill. It is certainly not ideal. But along with votes on some modest amendments that attempt to ensure the program can actually work as promised, it is now the only realistic way forward. So I remain determined to continue working toward the best outcome for the American people possible under the circumstances.

This is where we are, colleagues. We have the House-passed bill with some serious flaws and an inability to get a short-term extension to try to improve the House-passed bill in the way we normally do this—through some kind of consultative process.

So bearing that in mind, I move to proceed to the motion to reconsider vote No. 194, the vote by which cloture was not invoked on the motion to proceed to H.R. 2048.

The PRESIDING OFFICER. The question is on agreeing to the motion.

The motion was agreed to.

Mr. MCCONNELL. Mr. President, I move to reconsider the motion to invoke cloture on the motion to proceed to H.R. 2048.

The PRESIDING OFFICER. The question is on agreeing to the motion.

The motion was agreed to.

CLOTURE MOTION

The PRESIDING OFFICER. Pursuant to rule XXII, the Chair lays before the Senate the pending cloture motion, which the clerk will state.

The senior assistant legislative clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of rule XXII of the Standing Rules of the Senate, do hereby move to bring to a close debate on the motion to proceed to H.R. 2048, an act to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes.

Mitch McConnell, Lamar Alexander, Michael B. Enzi, David Vitter, John Cornyn, Johnny Isakson, Lisa Murkowski, John Barrasso, Richard Burr, Pat Roberts, Roy Blunt, Bob Corker, Orrin G. Hatch, Jerry Moran, Patrick J. Toomey, Mike Lee, Ted Cruz.

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

The question is, Is it the sense of the Senate that debate on the motion to proceed to H.R. 2048, an act to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes, shall be brought to a close, upon reconsideration?

The yeas and nays are mandatory under the rule.

The clerk will call the roll.

The senior assistant legislative clerk called the roll.

Mr. CORNYN. The following Senators are necessarily absent: the Senator from Wyoming (Mr. ENZI), the Senator from South Carolina (Mr. GRAHAM), and the Senator from Nebraska (Mr. SASSE).

Mr. DURBIN. I announce that the Senator from New Jersey (Mr. MENENDEZ), the Senator from Washington (Mrs. MURRAY), and the Senator from Hawaii (Mr. SCHATZ) are necessarily absent.

The PRESIDING OFFICER (Mr. BARRASSO). Are there any Senators in the Chamber wishing to vote or to change their vote?

The yeas and nays resulted—yeas 77, nays 17, as follows:

[Rollcall Vote No. 196 Leg.]

YEAS—77

Alexander	Franken	Murkowski
Ayotte	Gardner	Murphy
Baldwin	Gillibrand	Nelson
Bennet	Hatch	Perdue
Blumenthal	Heinrich	Peters
Booker	Heitkamp	Portman
Boozman	Heller	Reed
Boxer	Hirono	Reid
Brown	Hoeven	Rounds
Burr	Inhofe	Sanders
Cantwell	Isakson	Schumer
Capito	Johnson	Scott
Cardin	Kaine	Shaheen
Carper	King	Stabenow
Casey	Kirk	Sullivan
Cassidy	Klobuchar	Tester
Cochran	Lankford	Tillis
Coons	Leahy	Toomey
Corker	Lee	Udall
Cornyn	Manchin	Vitter
Cruz	Markey	Warner
Daines	McCain	Warren
Donnelly	McCaskill	Whitehouse
Durbin	McConnell	Wicker
Feinstein	Merkley	Wyden
Flake	Mikulski	

NAYS—17

Barrasso	Ernst	Roberts
Blunt	Fischer	Rubio
Coats	Grassley	Sessions
Collins	Moran	Shelby
Cotton	Paul	Thune
Crapo	Risch	

NOT VOTING—6

Enzi	Menendez	Sasse
Graham	Murray	Schatz

The PRESIDING OFFICER. On this vote, the yeas are 77, the nays are 17.

Three-fifths of the Senators duly chosen and sworn having voted in the affirmative, upon reconsideration, the motion is agreed to.

The Senator from Kentucky.

Mr. PAUL. Mr. President, could we have order?

The PRESIDING OFFICER. The Senate will be in order.

Mr. PAUL. Will the Chair inform me when I have 5 minutes remaining?

The PRESIDING OFFICER. The Senator will be so notified.

Mr. PAUL. Mr. President, tonight begins the process of ending bulk collection. The bill will ultimately pass. We always look for silver linings. I think the bill may be replacing one form of bulk collection with another, but the government, after this bill passes, will no longer collect our phone records. My concern is that the phone companies still may do the same thing. Currently, my understanding is the NSA is at the phone company sucking up the phone records and sending them to Utah. My concern is——

The PRESIDING OFFICER. Order in the Senate, please. The Senator deserves to be heard.

Mr. PAUL. My concern is that under the new program, the records will still be sucked up into NSA computers, but the computers will be at the phone company, not in Utah. So the question is, Will it be a distinction without a difference? The question also will be, Will this be individualized?

One of the issues about the Fourth Amendment that was the biggest part of the Fourth Amendment for our Founding Fathers was that a warrant should be individualized. General warrants were what we fought the Revolution over. James Otis fought a famous case in the 1760s, and he fought against the British soldiers writing their own warrants.

What is interesting is that part of the PATRIOT Act allows our police to write their own warrants. We have something called national security letters. These have been done by the hundreds of thousands. Interestingly, when the President was in the Senate, he was opposed to national security letters and said that they should have judicial warrants. Now, it is interesting that in this bill that will pass, it is supported by the President, supported by the Director of National Intelligence, and now supported in a wide bipartisan fashion.

It concerns me whether or not——

The PRESIDING OFFICER. The Senate will be in order.

Will the Senator please suspend.

The Senate will be in order. Please take your conversations out of the well, out of the Chamber. The Senator deserves to be heard.

Mr. PAUL. It concerns me that the President, who supports the bulk data collection and has been performing it illegally for 6 years, now supports this bill. The devil is in the details.

The question is, Will the new bill still allow bulk collection by the phone companies? Will they be able to put into the search engine not an individual about whom we have suspicion but an entire corporation? This is what was revealed when we saw the warrant that had Tsarnaev's name on it.

The Director of National Intelligence came before the American people, came before Congress and swore under oath that they weren't doing this. Part of my problem with the intelligence-gathering in our country is it is hard for me to have trust. It is hard for me to have trust in the people to whom we are giving great power.

They also insist we won't be able to catch terrorists. They insist the bulk collection allowed them to catch terrorists. But then it turned out, when it was investigated, when we looked at the classified documents, when the President's bipartisan privacy and civil liberties commission looked at this, when his review board looked at this, and then when the Department of Justice inspector general looked at this,

they all found that there was no unique data, there was no great discovery, there was no great breaking up of a terrorist ring.

People have brought up the Boston Bomber, the Tsarnaev boy. They say: Well, we need this. We need the PATRIOT Act after the bombing to get his phone records.

That is the most absurd thing I have ever heard. He has already committed a bombing. In fact, I think he was dead at that point, and they are saying we couldn't get a warrant to look at his phone records? It is absolutely absurd.

I had a meeting with somebody from the intelligence community about 6 months ago, and I asked them this question: How do we get more information about terrorists—with a warrant with their name on it, where we can go as deep into the details as we want, or this metadata collection that uses a less-than-constitutional standard? And he said: Without question, we get more information with a warrant than we do through the metadata.

When someone commits an act of atrocity, there is no question we would get a warrant, but I would go even further. I would say that I want to get more warrants on people before they blow up things. I would say that we need more money spent on FBI agents analyzing data and trying to find out whom we have suspicion about so we can investigate their records. I think we spend so much money on people about whom there is no suspicion that we don't have enough time and money left to go after the people who would actually harm us.

The people who argue that the world will end at midnight tonight——

The PRESIDING OFFICER. The Senator will please suspend.

Order in the Chamber. Please take your conversations off the floor.

Mr. PAUL. The people who argue that the world will end and that we will be overrun by jihadists tonight are trying to use fear. They want to take just a little bit of our liberty, but they get it by making us afraid. They want us to fear and give up our liberty. They tell us that if we have nothing to hide, we have nothing to fear. That is a far cry from the standard we were founded upon—innocent until proven guilty.

One of the objections I tried to bring forward earlier but was interrupted repeatedly was that the PATRIOT Act was originally intended to go after foreigners and terrorists. We allowed a less-than-constitutional standard. We didn't ask for probable cause; we just said it had to be relevant, the information had to be relevant to an investigation about terrorists. But here is the problem, and this is one of the big problems I have with the PATRIOT Act.

We now use parts of the PATRIOT Act to arrest people for domestic crime. Section 213, sneak-and-peek, where the government can come into your house, place listening devices, never announce they were ever in your house, and then leave and monitor your behavior and never let you know they were there, is being used 99.5 percent of the time for domestic crime.

So, little by little, we have allowed our freedom to slip away. We allowed the Fourth Amendment to be diminished. We allowed the narrowing loss of something called probable cause.

People say: Well, how would we get terrorists with that?

The vast majority of warrants are approved in our country—the vast majority of warrants that are Fourth Amendment warrants where we individualized and put a name on it and asked probable cause. If tonight the police are looking for a rapist or a murderer, they will go to the house, and if they suspect the person is inside but nothing is imminently happening, they will stand on the curb and they almost always get a warrant.

Do you think there is a judge in this land who would not grant a warrant—particularly after the Boston bombing—to look at the Tsarnaev brothers' records? There is not a judge in the land who would say no. I would venture to say that in advance there is not much chance that a judge would say no if you went to them and said: The Russians have given us indication and evidence that he has been radicalized and has associated overseas with people who are training to attack us.

There is no reason why the Constitution can't be used. But we just have to not let those who are in power make us cower in fear. They use fear to take your freedom, and we have to be very, very careful of this.

Now, some are saying I am misrepresenting this, that I am saying the government is listening to your phone calls. I am saying they are collecting your phone records. There are programs, though, in which there may be looking at content—emails, for example. The current law says that after 6 months even the content of your email has no protection. We have a very good piece of legislation to try to fix that. But realize that those who are loud, those who are really wanting you to give up your freedom, don't believe the Fourth Amendment protects your records at all.

And this is a big debate. We went to the court. The Second Circuit Court of Appeals—the highest court in the land just below the Supreme Court—said that what they are doing is illegal, but we don't yet have a ruling on whether it is constitutional.

One of my fears about the bill we are going to pass—the sort of in-between step some think may be better—is that it could moot the case. This means the court case will never get heard by the Supreme Court. I have a court case against the NSA. There is another district court that has ruled against the NSA. We now have an appellate ruling against the NSA. The court may well look at the activity of the Senate and say: Well, you guys have fixed the problem. We don't need to look at it anymore. It is no longer relevant.

My other concern about this new bill that is going to pass is that the same people will judge it who judged the previous system. These people are called the rubberstamp courtroom, also known as FISA. Realize that the FISA Court is the court that said the collection of all Americans' records is relevant. The appellate court basically laughed at this notion and said that it sort of destroys any meaning to the word ''relevant'' if you collect everybody's records. It is not even a modifier. Instead of saying ''relevant,'' they should have said ''You can have everyone's records all the time.''

One of my other concerns about the in-between solution we are going to choose is that some are conjecturing—and you have to be suspicious of a government that often lies about their purpose—some are conjecturing that they are going to collect more phone data under the new system. One of the complaints last week, as there was discussion about this—in the newspaper, it was reported that really they were only collecting about 20 to 30 percent of your cell phone data. They were trying to collect all of your land line data, but they weren't for some reason collecting all of your cell phone data. One of my concerns is that as we go to this new system, they may actually be better at collecting our phone records and they may well be able to collect all of our cell phone data.

Unless we go to a system where we individualize the warrants, unless we go to a system where a person's name is on the warrant, I am going to be very, very concerned.

Now, we will present amendments on this bill. We tried to negotiate to be allowed to present amendments, but there wasn't a lot of negotiating that went on in the last week—in fact, there was none. We will still try. We will put amendments forward, and we will try to get amendments to make the bulk collection less bad when it does occur. One of the things we would like to do is to say that when they search the phone records, they can't put the name of a corporation in there; they would have to put in an individual's name.

It is kind of tricky, the way these things are worded. The wording of this bill will say they can only put a U.S. person into the selector term to search all phone records. The problem is that they define ''U.S. person'' as also meaning corporation or association or grouping. So there is a little bit of looseness to the language. So if we are still going to allow corporations, what is to stop them from going back and putting AT&T or Verizon in the selection? Once again they will be looking at all the phone records, and all we will have done is transferred the phone records from government control in Utah to phone company control in another location. Will we be trading bulk collection in Utah for bulk collection under the phone companies?

There are good people who believe this bill will reform, and I think they

are well-intended. I think they are good people who really think that we will end bulk collection and that it won't happen. My fear, though, is of the people who interpret this work at a place known as the rubberstamp factory over at FISA. It is a secret court, and it is a court in which 99.5 percent of the time they approve warrants. Warrants are simply rubberstamped over there. In fact, they approved that ''relevant'' meant all of your records. So my question is, If they put AT&T as a selector item, will we have the same thing, just in a different location?

I have several amendments I am interested in if we are able to amend the bill.

One is that the search would have to be an individual. That is more consistent with the Fourth Amendment.

Another one would change the standard to the constitutional standard, which would be that there would have to be probable cause, which is a higher standard than simply saying it is relevant. Then we would actually be sending a new signal to the FISA Court.

Another amendment I have, which I think would go a long way toward making the PATRIOT Act less bad—I think is the best way to put it—would be to say that any information gathered under a less-than-constitutional standard could only be used for foreigners and terrorists. See, that was the promise. At the time, there were people who opposed the PATRIOT Act—not enough, but there were a few—and when they opposed the PATRIOT Act, they said their fear was that it would be used against American citizens.

They said: No, no, we are only going after terrorists. But the law allows them to do it, and we now have sections of the PATRIOT Act which 99.5 percent of the time are being used for domestic crime. We have also seen that the Drug Enforcement Agency—it is alleged—is using information gathered under the PATRIOT Act to then go back and recreate cases against people for domestic crime.

The question we have to ask ourselves is, Are we so frightened that we are willing to give up our freedom? Are we really willing to trade liberty for security?

I think the U.S. Court of Appeals had some great points that they made when they ruled against the government, and I think what is important to know is that the President has continued to do this illegally. You have seen him on television. The President has been saying: Well, Congress is just getting in the way. If Congress would just do their job and get rid of this, everything would be OK. But the truth is that Congress never authorized this. Even the authors of the PATRIOT Act said this was not something Congress ever even contemplated. The court is now saying that as well. This was done by the executive branch—admittedly, both a Republican executive branch and a Democratic executive branch—but this wasn't created by Congress.

So when the President says ''Well, Congress should just do this,'' the question that has never been asked by anyone in the media is ''Why doesn't he stop it?'' Everybody who has given advice has said he would, and he will come out and say he believes in a balanced solution, but he really is just abdicating the solution and has never discontinued the program, even when he has been told explicitly by the court that the program is an illegal program.

This is what the U.S. court of appeals said in the case ACLU v. Clapper:

> We agree with the appellants that such an expansive concept of ''relevance'' is unprecedented and unwarranted. . . . The records demanded are not those of suspects under investigation, or of people or businesses that have contact with such subjects, or of people or businesses that have contact with others who are in contact with the subjects.

So even two steps removed, we are gathering records that are completely irrelevant to the investigation. We are gathering up the phone records of innocent Americans.

The other side will say: Well, we are not looking at them.

So I have been thinking about this. Our Founders objected to the British soldiers writing warrants. They objected to them coming into their house and grabbing their papers. Do you think our Framers would have been happy if the British Government said: OK, we are just breaking your door down, we are just getting your papers, but we are not going to look at them. Do you think that would have changed the mindset of the Framers? So the fact that they say they are not looking at our records—is that any comfort or should it be any comfort? The act of violation is in taking your records. The act of violation is in allowing the police or a form of the police—the FBI—to write warrants that are not signed by a judge.

The court goes on to say: ''The interpretation that the government asks us to adopt defies any limiting principle.'' The idea of a limiting principle when the court looks at things is that, the way I see it, is the difference between something being arbitrary, where there is no sort of principle that confines what would happen—if you have a law that has no limiting principle, it is essentially arbitrary.

This is what Hayek wrote about in ''The Road to Serfdom.'' Hayek talked about the difference between the rule of law and having an arbitrary interpretation of the law.

The danger of having an arbitrary interpretation of the law and the danger of having general warrants is that they have been used in the past with bias. People have brought their own bias into this. In the sixties, the bias was against civil rights activists and against Vietnam war activists. In the forties, the bias was in incarcerating and interring Japanese Americans. But what was consistent in all of these circumstances was that there was a generalization—a generalization based on the color of your skin, whether you were Asian American or African American, and also about the shade of your ideology. There is a danger in allowing the government to generalize without suspicion and to disobey the Fourth Amendment, and the danger comes that the government could one day generalize and bias could enter into things.

We have on our records right now laws that allow an American citizen to be detained. It is not specifically a part of the PATRIOT Act, but it is along the same lines as this, that you are getting rid of the due process amendments and the ability of the Bill of Rights to protect an individual. When we allow an individual to be detained without a trial, what happens is that there is the possibility that someone could decide we don't like ''those'' people. And when you say that could never happen, think about the times in our history when it has.

Richard Jewell, everybody said he was the Olympic Bomber. He was convicted on TV. Within hours, people said: Richard Jewell is guilty. Think about if he had been a Black man in 1920 in the South what may have happened to him. Think about the possibility for bias entering into our government. Think about what Madison said about government is—Madison said that we restrain government because we are worried that government may not be comprised of angels. If government were comprised of angels, we would not have to worry about restraining government.

Patrick Henry said that the Constitution was about restraining government, not the people. It is not enough for people to say: Oh, I am a good man or I am a good person or the NSA would never do this. The other problem that makes us doubtful is that the NSA has not been honest with us. If they want to develop trust again, the President should have immediately let the person who lied to us go, the Director of National Intelligence.

The appeals court concluded by saying that the government's bulk collection of telephone metadata exceeds the scope of what Congress has authorized and therefore violates section 215 of the PATRIOT Act. Some will try to argue that this debate was not worth the time we took on it. I could not disagree more. I am like everybody else. You know, I prize my time with my family and being at home on the weekends. I wish we would have done this in a more sensitive way, where we would have had more time and had an open amendment process.

But we waited until the end. We waited until the final deadline. This is a characteristic of government. It is a flaw in government, frankly. We lurch from deadline to deadline. People wonder why Congress is so unpopular. It is because we go from deadline to deadline and then it is: Hurry up. We have no time to debate. We just must pass it as is.

The biggest debate against amendments is—and it finally convinced people who did not like this. They so much dislike amendments and slowing down the process, they are just going to take it. Even though they don't like it, they are going to pass what the House passed. It is unlikely any amendments will pass.

But the thing is, we need to get away from lurching from deadline to deadline. What happens, with budget or spending or any of these bills, is we are presented with thousand-page bills with only hours to go. About a year ago this came up. At that time, we were presented with a 1,000-page bill with 2 hours to go. I read the Senate rules. It said: We are supposed to be presented with the bill for 48 hours in advance.

So I raised my hand and made a motion. The motion I made was: Guys, we are breaking the rules here. Men and women, we are breaking the rules here. So they just voted to amend the rules for that bill and ignore the rules. This is why the American people are so frustrated. People here in town think I am making a huge mistake. Some of them, I think, secretly want there to be an attack on the United States so they can blame it on me. One of the people in the media the other day came up to me and said: Oh, when there is a great attack, are you going to feel guilty that you caused this great attack?

The people who attack us are responsible for attacks on us. Do we blame the police chief for the attack by the Boston Bombers? The thing is, is that there can be attacks even if we use the Constitution. But there have been attacks while collecting your bulk data. So the ones who say: Well, when an attack occurs, it is going to be all your fault, are any of them willing to accept the blame? We have bulk collection now. Are any of them willing to accept the blame for the Boston bombing, for the recent shooting in Garland?

No, but they will be the first to point fingers and say: Oh, yes, it is all your fault. We never should have given up on this great program. I am completely convinced that we can obey the Constitution, use the Fourth Amendment as intended, spirited letter of the law, and catch terrorists. When we look objectively at this program, when they analyzed the classified information, they found that there was no unique data. We had to fight them tooth and nail because they started out saying that 52 cases were cracked by the bulk data program.

But then when the President's own bipartisan commission looked at it, it turned out that none of that was true. This gets back to the trust issue. If we are going to be lied to by the Director of National Intelligence, it is hard for us to believe them when they come forward and they say: Oh, this is protecting us. We have to have it. But what we are hearing is information from someone who really did not think it was a big deal to lie to us about whether the program even existed.

Mark my words, the battle is not over. There are some—and I talked with one of the, I would say, smarter people in Silicon Valley, somebody who knows this from an intimate level, how things work, and how the codes and programs work.

He maintains that the bulk collection of phone data is the tip of the iceberg, that there is more information in other data pools that are classified. Some of this is done through an Executive order called 12333. I am not sure I know everything in it. I have had no briefings on it. So anything I will tell you is from the newspaper alone. But the thing is, is that I would like to know: Are we also collecting your credit card information? Are we collecting your texts? Are we collecting your emails?

They have already told us the Fourth Amendment does not protect your emails, even the content, after 6 months. In fact, really they have told you, the Fourth Amendment does not apply to your records at all. So be very careful about the people who say: Trust us. We will never violate your freedom. We will never take advantage of things. The President's Privacy and Civil Liberties Oversight Board's conclusion was that:

> Section 215 of the PATRIOT Act has shown minimal value in safeguarding the Nation from terrorism. We have not identified any single instance involving a threat to the United States in which the program made a concrete difference in the outcome.

The President's privacy board went on to say:

> The government's collection of a person's entire telephone calling history has a significant and detrimental effect on individual privacy.

When they talked about whether the phone records were relevant to an investigation, the President's Commission said this:

> First, the telephone records acquired under the program have no connection to any specific FBI investigation at the time of their collection. Second, because the records are collected in bulk, potentially encompassing all telephone calling records across the Nation, they cannot be regarded as relevant to any FBI investigation.

Here is the continuing danger to us, though: It is, I think, maybe a minor success that we are going to prevent the government from collecting these records. But realize that the interpretation of this will still occur in secret in the FISA Court. This is the FISA Court that said that collecting everyone's records was relevant.

It completely destroys the notion that the word ''relevant'' has any meaning at all. This will be the question: Whether we can trust the FISA Court to make an interpretation that is at a higher degree of discernment than the one in which they said ''relevant'' can mean anything. The original USA FREEDOM Act, as passed originally by the House committee, was a better bill. It was gradually watered down until even the Director of National Intelligence, the one who lied about the program, now supports it, which gives me some misgivings.

But the records that will be collected—the question is, How will we have an interpretation by the FISA Court? The original bill had an advocate. I thought this was a good part of the original bill. There would be a judicial advocate who would argue on the side of those who were having their records taken. So there would be an adversarial court, lawyers on both sides.

Many people who write about jurisprudence and trying to find justice say that one of the essential functions of a court system, in order to find justice, is that there has to be a lawyer on both sides. There has to be an advocate on both sides. The truth is not always easy to find. The truth is presentation of facts by one side, presentation of contrary facts by the other side, and someone has to figure out which facts are more believable or which facts trump other facts.

So I think a judicial advocate would have been good. They are still going to have it. They call it by a different name now, but it will be optional at the discretion of the FISA Court. So the court that ruled that all of your records are relevant now will have a choice as to whether to give you an advocate. That does not give me a great deal of comfort.

There are other ways we could do this. We occasionally do look at terrorism cases in regular Federal court. When names come up that could jeopardize someone's safety at our intelligence agency or a secret, Federal courts can go into secret session. I have heard the Senator from Oregon often mention this. I think it is a great point that no one wants to reveal the names of anyone or the code or the secrets of how we do this. But if we are talking about constitutional principles, we want to do it in the open. Laws should not be discussed in secret.

As we move forward, the PATRIOT Act will expire tonight. It will only be temporary. They will ultimately get their way. But I think the majority of the American people actually do believe the government has gone too far. In Washington, it is the opposite, but I think Washington is out of touch. There will be 80 votes, you know, to say: Continue the PATRIOT Act—maybe more.

But if you go into the general public, if you get outside the beltway and visit America, you find it is completely the opposite. There was a poll a couple of weeks ago that said: Over 80 percent of people under age 40—over 80 percent of them—think that the government collecting your phone records is wrong and should not occur. So I think really this will be useful. People say: You are destroying yourself. You should have never done this. The American people will not side with you.

People wished me harm and wished that this would be unsuccessful. But you know what, I came here to defend the Bill of Rights and to defend the

Constitution, popular or not. But I frankly think that the Bill of Rights and the Constitution are very popular, very important, and I will continue, as long as I have breath and as long as I am here to defend them.

I yield back the remainder of my time.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Mr. President, before he leaves the floor, I just want to make sure, having worked with Senator PAUL for many, many months now, that I especially appreciate his efforts in the last few days in this week to try to accommodate this body with respect to amendments. My colleague has said repeatedly that he was very interested in a short list of amendments, that he hoped to have some modest time that would be available for these amendments.

He and I have worked together on a number of them. I think it is a reflection, as people think about this debate and on a topic that is of such enormous importance, that my colleague from Kentucky, especially with respect to this amendment issue, has tried continually to be reasonable and to be accommodating to this body.

Until just a few hours ago, I was at home in Oregon having townhall meetings, flew all night to be here for this extremely important session. Of course, the topic we discussed this evening was front and center in terms of my constituents.

The message from Oregonians at these townhall meetings was very clear. The people whom I have the honor to represent in the Senate want policies that advance their security and protect their liberties. The program we have been talking about tonight in the Senate really does not deliver either. It does not make us safer. It chips away at our liberties.

I am going to spend a little bit of time this evening making the case for those kinds of arguments and laying out the challenge for the days ahead.

Now, with respect to this safety issue, all of us understand—particularly the Presiding Officer, who has been on the Intelligence Committee, as I have, for over 14 years—that it is a dangerous world. Anyone who serves on the Intelligence Committee knows that beyond any kind of debate.

So we want policies that really deliver both security and liberty. This is what the President's own experts had to say with respect to this program that involves collecting millions and millions of phone records on law-abiding Americans. This was a group that was appointed and spent a considerable amount of time looking at the bulk phone records collection program. They issued a report, and will I just paraphrase what is the central finding, on page 104 of their report: As to information contributed to terrorist investigations by the use of section 215 telephony metadata—that is the collecting all of these millions and millions of phone records—these experts say that ''could readily have been obtained in a timely manner using conventional Section 215 orders.''

Now, the reason that is important is it spells out and recognizes that those who signed this report are individuals with some of the most pristine antiterror credentials in this country—Mike Morell, for example, the former Acting Director of the CIA; Richard Clarke, who held an extremely important position in two administrations and served with both Republicans and Democrats. Both of them are signatories to this important report.

Beyond that—and it has not received much attention—the reality is that our government, on top of everything else, has emergency authorities so that when those who are charged with protecting our country believe there is a threat to the Nation, they are allowed to issue an emergency authorization to get the information they need right away, and then they can go back and get the warrant approved after the fact.

Nobody is talking about eliminating that emergency authority. So what we have is a program that the most authoritative antiterror experts in the country believe does not make our Nation any safer. I read the most significant finding in their report.

On top of that, as I just indicated, emergency authorities are still preserved. In fact, I have indicated to our President and to those who work in the intelligence agencies that if at any point the executive branch and, particularly, the intelligence agencies feel that their emergency authorities are inadequate to protect the country, I personally would be willing to support efforts to ensure that those emergency capabilities are reformed and our country can take the steps it needs when it is necessary.

On top of this question, with respect to the issue of our safety, I want to talk about what I heard at some length earlier today with respect to how the program worked. I heard a number of Senators say that nobody in government is listening to these calls. That was repeated a number of times on the floor of this body.

When the government, under this program, knows whom you called, when you called, and where you called from, in many instances the government doesn't need to be listening. If the government knows, under this program, that a person called a psychiatrist 3 times in 36 hours—twice after midnight—that is a lot of private and personal information. The government doesn't need to be listening to that call.

So as to this notion that some who have wanted to make sure that our country would have both security and liberty are saying that it is a fantasy that the government is listening to calls, I could tell you that those who have been trying to reform the program have said, in effect, that the government doesn't need to listen to those calls. If the government has that amount of private and personal information, the government knows a lot about you, and it really doesn't need to listen. Certainly, if you are talking about a land line, then the government knows where you are calling from if they have a phone book.

So with respect to this question of the government listening, I want it particularly understood that a program such as this, when the government has this kind of information, I believe, represents a threat to our liberty. The reason why I think so is that hardly a week goes by when databases aren't violated. No. 1, we see that reported regularly in the press. No. 2, we have known about unfortunate times in our history—J. Edgar Hoover comes to mind—when this kind of information could be used. And, No. 3, I have been very concerned, given what our former colleague, Senator UDALL, and I had to do with respect to bulk phone record collection of email. We battled to end this. Of course, this was email that could be read by government agencies. We battled with various intelligence leaders saying that we felt this was a violation of people's rights and it wasn't effective. They asserted for months and months that it was. Finally, one day they woke up and said the program wasn't needed any more.

None of this would have even happened had not Senator Udall and I made that case repeatedly. The intelligence leadership knew that we were not going to give it up, but that is what goes on if there isn't a check on some of these kinds of procedures.

Senator PAUL made mention of the fact that the intelligence leadership has not exactly been straight with the American people on these issues. I emphasize that we are not talking about the thousands and thousands of law-abiding patriotic, dedicated, wonderful people who work in the intelligence field. Day in and day out they do so much for our country. We are so appreciative of all they do. They are the ones who do the hard work, for example, to capture Bin Laden and day in and day out to make us safer. But the intelligence leadership, on the other hand, as noted by our colleague from Kentucky, has not always been straight with the American people. I spent many months trying to decipher what the former NSA Director meant when he said the government doesn't collect any dossiers on millions of Americans.

I pointed out I had been on the Intelligence Committee for a long time and I had never heard the term ''dossier'' used. So I tried to learn more about it, used private opportunities and public opportunities, and just couldn't get the information. So, finally, I said: I have to ask this question in public.

On the Intelligence Committee you don't get but perhaps 20 or 25 minutes a year to ask questions in public, to hold intelligence leaders accountable

on policy matters—not secret operations, because secret operations have to stay secret, but policy matters.

So, after being stonewalled for many months—many months—I finally said I have to ask this question in public. So to make sure no one would feel ambushed, I sent the question to the Director of National Intelligence, Mr. Clapper. I sent it a day ahead of time.

Then I didn't hear anything about its being inappropriate or in violation of classification rules. So I asked in public: Does the government collect any type of data at all on millions or hundreds of millions of Americans? I was told no, and that answer was obviously false. I tried to get it corrected, and we still couldn't get it corrected.

Of course, then Mr. Snowden spoke out publicly and pointed that out. Since that time, the Director of National Intelligence and his representatives have given these five different explanations for why that answer was given. So that is why you have to ask the hard questions. You have to ask the hard questions about these issues.

I see my friend and colleague Senator HEINRICH has joined us tonight. I am so pleased that he has joined the Intelligence Committee. Senator HEINRICH is one of those Senators who subscribes to that view that I just mentioned—that it is our job to ask the hard questions. It may be uncomfortable. It is not designed in any way to convey disrespect. We see it as our job to ask the hard questions.

I would be interested in my colleague's thoughts with respect to this issue and to have him be given a chance to participate in this colloquy.

The PRESIDING OFFICER (Mr. JOHNSON). Without objection, it is so ordered.

Mr. HEINRICH. First, I thank my friend from Oregon and I recognize the substantial leadership he has shown on this issue over the years. Long before I came to the Intelligence Committee and long before Edward Snowden began to steal documents, Senator WYDEN, along with Senator Mark Udall and others, were doing everything they could—without disclosing classified information—to shine a light on the fact that the U.S. Government was collecting massive volumes of data on millions of law-abiding American citizens. My friend from Oregon deserves our thanks for that leadership.

Now, after the bulk call data collection program was revealed to the public, the government, frankly, defended it and defended it vigorously. It took a number of months for the intelligence community and the rest of the administration to take a deep breath and really assess whether bulk metadata collection was necessary, whether it was effective, and to consider whether there were other less intrusive, more constitutionally grounded ways to accomplish these same goals.

Starting with the President's Review Group on Intelligence and Communications Technologies, the administration began to agree that ''some of the authorities that were expanded or created in the aftermath of September 11 unduly sacrifice fundamental interests in individual liberty, personal privacy, and democratic governance.'' And they recommended changing those authorities in order to ''strike a better balance between the competing interests and providing for the common defense and securing 'the Blessings of Liberty to ourselves and our Posterity.' ''

Following that, multiple efforts have been made to update and reform FISA and to update and reform the USA PATRIOT Act. None of those have been successful. But now we are forced to come to a resolution through a combination of, frankly, procrastination, and, I think, misguided hope that the American people would look the other way while the government continued to vacuum up and store their personal information and data as part of a program that even the intelligence community acknowledges can be accomplished through less intrusive means.

I will be honest. The current USA FREEDOM Act isn't what I consider perfect. For example, I prefer that it include strong reform of section 702 collection, but I accept that circumstances require us to be pragmatic, require us to govern and move forward and to work with one another in both parties to find compromise. That is what the USA FREEDOM Act is. It is a product of bipartisan compromise.

That is why it passed the House of Representatives by a vote of 338 to 88. And let's be blunt, many of those who voted against it didn't do so because they support bulk collection. They did so because they want to see section 215 wither and die in its entirety. That is the political reality we face today, and we need to accept it rather than demanding a continuation of a program that the appeals court has determined is illegal.

Mr. WYDEN. I thank my colleague for his statements and would just want to explore this a little bit further. I hope that those who are following this debate understand that my colleague from New Mexico is a real rising star in the Senate. He and I would like the USA FREEDOM Act to go further, and we both worked together on legislation that would make additional reforms. Certainly, our colleagues on the Intelligence Committee and here in the Senate can expect to see us continuing to work together to advance these additional reforms over the coming months and years. For now, the two of us are saying we ought to support the USA FREEDOM Act and then move on—move on to other critical areas.

I particularly want to see closed what is called the backdoor search loophole, which my colleague from New Mexico talked about. What this means, colleagues, is that when you are engaged in a lawful search of someone who is a threat overseas, pursuant to section 702 of the Foreign Intelligence Surveillance Act, very often law-abiding Americans can get swept up in this search and have their emails looked at.

This is a problem today, and my view is it is likely to be a growing concern in the future because, increasingly, communications systems around the world are becoming globally integrated, so the amount of emails that are reviewed of Americans is likely to grow. But we can't get that change here tonight. So, as my colleague from New Mexico has mentioned, the USA FREEDOM Act would make several worthwhile reforms, such as increasing transparency, reducing the government's reliance on secret laws. But from my perspective, the centerpiece of it is ending the bulk collection of Americans' information under the PATRIOT Act.

I have been trying to close this particular loophole for close to a decade now. Some of our colleagues have said the bulk collection has never been abused; that no one's rights have been violated. My own view is—and I will ask what my colleague thinks—that vacuuming up all this information, particularly when databases get violated all the time—we have seen historically instances where there has been improper conduct by the government. I believe dragnet surveillance violates the rights of millions of our people every day.

Vacuuming up the private phone records of millions of Americans with no connection to wrongdoing is simply a violation of their rights.

And vacuuming up Americans' email records, which I pointed out before my colleague came to the floor—which he and our former colleague Senator Udall and I battled—is surely a violation of the rights of Americans as well. Colleagues, that wouldn't have been pointed out at all—it wouldn't have been pointed out at all—unless Senator Udall and I, with the help of our friend from New Mexico, hadn't been pushing back on it. Finally, one day the government said: Well, we will get rid of it because it wasn't effective. They got rid of it because they saw they were going to get hard questions, the kinds of questions my friend from New Mexico has been asking.

Now, with respect to the legality of this program, I know my colleague and I actually filed a legal brief, along with our former colleague Mark Udall, when the Court of Appeals for the Second Circuit was examining that program. In our brief, it was argued that we were able to debunk many of the claims that had been made about the effectiveness of the program.

I think it would be helpful if my colleague from New Mexico laid out some of that analysis here tonight. I would ask the Senator from New Mexico to begin, and I would encourage him to start by addressing the claim that the bulk collection of Americans' phone records is essential for stopping terrorist attacks. My question to my colleague is, Is there any evidence, any

real concrete evidence, to support that claim?

Mr. HEINRICH. I thank my friend from Oregon and begin by saying that despite what we may have heard from talking heads on the Sunday shows and on the cable news networks, the answer is no. There is simply no evidence to support those claims.

When this mass surveillance was first revealed to the public 2 years ago, the executive branch initially responded to questions like this by claiming that various post-9/11 authorities had resulted in the thwarting of approximately ''54 terrorist events in the U.S. homeland and abroad.''

Now, a number of us, including my friend from Oregon and my former colleague from Colorado, Senator Udall, began to pull on that thread to really parse down and see just what the executive branch was talking about. First, of those 54 terrorist events, it turned out that only 13 were actually focused in the United States. But more importantly, those numbers conflated multiple different programs, including authorities under section 215 and different authorities under section 702.

On June 19, 2013, my colleague from Oregon and Senator Udall pointed out that ''it appears that the bulk phone records collection program under section 215 of the USA PATRIOT Act played little or no role in most of these disruptions. Saying that 'these programs' have disrupted 'dozens of potential terrorist plots' is misleading if the bulk phone records collection program is actually providing little or no unique value.''

Of the original 54 instances the executive branch pointed to, every one of them crumbled under scrutiny. None of them actually justified the continued existence of the bulk collection program.

Let me take a moment, with the indulgence of our colleagues, and read what was written by Judge Leon of the District Court for the District of Columbia, when he ruled in the Klayman v. Obama case. This is a little long, but I think it is important this be part of the official record of this debate.

Judge Leon writes:

[T]he Government does not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three ''recent episodes'' cited by the Government that supposedly ''illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack'' involved any apparent urgency.

He continues to write that:

[]In the first example, the FBI learned of a terrorist plot still ''in its early stages'' and investigated that plot before turning to the metadata ''to ensure that all potential connections were identified.'' []Assistant Director Holley does not say that the metadata revealed any new information—much less time-sensitive information—that had not already come to light in the investigation up to that point.

The judge continues:

[]In the second example, it appears that the metadata analysis was used only after the terrorist was arrested ''to establish [his] foreign ties and put them in context with his U.S. based planning efforts.'' []And in the third, the metadata analysis ''revealed a previously unknown number for [a] co-conspirator . . . and corroborated his connection to [the target of the investigation] as well as to other U.S.-based extremists.''

Continuing to quote Judge Leon:

[]Again, there is no indication that these revelations were immediately useful or that they prevented an impending attack. Assistant Director Holley even concedes that bulk metadata analysis only ''sometimes provides information earlier than the FBI's other investigative methods and techniques.''

Finally, Judge Leon writes:

[]Given the limited record before me at this point in the litigation—most notably, the utter lack of evidence that a terrorist attack has ever been prevented because of searching the NSA database was faster than other investigative tactics—I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.

That is where the judge leaves off. And I will turn back to the Senator from Oregon to address the three cases we discussed in more detail in our amicus brief to the Second Circuit.

Mr. WYDEN. I thank my colleague. The first of these examples—and they really are kind of overblown examples about the effectiveness of bulk collection—is the case of an individual named Najibullah Zazi. Mr. Zazi was a known terrorism suspect, and a number of people have suggested that bulk phone records collection was somehow essential to stopping him because a query of the bulk phone records database for numbers linked to Mr. Zazi returned a previously unknown number belonging to another terrorism suspect.

However, since the government had already identified Zazi as a terrorism suspect prior to querying the bulk phone records database, it had all the evidence it needed to obtain the phone records of Zazi and his associates using an individualized section 215 order or other legal authorities.

In the second case, some have pointed to Mr. Moalin, the San Diego man convicted of sending $8,500 to support al-Shabaab in Somalia. The intelligence community has indicated that information from the bulk phone records database ''established a connection between a phone number known to be used by an extremist overseas . . . and an unknown San Diego-based number'' that belonged to Mr. Moalin. Yet there are ample existing authorities under which the United States can conduct surveillance on a phone number known to be used by extremists overseas and other phone numbers in contact with that phone number.

The argument that Mr. Moalin's case is an example of a unique value of bulk phone records collection is just not accurate. My view is this is yet another case that offers a misleading exaggeration with respect to the effectiveness of bulk phone records collection.

Finally, several supporters of the bulk metadata program have claimed that ''[i]f we had had [the bulk phone-records] program in place at the time [of the September 11, 2001 attacks,] we would have been able to identify'' the phone number of one of the hijackers, Khalid al-Mihdhar.

Just as in these other cases, however, the record indicates that Mr. Mihdhar's phone number could also have been obtained by the government using a variety of alternate means. Before September 11, the government was surveilling a safe house in Yemen but failed to realize that Mr. Mihdhar, who was in contact with the safe house, was actually inside the United States. The government could have used any number of authorities to determine whether anyone in our country was in contact with the safe house it was already targeting. It didn't need a record of every Americans' phone calls to establish that simple connection.

Mr. HEINRICH. I wish to expound on that point a bit, about the many other ways the government can legitimately acquire phone records of terrorism suspects, because I think this is a very important point to understand the tools that already exist that have been very effective and have proven themselves over time.

There are actually a number of legal authorities that can get the same information without the government collecting billions of call records—billions of call records that, in large part, belong to innocent Americans.

For example, the Stored Communications Act permits the government to obtain precisely the same call records that are now acquired through bulk collection under section 215 when they are ''relevant and material to an ongoing criminal investigation.''

Additionally, national security letters, which I point out do not require a court order, can also be used by the government to obtain call records for intelligence purposes.

Further, the government can also acquire telephony metadata on a real-time basis by obtaining orders from either regular Federal courts or the FISC for the installation of pen registers or trap-and-trace devices.

Finally, individualized orders for phone records, as opposed to orders authorizing broad bulk collection, can also be obtained under section 215.

I think those of us early in this debate thought that was what was going to occur under the PATRIOT Act in the first place. But that is what the USA FREEDOM Act seeks to require while prohibiting the bulk collection of millions of personal records. It even includes emergency authorization authority for the government to get records prior to getting court approval, subject to later court approval, in an emergency.

The government can use any of these authorities without any more evidence

than what is currently required to use the bulk phone records database, with less impact, I would point out, on the privacy interests of millions of innocent Americans.

I think at this point the Senator from Oregon and I have laid out our case as to why this dragnet bulk surveillance program fails to make our country measurably safer and why it should end. I am pleased to say that a number of people have finally come around to our way of thinking on this.

Mr. WYDEN. I thank my colleague. I will wrap up and then give the last word to my friend from New Mexico on the subject. He is absolutely right that some of the most authoritative leaders in our country—experts on terror—have reached the same judgment we have. I made mention of the President's Review Group on Intelligence and Communications Technologies, and I really would encourage colleagues who are following this debate and citizens across the country—that report is available online, and it is available in our office. Page 104 of that report is very explicit. It says that the information that would otherwise be obtained in collecting all of these phone records—millions of phone records of law-abiding Americans, people such as Mike Morell, former Acting Director of the CIA, and Richard Clark, who served in two administrations—they said it could have been obtained through conventional processes.

This is a program that is not making us safer. And it is not my judgment that ought to be the last word; it should be that of people like those I just quoted.

The Privacy and Civil Liberties Oversight Board's report on the telephone records program said pretty much the same thing:

> [T]he Section 215 program has shown minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation.

I will close by way of saying—and I touched on this before my friend from New Mexico arrived—I would like to do a lot more than I believe is likely to happen here quickly in the Senate. I do want to see us finally throw in the dustbin of history this bulk phone records collection program because it doesn't make us safer and it compromises our liberty. But, as I indicated to my friend from New Mexico, I would also like to close this backdoor search loophole in the FISA Act, which is going to be a bigger problem in the days ahead given the evolution of communications systems and how they have become globally integrated.

I will close by saying that one of the most important issues we are going to have to tackle in the days ahead is going to deal with encryption. Encryption, of course, is the encoding of data and messages so that they cannot be easily read. The reason this will be an enormously important issue—and my colleague and I have talked about this—is because of the NSA overreach, the collection of all these phone records of law-abiding people. A lot of our most innovative, cutting-edge companies have found their customers raising real questions about whether their products can be used safely, and a lot of the purchasers who buy their products around the world are saying: Maybe we shouldn't trust them. Maybe we should try to start taking control over their servers and have local storage requirements and that sort of thing. So what our companies did, because they saw the effect of the overreach by the NSA, was they started to use encryption to protect the data and messages of the consumers who buy their products.

Most recently, the head of the FBI, Mr. Comey, rather than try to come back with a solution that protected both our privacy and our security, he said he was interested in requiring companies to build weaknesses into their products. Just think about that—requiring companies to build weaknesses into their products. So the government—which, in effect, caused this problem with the overreach—in effect, rather than trying to find a solution that worked for both security and liberty, said: We will start talking about requiring companies to actually build weaknesses into their products.

I and others have pointed out that once you do that, hang on to your hat. When the good guys have the keys, that is one thing, but when companies are required to build weaknesses into their products, the bad guys are going to get the keys in a hurry, too. And with all the cyber hacking and the risks we already have, we ought to be really careful about going where Mr. Comey, our FBI Director, has proposed to go.

But that is not for tonight. Tonight is not an occasion where we will be able to, on a bipartisan basis, close the backdoor-search loophole or where we will be able to come up with a sensible policy with respect to encryption rather than requiring companies to actually build weaknesses in their products. We will not be able to do that tonight. But we will now have a chance here in the Senate to take steps that have been bipartisan both here in the Senate and in the other body, in the House of Representatives, to end the bulk phone records collection program because it doesn't make us safer and it threatens our liberties.

I always like to close by thinking about Ben Franklin, who said that anybody who gives up their liberty to have security really doesn't deserve either.

I am so pleased to have a chance to serve with my colleague from New Mexico on the Intelligence Committee, who is going to be a thoughtful advocate for these kinds of policies, in my view, for many years to come. I thank him for his involvement tonight and would be happy to give him the last word of our colloquy at this time.

I yield to my colleague.

Mr. HEINRICH. I thank my friend from Oregon. I think he could not have chosen a more appropriate way to end than to reference what Ben Franklin said so many years ago, that great quote that ''those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.''

While many reforms still lie in front of us, I think, as we move forward to approving the USA FREEDOM Act, we move a lot closer to the balance that Ben Franklin articulated so well over 200 years ago. I look forward to working with my colleague from Oregon and all of our colleagues in achieving that balance and standing up for our constituents.

Mr. WYDEN. Mr. President, I yield the floor.

Mr. LEAHY. Mr. President, we did not have to end up here, just hours away from the midnight expiration of three surveillance authorities, and having just moved to proceed to the USA FREEDOM Act.

I have tried since last year to move legislation through the Senate to address these sunsets. In November, Senator REID brought the USA FREEDOM Act to the floor but the Republican leadership of the Senate blocked debate on it. When they took over the Senate, they assured us that they would send bills—including this one—through appropriate committee process. There were promises that the new leadership would not fill the amendment tree, and would use a transparent legislative process. But not one of those promises has been fulfilled with respect to any legislation dealing with the upcoming sunsets.

Once again this year, I proposed with Senator LEE a new version of the USA FREEDOM Act. That bill had significant process in the House, where it passed by an overwhelming margin earlier this month. And once again, the bipartisan coalition here in the Senate tried to get the bill passed. Two Fridays ago, the Senate Republican leadership did not allow us to debate the bill.

Tonight, the Senate did the right thing by invoking cloture on the motion to proceed to the USA FREEDOM Act. I am glad to see several Republicans switched their votes. This is significant progress, but it is late in coming.

We should have proceeded to this bill two Fridays ago. Had we done so, we could have stayed here to do our work, considered amendments, and passed the bill well in advance of tonight's sunset. Instead, we are hours away from expiration and just now considering legislation that many of us have been working on for years. Our intelligence community needs predictability and certainty, not a manufactured crisis.

If all Senators cooperate, we can finish this bill tonight. We can consider a

handful of amendments under a time agreement, and pass this bill before midnight. That would be the responsible thing to do.

Mr. BARRASSO. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

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

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

Mr. MCCONNELL. Madam President, I know of no further debate on the motion.

The PRESIDING OFFICER. The question is on agreeing to the motion to proceed.

The motion was agreed to.

USA FREEDOM ACT OF 2015

The PRESIDING OFFICER. The clerk will report the bill by title.

The legislative clerk read as follows:

A bill (H.R. 2048) to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes.

AMENDMENT NO. 1449

(Purpose: In the nature of a substitute)

Mr. MCCONNELL. Madam President, I have a substitute amendment at the desk that I ask the clerk to report.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Kentucky [Mr. MCCONNELL] proposes an amendment numbered 1449.

Mr. MCCONNELL. 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 printed in today's RECORD under ''Text of Amendments.'')

Mr. MCCONNELL. I ask for the yeas and nays on my amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 1450 TO AMENDMENT NO. 1449

Mr. MCCONNELL. Madam President, I have an amendment at the desk.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Kentucky [Mr. MCCONNELL] proposes an amendment numbered 1450 to amendment No. 1449.

Mr. MCCONNELL. 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:

Strike Sec. 110(a) and insert the following:

(a) IN GENERAL.—The amendments made by sections 101 through 103 shall take effect on the date that is 12 months after the date of the enactment of this Act.

Mr. MCCONNELL. I ask for the yeas and nays on my amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 1451 TO AMENDMENT NO. 1450

Mr. MCCONNELL. I have a second-degree amendment at the desk.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Kentucky [Mr. MCCONNELL] proposes an amendment numbered 1451 to amendment No. 1450.

The amendment is as follows:

(Purpose: To improve the amendment)

At the end, add the following:

(b) NONEFFECT OF CERTAIN PROVISIONS.—Section 401 of this Act, relating to appointment of amicus curiae, shall have no force or effect.

SEC. 110A. APPOINTMENT OF AMICUS CURIAE.

Section 103 (50 U.S.C. 1803) is amended by adding at the end the following new subsections:

''(i) AMICUS CURIAE.—

''(1) AUTHORIZATION.—A court established under subsection (a) or (b) is authorized, consistent with the requirement of subsection (c) and any other statutory requirement that the court act expeditiously or within a stated time—

''(A) to appoint amicus curiae to—

''(i) assist the court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law; or

''(ii) provide technical expertise in any instance the court considers appropriate; or

''(B) upon motion, to permit an individual or organization leave to file an amicus curiae brief.

''(2) DESIGNATION.—The courts established by subsection (a) and (b) shall each designate 1 or more individuals who may be appointed to serve as amicus curiae and who are determined to be eligible for access to classified national security information necessary to participate in matters before such courts (if such access is necessary for participation in the matters for which they may be appointed). In appointing an amicus curiae pursuant to paragraph (1), the court may choose from among those so designated.

''(3) EXPERTISE.—An individual appointed as an amicus curiae under paragraph (1) may be an individual who possesses expertise on privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise to the court.

''(4) DUTIES.—An amicus curiae appointed under paragraph (1) to assist with the consideration of a covered matter shall carry out the duties assigned by the appointing court. That court may authorize the amicus curiae to review any application, certification, petition, motion, or other submission that the court determines is relevant to the duties assigned by the court.

''(5) NOTIFICATION.—A court established under subsection (a) or (b) shall notify the Attorney General of each exercise of the authority to appoint an amicus curiae under paragraph (1).

''(6) ASSISTANCE.—A court established under subsection (a) or (b) may request and receive (including on a non-reimbursable basis) the assistance of the executive branch in the implementation of this subsection.

''(7) ADMINISTRATION.—A court established under subsection (a) or (b) may provide for the designation, appointment, removal, training, or other support of an amicus curiae appointed under paragraph (1) in a manner that is not inconsistent with this subsection.

''(j) REVIEW OF FISA COURT DECISIONS.—Following issuance of an order under this Act, a court established under subsection (a) shall certify for review to the court established under subsection (b) any question of law that may affect resolution of the matter in controversy that the court determines warrants such review because of a need for uniformity or because consideration by the court established under subsection (b) would serve the interests of justice. Upon certification of a question of law under this subsection, the court established under subsection (b) may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy.

''(k) REVIEW OF FISA COURT OF REVIEW DECISIONS.—

''(1) CERTIFICATION.—For purposes of section 1254(2) of title 28, United States Code, the court of review established under subsection (b) shall be considered to be a court of appeals.

''(2) AMICUS CURIAE BRIEFING.—Upon certification of an application under paragraph (1), the Supreme Court of the United States may appoint an amicus curiae designated under subsection (i)(3), or any other person, to provide briefing or other assistance.''.

AMENDMENT NO. 1452

Mr. MCCONNELL. I have an amendment to the text proposed to be stricken.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Kentucky [Mr. MCCONNELLL] proposes an amendment numbered 1452 to the language proposed to be stricken by amendment No. 1449.

(The amendment is printed in today's RECORD under ''Text of Amendments.'')

Mr. MCCONNELL. I ask for the yeas and nays on my amendment.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The yeas and nays were ordered.

AMENDMENT NO. 1453 TO AMENDMENT NO. 1452

Mr. MCCONNELL. I have a second-degree amendment at the desk.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Kentucky [Mr. MCCONNELL] proposes an amendment numbered 1453 to amendment No. 1452.

The amendment is as follows:

At the end of the amendment, add the following:

''This Act shall take effect 1 day after the date of enactment.''

CLOTURE MOTION

Mr. MCCONNELL. Madam President, I have a cloture motion at the desk.

The PRESIDING OFFICER. The cloture motion having been presented under rule XXII, the Chair directs the clerk to read the motion.

The legislative clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of rule XXII of the