

omit key considerations that can prove critical for those seeking to understand the import of the court's full opinion. This is particularly likely to be a problem in the fact-focused area of FISA practice, under circumstances where the government has already decided that it cannot release the underlying opinion even in redacted form, presumably because the opinion's legal analysis is inextricably intertwined with classified facts.

ADDITIONAL TECHNICAL COMMENTS ON H.R. 2048

The Judiciary, like the public, did not participate in the discussions between the Administration and congressional leaders that led to H.R. 2048 (publicly released on April 28, 2015 and reported by the Judiciary Committee without changes on April 30). In the few days we have had to review the bill, we have noted a few technical concerns that we hope can be addressed prior to finalization of the legislation, should Congress choose to enact it. These concerns (all in the *amicus curiae* subsection) include:

Proposed subparagraph (9) appears inadvertently to omit the ability of the FISA Courts to train and administer amici between the time they are designated and the time they are appointed.

Proposed subparagraph (6) does not make any provision for a "true amicus" appointed under subparagraph (2)(B) to receive necessary information.

We are concerned that a lack of parallel construction in proposed clause (6)(A)(i) (apparently differentiating between access to legal precedent as opposed to access to other materials) could lead to confusion in its application.

We recommend adding additional language to clarify that the exercise of the duties under proposed subparagraph (4) would occur in the context of Court rules (for example, deadlines and service requirements).

We believe that slightly greater clarity could be provided regarding the nature of the obligations referred to in proposed subparagraph (10). These concerns would generally be avoided or addressed by substituting the FIA approach. Furthermore, it bears emphasis that, even if H.R. 2048 were amended to address all of these technical points, our more fundamental concerns about the "panel of experts" approach would not be fully assuaged. Nonetheless, our staff stands ready to work with your staff to provide suggested textual changes to address each of these concerns.

Finally, although we have no particular objection to the requirement in this legislation of a report by the Director of the AO, Congress should be aware that the AO's role would be to receive information from the FISA Courts and then simply transmit the report as directed by law.

For the sake of brevity, we are not restating here all the comments in our previous correspondence to Congress on proposed legislation similar to H.R. 2048. However, the issues raised in those letters continue to be of importance to us.

We hope these comments are helpful to the House of Representatives in its consideration of this legislation. If we may be of further assistance in this or any other matter, please contact me or our Office of Legislative Affairs at 202-502-1700.

Sincerely,

JAMES C. DUFF,
Director.

ORDER OF PROCEDURE

Mr. McCONNELL. Madam President, I ask unanimous consent that the Senate stand in recess from 12:30 p.m. until

2:15 p.m. to allow for the weekly conference meetings.

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

Mr. McCONNELL. Madam President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

RESERVATION OF LEADER TIME

The PRESIDING OFFICER. Under the previous order, the leadership time is reserved.

USA FREEDOM ACT OF 2015

The PRESIDING OFFICER. Under the previous order, the Senate will resume consideration of H.R. 2048, which the clerk will report.

The senior assistant 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.

Pending:

McConnell/Burr amendment No. 1449, in the nature of a substitute.

McConnell amendment No. 1450 (to amendment No. 1449), of a perfecting nature.

McConnell amendment No. 1451 (to amendment No. 1450), relating to appointment of *amicus curiae*.

McConnell/Burr amendment No. 1452 (to the language proposed to be stricken by amendment No. 1449), of a perfecting nature.

McConnell amendment No. 1453 (to amendment No. 1452), to change the enactment date.

Mr. DURBIN. Mr. President, I ask unanimous consent to speak for 2 minutes as in morning business.

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

REMEMBERING HADIYA PENDLETON AND COMMEMORATING NATIONAL GUN VIOLENCE AWARENESS DAY

Mr. DURBIN. Mr. President, on January 29, 2013, Hadiya Pendleton was gunned down while standing in a park on the South Side of Chicago. Hadiya was a talented, beautiful, caring young woman with a bright future ahead of her. She was 15 years old, a sophomore honor student at King College Prep. Her family described her as a spectacular source of joy and pride for them.

One week before her death, Hadiya was here in Washington with her school band, performing for President Obama's second inauguration. She was thrilled by that opportunity. But a few days later, she was gone, murdered by men who mistook her and friends for members of a rival gang.

What a senseless tragedy to lose children to gun violence. It happens every day in America. Overall, on average, 88 Americans are killed by gun violence every day.

Today, June 2, 2015, would have been Hadiya Pendleton's 18th birthday. Today also marks the first annual National Gun Violence Awareness Day. It is an idea that was inspired by Hadiya's family and friends in Chicago. They decided they would ask us to wear something orange today. It is a color that hunters use when they are in the woods to make sure that no one shoots them.

All across the Nation, Americans are wearing orange in tribute to Hadiya Pendleton, in tribute to the tens of thousands of other Americans killed by gun violence every year, and in support of a simple goal: Keep our kids safe. I am proud to join them in wearing orange today. I want to commend Hadiya's parents—my friends—Nate and Cleo, her brother Nate, Jr., and her friends who have turned their pain into purpose.

They are working to reduce the scourge of gun violence and to spare other families and loved ones what they have gone through. I hope lawmakers here in Washington and throughout the Nation will pay attention and commit themselves to do something about these terrible shootings and deaths. We need to do all that we can to keep guns out of the hands of those who would misuse them and, especially, keep our children safe.

I yield the floor.

The PRESIDING OFFICER. The Senator from Maine.

Ms. COLLINS. Mr. President, in the aftermath of the terrorist attacks on our country on 9/11/2001—terrorist attacks that killed some 3,000 people—I authored legislation, along with former Senator Joe Lieberman of Connecticut, to implement the recommendations of the 9/11 Commission to reform and restructure the intelligence community, to improve its capabilities, and also to increase accountability and oversight.

Now, this law is different and distinct from the PATRIOT Act. Our law established the Office of the Director of National Intelligence to coordinate all of the agencies involved in intelligence gathering so that we would reduce the possibility of the dots not being connected and to allow terrorist attacks and plots to be detected and thwarted.

Our legislation also created the National Counterterrorism Center, which helps to synthesize the information across government and share it with State and local governments to help keep us safer. Our bill created the Privacy and Civil Liberties Oversight Board, and it installed privacy officers in the major intelligence agencies.

But our law, the Intelligence Reform and Terrorism Protection Act, shared the common goal of the PATRIOT Act of better protecting our Nation from terrorist attacks because none of us who lived through that terrible day

ever wanted to see Americans die again because our Nation failed to use the tools and capabilities it had to prevent terrorist attacks.

We have had terrorist attacks since that time. The Boston Marathon is an example of a terrorist attack that occurred despite our best efforts, but we have been able to thwart and uncover and detect and stop terrorist attacks—both here and abroad—due to the important tools and capabilities our government has. Like the Presiding Officer, I serve on the Senate Select Committee on Intelligence. I have sat through countless hours of briefings, I have asked the hard questions about our intelligence programs, and I have challenged those who have come before us.

I wish to explain how the current program works at NSA because I believe there is so much misinformation about this important program. One of the most egregious misinformation points that have been made is that the NSA is listening to the content of calls made by American citizens to other American citizens. That is simply not true.

Let me tell you how this program works. First, it starts with a call, a phone number from a foreign terrorist or a foreign terrorist organization. When we get a foreign terrorist's—who is based overseas—telephone number, the NSA is allowed to query a database to see if that foreign-based terrorist is calling someone in our country. Why is that important? Well, we know ISIS and other terrorist groups have been recruiting Americans and trying to train them to attack our country. That is why it is important.

Only 34 highly trained, vetted Federal employees are allowed to query that database, and even then they are allowed to do so only if a Federal judge finds that a standard has been reached to allow that query to be made. Even if that query is approved by that Federal judge, the analyst can only see the phone numbers called by the terrorist, the date, the time, and the duration of the call.

If there is a match, then the case is turned over to the FBI for further investigation. The FBI must get a court order to wiretap the phone of the American who is talking to that foreign terrorist.

Last month, during a Senate Appropriations Committee hearing, I asked the Attorney General whether there have ever been any privacy violations regarding that telephone data. She replied no.

I am truly perplexed that anyone would argue that telephone data are better protected in the hands of 1,400 telecom companies and 160 wireless carriers than in a secure NSA database that only 34 carefully vetted and trained employees are allowed to query under the supervision of a Federal judge.

Under the USA FREEDOM Act—the House bill—when we get the telephone

number of an overseas terrorist, we potentially are going to have to go to each one of those 1,400 telecom companies, 160 wireless carriers, which potentially will involve thousands of people. The privacy implications are far greater if we have the telecoms control the data, far greater.

Moreover, we know private sector data is far more susceptible to hackers, to criminals. Look at all the breaches of sensitive data that have occurred during the past year alone. Plus, I simply don't think the system will work without a data-retention requirement now that most carriers have flat-rate telephone plans that don't require detailed call data records. The telecom companies have made very clear they will oppose any bill with a data-retention requirement, and there will be a race to the bottom to market the data in a way that says to people: Sign up with us and your data will be safe from the government.

That kind of demagoguery—even though the commerce committee has done an excellent study that shows the data broker companies sell our personal data, including our names, our phone numbers, our addresses to the highest bidder for telemarketing and other purposes, and some of that data ends up in the hands of con artists.

So I don't see how vesting the authority in the telecom communications companies increases the privacy of our data, safeguards it. I think just the opposite is the case. It is going to be less secure because it is going to be more exposed to hackers and criminals who will attempt to do data breaches and have successfully done so. It is going to be less secure because instead of 34 people having access to just the phone numbers and call duration data, we are going to have potentially thousands of people who are going to be asked to query their database. The system is going to be less effective because there is absolutely no guarantee this data will be retained by the telecom companies and the wireless carriers.

Finally, I am persuaded by the cautions given to us, by the direct warnings of former Director of the FBI Robert Mueller and the former Deputy Director of the CIA Mike Morell, who tell us that had this program been in place prior to 9/11, it is likely that terrorist plot would have been uncovered and thwarted.

The fact is the House bill substantially weakens a vital tool in our counterterrorism efforts at a time when the terrorist threat has never been higher. The current program has never been abused. The government cannot listen to your phone calls or read your emails unless there is a court order—because you are directly communicating with an overseas terrorist—and then it goes to the FBI for investigation.

It is a false choice that we have to choose between our civil liberties and keeping our country safe. There are actions we can and should take to strengthen the privacy protections in

the NSA program. Several were included in the bipartisan bill reported by the Intelligence Committee last year. Unfortunately, the USA FREEDOM Act provides a false sense of privacy at the expense of our national security.

For these reasons, while I will support the amendments today to try to make modest improvements to the House bill, I simply cannot support the bill on final passage.

I yield the floor.

THE PRESIDING OFFICER. The Senator from Utah.

Mr. LEE. Mr. President, I ask unanimous consent to speak for an additional 7 minutes, to be divided between Senator LEAHY and myself.

THE PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

Mr. LEAHY. Mr. President, I thank the Senator from Utah for his courtesy.

The fact is the USA FREEDOM Act that was passed overwhelmingly in the House of Representatives—that has strong bipartisan support here—is supported by the Director of National Intelligence. It is also supported by our Attorney General. It is supported by our intelligence community. And it is a step forward because, ultimately, the legislation protects the privacy of individuals.

I agree with the Senator from Maine that we have strong restrictions at the NSA on the information. However, they were not strong enough, of course, to stop Edward Snowden from walking off with all the information that was there.

We had six public hearings on these issues in the Senate Judiciary Committee last Congress. The original USA FREEDOM Act was introduced by Senator LEE and me and Congressman JIM SENSENBRENNER in the other body.

We all knew section 215, the roving wiretap authority, and “lone wolf” provision, would expire June 1, 2015. That is why we started working to change it. We are also well aware of the Second Circuit Court of Appeals decision that made part of the program illegal.

I think what we have in the USA FREEDOM Act is a carefully crafted bill by both Republicans and Democrats in the House and the Senate. That is why it passed 338 to 88 in the House. If we start amending it, we don't know how much longer it is going to take and we end up with no protections. I think that is not a choice we want to make.

On Sunday night, with only a few hours before the sunset of section 215 and the other two expiring FISA authorities, Republican leadership in the Senate finally agreed to begin debate on the USA FREEDOM Act.

For nearly 2 years, I have been working on a bipartisan basis with members in both the Senate and the House to address these matters. As chairman of the Senate Judiciary Committee last Congress, I convened six public hearings to examine the NSA's bulk collection program and consider reforms to

section 215 and other surveillance authorities.

In October 2013, I introduced the original USA FREEDOM Act with Congressman JIM SENSENBRENNER, Senator LEE, and others. We introduced an updated version of the USA FREEDOM Act in 2014 and pushed for the Senate to pass that bill last November, months before Sunday's expiration date.

The American people were demanding meaningful reforms, but the intelligence community also needed operational certainty.

We all knew that section 215, the roving wiretap authority, and the lone wolf provision would expire on June 1. That is why I started working months ago with Members of Congress from both parties and both Chambers to forge a compromise that protects both Americans' privacy and our national security.

We were able to reach agreement on a bill that certainly does not go as far as I would like, but that definitively ends the NSA's bulk collection of phone records, improves transparency and accountability, and includes other important reforms. Our bill—the USA FREEDOM Act of 2015—is a carefully crafted bill that has now earned the support of the intelligence community, privacy and civil liberties groups, librarians, the tech industry, and a bipartisan super-majority of the Republican-led House of Representatives. Our bill represents significant progress toward real surveillance reform.

Unfortunately, the Republican leadership in the Senate has tried to block this progress at every turn. They blocked the Senate from debating the USA FREEDOM Act last November. They again blocked the Senate from debating the bill 2 weeks ago, despite knowing full well that failure to swiftly consider the House-passed bill would lead to expiration of these critical surveillance authorities. This brinkmanship is not a responsible way to govern.

The expiration of the PATRIOT Act provisions on Sunday night was entirely avoidable, and the unfortunate consequence of a manufactured crisis. The Senate must now act responsibly and swiftly. It is time to pass the USA FREEDOM Act, which would restore the expired provisions and add much needed improvements and reforms.

I hope that we will invoke cloture and then quickly dispense with any germane amendments so that we can move to passage of the bill. The House passed the USA FREEDOM Act almost 3 weeks ago by an overwhelming 338 to 88 vote.

Senator LEE and I sought an open amendment process in the Senate, but we were blocked. Now, we simply do not have any time to spare. The Senate must pass this bill without any amendments so that the President can sign it into law immediately and restore these expired provisions today.

A vote for any amendment is a vote to prolong the expiration of the sur-

veillance authorities that ended on Sunday. If the Senate changes the underlying bill in any way, it must go back to the House for its consideration, and there are no guarantees that it will pass the new bill.

In fact, Chairman GOODLATTE of the House Judiciary Committee, Ranking Member CONYERS, Congressman SENSENBRENNER, and Congressman NADLER warned that “[t]he House is not likely to accept the changes proposed by Senator MCCONNELL. Section 215 has already expired. These amendments will likely make that sunset permanent.”

Let us have no more unnecessary delay or political brinkmanship. It is time to do our jobs for the American people—to protect their privacy and maintain our national security. Now is not the time to seek unnecessary changes to this bill. If Senators believe that the Senate should consider some of these changes, we can consider them after we pass the USA FREEDOM Act.

I urge Senators to vote for cloture because we need to move forward. We cannot afford to waste any more time. The USA FREEDOM Act includes important reforms, and we need to give the intelligence community the tools they need to keep us safe. That means we must pass the USA FREEDOM Act without change and without any more unnecessary delay.

Mr. President, I yield to the Senator from Utah.

Mr. LEE. Mr. President, I first want to thank my friend and colleague, the senior Senator from Vermont, for his tireless work on this issue. Senator LEAHY and I, along with Senator HEINRICH and so many others who are participating in this process, have worked together to develop a legislative strategy that is both bicameral and bipartisan. This legislation we are about to vote on today was passed with an overwhelming supermajority in the House of Representatives—338 votes to 88 votes. This is a testament to the fact that in so many instances there is more that unites us than divides us in today's political environment. This is an example of the type of win-win situation we can develop.

This bill protects America's national security, and it does so in a way that is respectful of the privacy interests and both the letter and the spirit of the Fourth Amendment.

The American people understand intuitively that it is none of the government's business whom they are calling, when they are calling them, who calls them, and how long their calls last. The American people intuitively understand what graduate researchers have confirmed, which is that this type of calling data—even just the data itself, not anything having to do with recorded conversations, just the data—reveals a lot about an individual, about his or her political preferences, religious views, marital status, the number of children the person may have, and all kinds of interests that are none of the government's business.

Moreover, the way this data is collected is inconsistent with the way our government is supposed to operate. Rather than going out and demonstrating some type of connection between the data set requested and a particular investigation, under the current system the government simply issues orders saying: Send us all of your data. Send us all your data on all calls made by all of your customers. We want all of it. If that means 300 million phone numbers, we want all of that regardless of its connection to any suspected terrorist operation.

That is wrong. Our bill would change that, and it would change it quite simply by requiring the government to request information connected to a particular phone number—a phone number that is itself suspected of being involved in some type of terrorist activity.

This bill represents a good compromise. This bill represents reason. This bill would protect America's national security while also protecting privacy. This bill, in so doing, recognizes that our privacy is not and ought not ever be deemed to be in conflict with our security. Our privacy is, in fact, part of our security.

We are, unfortunately, considering this bill with too little time left. In effect, we are considering this bill after the PATRIOT Act provisions at issue have expired. This is unfortunate. It was unnecessary, and it represents a longstanding bipartisan problem within the Senate—a problem pursuant to which we establish cliffs. We establish these artificially designed deadlines.

We have known about this particular deadline for 4 years. For 4 years, we knew these provisions were going to expire. We should have taken up these provisions far in advance of now. Many of us tried. We did so unsuccessfully. Senator LEAHY and I and others have been working on this legislation for years. We have been ready, willing, eager, and anxious to do so, and we haven't been able to do so until very recently. Now, because of the fact that these provisions have expired, it is incumbent upon us to move these things forward in all deliberate speed.

Whatever the outcome of this vote and of those votes which will follow later today, the American people deserve better than this. Vital national security programs that touch on our fundamental civil liberties deserve a full, open, honest, and unrushed debate. This should not be subject to cynical, government-by-cliff brinkmanship. If Members of Congress—particularly Republican Members of Congress—ever want to improve their standing among the American people, then we must abandon this habit of political gamesmanship.

Finally, it is time for us to pass this bill—this bill which passed overwhelmingly in the House of Representatives, this bill which carefully balances important interests the American people care deeply about.

I urge my colleagues to support this legislation.

Mr. President, this week the Senate will consider the USA FREEDOM Act of 2015, H.R. 2048. I am proud to have introduced the Senate companion to this bill, S. 1123, along with Senator PATRICK LEAHY, ranking member of the Senate Judiciary Committee. We have worked closely with our partners in the House of Representatives, House Judiciary Committee Chairman BOB GOODLATTE, Ranking Member JOHN CONYERS, and Congressmen JIM SENSENBRENNER and JERROLD NADLER.

Since revelations in June 2013 that the National Security Agency was secretly and indiscriminately collecting Americans' telephone records, Senator LEAHY and I have worked together on legislation to end this mass surveillance program and to enact greater transparency and oversight over the government's intelligence gathering operations. The USA FREEDOM Act of 2015 is the result of that 2-year collaboration, and it contains strong reforms. Most importantly, it would definitively end the NSA's bulk collection of Americans' telephone metadata and ensure that the Foreign Intelligence Surveillance Act pen register statute and the national security letter statutes cannot be used to justify bulk collection.

On May 13, 2015, the House passed the USA FREEDOM Act by an overwhelming, bipartisan 338-to-88 vote. More than 80 percent of House Republicans and 75 percent of House Democrats voted for the bill, including the chairmen and ranking members of the House Judiciary and Intelligence Committees, as well as the leadership of both parties.

The resounding vote in the House is a direct result of the commonsense and meaningful reforms contained in the bill. It is also a testament to the will of the American people, who have been unequivocal in their demand for reform and their demand that the NSA stop the indiscriminate collection of their private records.

As our colleagues in the Senate consider the USA FREEDOM Act of 2015, Senator LEAHY and I want to detail the extensive legislative process undertaken to develop this bill and provide additional clarity on the bill's provisions.

Senator LEAHY, I know that you have a long history of pushing for meaningful oversight and transparency of our government's intelligence gathering operations.

Mr. LEAHY. I thank the Senator from Utah for his advocacy on behalf of Americans' privacy rights and for his dedicated efforts to end the NSA's illegal program.

In June 2013, Americans learned for the first time that section 215 of the USA PATRIOT Act has for years been secretly interpreted to authorize the collection of Americans' phone records on an unprecedented scale. And they learned that the NSA has engaged in repeated, substantial legal violations

in its implementation of section 215 and other surveillance authorities.

Since that time, Congress and the American public have been engaged in an important debate about the breadth of government surveillance powers and the legal rationale used to authorize the collection of Americans' data. Under my chairmanship last Congress, the Senate Judiciary Committee held six open and public hearings that sharpened the committee's thinking and furthered the public dialogue on these important issues. Senator LEE, Congressman JIM SENSENBRENNER, Congressman JOHN CONYERS, and I introduced bicameral, bipartisan legislation, the USA FREEDOM Act of 2013, S. 1599/H.R. 3361, on October 29, 2013, to end bulk collection and reform our surveillance laws. The President announced his support for ending the bulk collection of Americans' phone records in March 2014. The House of Representatives passed a new version of the USA FREEDOM Act in May 2014, and after lengthy discussions with the executive branch, the technology industry, privacy advocates, and other stakeholders, Senator LEE and I introduced the USA FREEDOM Act of 2014, S. 2685, on July 29, 2014. On November 18, 2014, the full Senate failed to invoke cloture on the motion to proceed to the USA FREEDOM Act of 2014, by a vote of 58 to 42.

Despite falling two votes shy last Congress, Senator LEE and I knew that the May 31, 2015, expiration date was approaching, and we continued to work on a bill to reform these authorities. Senator LEE, can you explain the process we have undertaken this year?

Mr. LEE. Since November 2014, Senator LEAHY and I have been engaged in conversations with House Judiciary Committee Chairman GOODLATTE, Ranking Member CONYERS, and Congressmen SENSENBRENNER and NADLER to develop a new version of the USA FREEDOM Act. After extensive negotiations with the administration, intelligence community officials, privacy and civil liberties groups, the technology industry, and other stakeholders, we introduced the USA FREEDOM Act of 2015, S. 1123/H.R. 2048, on April 28, 2015.

Of course, the USA FREEDOM Act of 2015 was not introduced in a vacuum. Nearly 2 years ago, on June 5, 2013, the Guardian newspaper published an article and posted a classified FISA Court order revealing that the U.S. Government had been engaging in the bulk collection of Americans' telephone metadata. One day later, on June 6, 2013, the Washington Post published an article and posted further classified information about a separate government surveillance program called PRISM involving the collection of the contents of Internet communications. The administration subsequently acknowledged that the NSA's bulk collection of telephone metadata was being conducted pursuant to section 215 of the USA PATRIOT Act. The NSA's

PRISM program to collect the contents of Internet communications of certain overseas targets was being conducted pursuant to section 702 of FISA, which was enacted as part of the FISA Amendments Act.

Once these programs were revealed, then-Chairman LEAHY convened a number of hearings so that the American people could better understand what the NSA was doing.

Senator LEAHY, can you remind us of the Judiciary Committee's activities in the 113th Congress?

Mr. LEAHY. As I mentioned, during the last Congress, the Senate Judiciary Committee held six open, public hearings to examine the legal basis, effectiveness, and impact of these programs on Americans' privacy rights and civil liberties. We heard testimony from a wide range of government officials, legal scholars, technologists, and outside experts as the Committee sought to understand and evaluate the numerous issues raised by these activities.

On July 31, 2013, I chaired the first full Judiciary Committee hearing to examine government surveillance programs with administration officials and outside experts. At the hearing, the NSA Deputy Director confirmed that the NSA's bulk telephony program did not help to thwart dozens of terrorist plots, as some administration officials defending the program had been contending. He confirmed that section 215 was only uniquely valuable in thwarting one terrorist "plot"—the case of Basaaly Moalin, a Somali immigrant who was convicted of material support for sending \$8,500 to al-Shabaab in Somalia.

As a result of continued public debate about the government's surveillance activities, on August 9, 2013, President Obama announced that he was ordering the Director of National Intelligence, DNI, to establish a group of outside experts to review the government's intelligence and communications technologies and provide recommendations on possible reforms to surveillance authorities. He also announced the public release of additional documents, including a Department of Justice white paper outlining the legal justification for the section 215 bulk collection program.

Over the course of the following months, the DNI declassified and released a host of documents related to activities conducted under section 215 of the USA PATRIOT Act and section 702 of FISA. The released documents detailed serious incidents of non-compliance and violations of law in implementing both of these programs. For example, the documents revealed that for several years, the NSA was unlawfully collecting thousands of wholly domestic emails and other electronic communications as part of its section 702 collection. In addition, FISA Court orders relating to the section 215 program revealed significant compliance problems and were highly critical of the NSA's oversight and operation of the program.

On October 2, 2013, I chaired a second full Judiciary Committee hearing on government surveillance authorities. NSA Director Alexander revealed for the first time that the NSA had previously conducted a pilot program to test its capability of handling location data as part of the section 215 phone records program, although he emphasized that it was only a test. The second panel of witnesses at the hearing testified about the government's legal justification for the collection of telephone records under section 215. A technologist and computer scientist provided testimony to illustrate the power of metadata and the blurring distinction between content and metadata in the digital age.

Shortly after that hearing, on October 29, 2013, I joined with Senator LEE, Congressman SENSENBRENNER, and Congressman CONYERS to introduce the bipartisan, bicameral USA FREEDOM Act of 2013 to comprehensively reform a range of surveillance authorities. This legislation served as the basis for many of the reforms Congress is now debating.

On November 13, 2013, Senator FRANKEN chaired a Judiciary Committee subcommittee hearing on legislation that he had introduced, the Surveillance Transparency Act of 2013, components of which were included in the USA FREEDOM Act. Government witnesses testified about executive branch efforts to promote greater transparency of surveillance activities. In addition, several outside witnesses, including representatives from the U.S. technology industry, spoke about the economic harm and damage to American technology companies as a result of revelations of government surveillance activities. These witnesses testified that American businesses stand to lose billions of dollars in the coming years as a result of revelations about U.S. surveillance activities.

On November 18, 2013, the DNI declassified and released a host of documents related to a previously classified program that collected bulk Internet metadata. The documents included a FISA Court opinion authorizing the bulk collection of Internet metadata under the FISA pen register and trap and trace device authority. As with the section 215 telephone metadata program, the declassified documents revealed that the bulk Internet metadata collection program also encountered major compliance problems during its operation. In 2011, the program was ended by the government because it was not meeting operational expectations.

On December 9, 2013, eight leading technology companies—AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo!—wrote an open letter to President Obama and Congress laying out five surveillance reform proposals. The companies called for a prohibition on the bulk collection of Internet data and argued that governments should limit surveillance to

specific, known users for lawful purposes. The companies also urged stronger checks and balances, including an adversarial process at the FISA Court.

On December 11, 2013, the Judiciary Committee held its fourth hearing on these issues. At the hearing, government witnesses discussed the possibility of placing a privacy advocate at the FISA Court, the recently declassified documents about the bulk collection of Internet metadata, and the scope of collection that is permitted under traditional section 215 orders. We learned that the problems with the Internet metadata program were so severe that the FISA Court suspended the program entirely for a period of time before approving its renewal. But then, in 2011, the government ended this Internet metadata program because, as Director Clapper explained, it was no longer meeting “operational expectations.” However, senior government lawyers testified that under the statute, there was no legal impediment to restarting this bulk Internet data collection program. If the executive branch—or a future administration—wanted to do so, it would simply apply for an order from the FISA Court.

On December 18, 2013, the President's Review Group on Intelligence and Communications Technology publicly released its final report, which included 46 recommendations and findings to reform government surveillance activities. The review group members included Richard Clarke, former counterterrorism adviser to Presidents George H.W. Bush, Bill Clinton, and George W. Bush; Michael Morell, former Acting Director of the CIA; Geoffrey Stone, professor at the University of Chicago Law School; Cass Sunstein, Harvard Law School professor and former senior OMB official in the Obama administration; and Peter Swire, a professor at the Georgia Institute of Technology and former adviser to Presidents Obama and Clinton. They concluded that the section 215 phone records program had not been essential to national security, saying: “The information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders.” The review group further stated that “Section 215 has generated relevant information in only a small number of cases, and there has been no instance in which NSA could say with confidence that the outcome would have been different without the section 215 telephony meta-data program.”

This sort of massive surveillance presents significant privacy implications in the digital age, and the review group's report provided valuable insights. The report explained that keeping a record of every phone call an individual has made over the course of several years “can reveal an enormous amount about that individual's private

life.” The report further explained that in the 21st century, revealing private information to third party services “does not reflect a lack of concern for the privacy of the information, but a necessary accommodation to the realities of modern life.” And the report questioned whether we can continue to draw a rational line between communications metadata and content. This is a critically important question given that many of our surveillance laws depend upon the distinction between the two.

The review group also addressed the national security letter, NSL, statutes. Using NSLs, the FBI can obtain detailed information about individuals' communications records, financial transactions, and credit reports without judicial approval. Recipients of NSLs are subject to permanent gag orders. The review group report made a series of important recommendations to change the way national security letters operate. I have been fighting to impose additional safeguards on this controversial authority for years—to limit their use, to ensure that NSL gag orders comply with the First Amendment, and to provide recipients of NSLs with a meaningful opportunity for judicial review.

Following release of the review group's report, the Judiciary Committee then held its fifth hearing on the NSA's programs and called the members of the review group to testify. On January 14, 2014, the members of the review group testified before the Senate Judiciary Committee and explained that in light of changing technology and the creation of more and more data, it recommended transitioning to a system where the government does not hold massive databases of Americans' metadata. Rather, metadata could be held by providers or a third party, and could be searched by the government only with advance judicial approval. The five members of the panel made clear that while we must always consider ongoing threats to national security, policymakers should consider all of the risks associated with intelligence activities: the risk to individual privacy, to free expression and freedom of association, to an open and decentralized Internet, to America's relationships with other nations, to trade and commerce, and to maintaining the public trust.

Following the review group's report, in January 2014, President Obama took an important step to restore American's privacy and civil liberties by embracing the growing consensus that the section 215 phone records program should not continue in its current form. During a speech at the Department of Justice, the President announced that he had directed the intelligence community to develop alternatives to the program and asked the Justice Department to seek advance judicial approval from the FISA Court to query the section 215 phone call database. Additionally, he ordered the

government to limit searches of the section 215 database to two “hops,” instead of three. He also recommended reforms to the secrecy surrounding national security letters.

A January 23, 2014, report by the Privacy and Civil Liberties Oversight Board, PCLOB, added to the growing chorus calling for an end to the government’s dragnet collection of Americans’ phone records. On February 12, 2014, the Judiciary Committee held its sixth public hearing, this time with the members of the PCLOB to explain the conclusions in their report. As with the President’s review group, the PCLOB report likewise determined that the section 215 program has not been effective, saying: “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. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.”

The PCLOB report also provided the public with a detailed constitutional and statutory analysis of this program and concluded that the program “lacks a viable legal foundation under Section 215” and “implicates constitutional concerns under the First and Fourth Amendments.” The PCLOB report further revealed that although the FISA Court first authorized this program in 2006, it did not issue an opinion setting forth a full legal and constitutional analysis of the program until 2013.

In March 2014, after consulting with the intelligence community, President Obama announced that his administration would work with Congress to pass legislation to end the NSA’s section 215 bulk phone records collection program and to transition to a new program in which the data is not held by the government. Ending bulk collection is a key element of what I, Senator LEE, and others have included in the various iterations of the USA FREEDOM Act.

After the President’s announcement, the House of Representatives took action. Senator LEE, would you like to expand on what transpired in the House?

Mr. LEE. On May 5, 2014, House Judiciary Committee Chairman GOODLATTE announced that he had agreed with Representatives SENSENBRENNER and CONYERS on a new version of the USA FREEDOM Act. On May 7, 2014, the House Judiciary Committee voted unanimously to report this revised USA FREEDOM Act. The next day, the House Permanent Select Committee on Intelligence convened a markup to consider the version of the bill reported by the House Judiciary Committee and voted unanimously to report the bill to the full House.

Following action by the House Judiciary and Intelligence Committees, further changes to the text of the reported bill were considered and a substitute amendment to the USA FREEDOM Act

was unveiled on May 20, 2014, when the House Rules Committee adopted a rule for floor consideration. Following the release of the substitute amendment, some concerns were raised that the substitute amendment did not effectively prohibit bulk collection, even though that was clearly its intent. On May 22, 2014, the House of Representatives passed the amended version of the USA FREEDOM Act by a vote of 303 to 121. Many of those who voted no on the bill did so because they were concerned that its reforms did not go far enough.

After the House passed its version of the USA FREEDOM Act, Senator LEAHY and I worked hard to build on that legislation.

Senator LEAHY, can you talk about what led to the USA FREEDOM Act of 2014, S. 2685?

Mr. LEAHY. Immediately following passage of the House version in May 2014, Senator LEE and I began working to address concerns that the text of the House bill, although clearly intended to end bulk collection, did not do so effectively. We spent several months in discussions with the intelligence community and a wide range of stakeholders, including other Senators, privacy and civil liberties groups, and the U.S. technology industry, to build on the framework established by the House-passed bill.

Those negotiations led to the introduction of the USA FREEDOM Act of 2014, S. 2685, on July 29, 2014. More than 50 organizations, interest groups, trade associations, and technology companies from across the political spectrum publicly endorsed the bill. On September 2, 2014, the Attorney General and DNI wrote a letter in support of the USA FREEDOM Act of 2014. The letter noted that the bill preserved the intelligence community’s capabilities while also enhancing privacy and civil liberties and increasing transparency. Likewise, members of the President’s review group wrote a letter to myself and Senator GRASSLEY, explaining that the USA FREEDOM Act of 2014 was consistent with the recommendations contained in their December 2013 report.

On November 12, 2014, Senator REID filed cloture on the motion to proceed to the USA FREEDOM Act of 2014. A few days later, on November 17, 2014, the Obama administration released a Statement of Administration Policy on the USA FREEDOM Act of 2014 strongly supporting passage.

Despite the wide-ranging support for these commonsense reforms, on November 18, 2014, the full Senate failed to invoke cloture on the motion to proceed to the USA FREEDOM Act of 2014, by a vote of 58 to 42. I was extremely disappointed that the Republican leadership in the Senate decided to use a procedural vote to block debate and amendments on such an important piece of legislation.

With the start of the 114th Congress, Senator LEE and I began discussions with the House to develop a new

version of the USA FREEDOM Act. We knew that the June 1, 2015, sunset of several surveillance authorities, including section 215 of the USA PATRIOT Act, would come up fast. For several months, we engaged in conversations with House Judiciary Committee Chairman GOODLATTE, Representative SENSENBRENNER, and House Judiciary Committee Ranking Member CONYERS, as well as officials from the administration, intelligence community, privacy and civil liberties groups, the technology industry, and other stakeholders on a path forward. Those extensive deliberations produced another set of bipartisan, bicameral surveillance reforms to end the bulk collection of Americans’ phone records and amend other surveillance laws.

On April 28, 2015, Senator LEE and I introduced the USA FREEDOM Act of 2015, S. 1123, and Representatives SENSENBRENNER, GOODLATTE, CONYERS, NADLER, and others in the House introduced the House companion, H.R. 2048. The Senate version of the bill was originally cosponsored by Senators HELLER, DURBIN, CRUZ, FRANKEN, MURKOWSKI, BLUMENTHAL, DAINES, and SCHUMER. It has also received the support of the administration, privacy groups, and the technology industry.

On May 11, 2015, the Attorney General and Director of National Intelligence wrote a letter in strong support of the USA FREEDOM Act of 2015. The letter notes that the legislation “is a reasonable compromise that preserves vital national security authorities, enhances privacy and civil liberties and codifies requirements for increased transparency.” The Obama administration also issued a Statement of Administration Policy on May 12, 2015, in strong support of the USA FREEDOM Act of 2015.

In early May, as the House and Senate were preparing to consider the USA FREEDOM Act of 2015, the Second Circuit issued a decision confirming what we knew all along.

Senator LEE?

Mr. LEE. It did. On May 7, 2015, a three-judge panel from the U.S. Court of Appeals for the Second Circuit unanimously concluded that the NSA’s bulk collection program is illegal. The court held that section 215 of the USA PATRIOT Act does not authorize bulk collection of Americans’ private records and roundly rejected the argument that all of our phone records can be “relevant” to any particular authorized investigation.

In *ACLU v. Clapper*, the Second Circuit provided a detailed statutory and legal analysis of section 215 and the bulk collection program. It stated that the government’s “expansive” interpretation of “relevance” in the context of Section 215 “is unprecedented and unwarranted.” The court further stated:

The interpretation that the government asks us to adopt defies any limiting principle. The same rationale that it proffers for the “relevance” of telephone metadata cannot be cabined to such data, and applies

equally well to other sets of records. If the government is correct, it could use §215 to collect and store in bulk any other existing metadata available anywhere in the private sector, including metadata associated with financial records, medical records, and electronic communications (including e-mail and social media information) relating to all Americans.

Such expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans.

The court also rejected the government's attempt to compare the NSA's section 215 orders for bulk collection of telephony metadata to grand jury subpoenas, citing the expansive scope and breadth of the information requested. The court correctly noted:

The sheer volume of information sought is staggering; while search warrants and subpoenas for business records may encompass large volumes of paper documents or electronic data, the most expansive of such evidentiary demands are dwarfed by the volume of records obtained pursuant to the orders in question here. . . . The government can point to no grand jury subpoena that is remotely comparable to the real-time data collection undertaken under this program.

While the Second Circuit held that the NSA bulk collection program was illegal, it did not issue a preliminary injunction to enjoin the program. The Second Circuit remanded the case with instructions for the district court to consider whether an injunction was appropriate in light of the upcoming June 1, 2015, expiration of section 215 and ongoing efforts in Congress to enact legislation before the sunset.

As both Senator LEAHY and I have mentioned, the USA FREEDOM Act of 2015 passed the House of Representatives less than a week later by an overwhelming and bipartisan vote of 338 to 88.

In order to aid Senators' consideration of this bill, and to prevent misinterpretations of Congress's intent, we want to state clearly that we agree with the section-by-section analysis contained in House Report 114-109, "UNITING AND STRENGTHENING AMERICA BY FULFILLING RIGHTS AND ENSURING EFFECTIVE DISCIPLINE OVER MONITORING ACT OF 2015," to accompany H.R. 2048 as adopted by the House Judiciary Committee on May 8, 2015. There are a few additional matters that Senator LEAHY and I should take an opportunity to clarify. Senator LEAHY?

Mr. LEAHY. The core of this legislation is its prohibition on the bulk collection of records under section 215 of the USA PATRIOT Act, the FISA pen register and trap-and-trace device statute, and the national security letter statutes. Though there are some minor wording changes, these provisions are substantively identical to the version in the USA FREEDOM Act of 2014. For section 215 and the FISA pen register and trap and trace device statutes, under the bill the government must use a "specific selection term" to limit its collection and demonstrate reasonable grounds to believe that the records

sought are relevant to the underlying investigation, which cannot be a threat assessment. These requirements are independent of each other, and both must be satisfied.

The USA FREEDOM Act of 2015 is being considered with full knowledge of the Second Circuit's decision in *ACLU v. Clapper* and its interpretation of the term "relevant," which rejects the prior reading of the Foreign Intelligence Surveillance Court. According to the Second Circuit, information that the government seeks to obtain must be presently relevant to the specific underlying investigation. The Second Circuit correctly noted:

"Relevance" does not exist in the abstract; something is "relevant" or not in relation to a particular subject. Thus, an item relevant to a grand jury investigation may not be relevant at trial. In keeping with this usage, §215 does not permit an investigative demand for any information relevant to fighting the war on terror, or anything relevant to whatever the government might want to know. It permits demands for documents "relevant to an authorized investigation." The government has not attempted to identify to what particular "authorized investigation" the bulk metadata of virtually all Americans' phone calls are relevant. Throughout its briefing, the government refers to the records collected under the telephone metadata program as relevant to "counterterrorism investigations," without identifying any specific investigations to which such bulk collection is relevant. . . . Put another way, the government effectively argues that there is only one enormous "anti-terrorism" investigation, and that any records that might ever be of use in developing any aspect of that investigation are relevant to the overall counterterrorism effort. The government's approach essentially reads the "authorized investigation" language out of the statute. Indeed, the government's information-gathering under the telephone metadata program is inconsistent with the very concept of an "investigation."

The USA FREEDOM Act of 2015 reauthorizes section 215, but it does so in light of the understanding of how the Second Circuit interprets "relevance."

Mr. LEE. I agree that the new requirement for a "specific selection term" in the USA FREEDOM Act of 2015 is separate from the requirement of "relevance." I would like to clarify one last point. Section 104 of the bill authorizes the FISA Court to impose additional, particularized minimization procedures for information obtained under section 501 of FISA. That section provides that the FISA Court may impose additional procedures related to "the destruction of information within a reasonable time period." That provision therefore provides authority for the FISA Court to specify a time period within which the government must destroy information.

Mr. LEAHY. I have been proud to work with Senator LEE for nearly 2 years to develop the legislation that we have been discussing. It has involved many hours of hard work over many months. The result is a solid bill with a set of commonsense reforms that has overwhelming support. The Senate should pass it today.

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 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, John Cornyn, Ron Johnson, Dean Heller, Steve Daines, Cory Gardner, Johnny Isakson, Richard Burr, Tim Scott, James Lankford, Jeff Flake, Mike Lee, Lisa Murkowski, John Barrasso, Thom Tillis, Chuck Grassley, Richard C. Shelby.

The PRESIDING OFFICER. Pursuant to rule XXII, the Chair now directs the clerk to call the roll to ascertain the presence of a quorum.

Mr. LEAHY. Mr. President, I ask unanimous consent that we waive the mandatory quorum.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

The question is, Is it the sense of the Senate that debate on 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?

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 Missouri (Mr. BLUNT) and the Senator from South Carolina (Mr. GRAHAM).

Mr. DURBIN. I announce that the Senator from Virginia (Mr. WARNER) is necessarily absent.

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

The yeas and nays resulted—yeas 83, nays 14, as follows:

[Rollcall Vote No. 197 Leg.]

YEAS—83

Alexander	Cardin	Donnelly
Ayotte	Carper	Durbin
Baldwin	Casey	Feinstein
Bennet	Cassidy	Fischer
Blumenthal	Coats	Flake
Booker	Cochran	Franken
Boozman	Collins	Gardner
Boxer	Coons	Gillibrand
Brown	Corker	Grassley
Burr	Cornyn	Hatch
Cantwell	Cruz	Heinrich
Capito	Daines	Heitkamp

Heller	McCaskill	Schatz
Hirono	McConnell	Schumer
Hoeben	Menendez	Scott
Inhofe	Merkley	Shaheen
Isakson	Mikulski	Stabenow
Johnson	Murkowski	Sullivan
Kaine	Murphy	Tester
King	Murray	Thune
Kirk	Nelson	Tillis
Klobuchar	Perdue	Toomey
Lankford	Peters	Vitter
Leahy	Portman	Warren
Lee	Reed	Whitehouse
Manchin	Reid	Wicker
Markey	Rounds	Wyden
McCain	Sasse	

NAYS—14

Barrasso	Moran	Sanders
Cotton	Paul	Sessions
Crapo	Risch	Shelby
Enzi	Roberts	Udall
Ernst	Rubio	

NOT VOTING—3

Blunt	Graham	Warner
-------	--------	--------

The PRESIDING OFFICER. On this vote, the yeas are 83, the nays are 14.

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

The majority whip.

Mr. CORNYN. Madam President, the Senate will hold a series of votes this afternoon on the underlying bill, and I think it is important for all of us to understand exactly what those amendments will do.

The underlying House bill makes some changes in the way the National Security Agency operates and uses what the Supreme Court of the United States has held is not private information—in other words, the time, duration, and number involved in a telephone call that is contained in a typical telephone bill.

The Supreme Court of the United States has said there is no right of privacy in that information. As the Senate knows, what the House bill does is it leaves these phone records in the possession of the telephone company. Then, over a period of 6 months, the National Security Agency is supposed to come up with a means of querying those records in the possession of the various phone companies.

Some, like me, have wondered why it is that we are trying to fix a system that is not broken, because there is absolutely no documented record of any abuse of this information as it is currently retained by the NSA. The way it is used is to help the intelligence community discover people who have communicated with known or suspected terrorists abroad in a way that will help to provide an additional piece of data that will hopefully help them prevent terrorist attacks from occurring on our home soil.

The FBI Director has said that in the 56 field offices in the United States, every single one of these field offices has an open inquiry with regard to potential homegrown terrorist attacks.

As I mentioned before, in Garland, TX, just a few weeks ago, two men traveled from Phoenix, AZ, and obtained full-body armor and automatic weapons and were prepared to wreak havoc and murder innocent people in

Garland, TX, because they were exercising their First Amendment rights and were displaying cartoons that these two jihadists felt insulted the Prophet Muhammad.

Thanks to the good police work of a Garland police officer, both of those people were taken out of action before they could kill anybody there at that site. But why in the world would we want to take away from our intelligence authorities the ability to detect whether individuals, such as these two jihadists from Phoenix who traveled to Garland, had been communicating with known terrorist telephone numbers in Syria or anywhere else in the world? These are foreign telephone numbers that are matched up and provide an essential link and, really, a tripwire for the intelligence community.

What the amendments that we will vote on this afternoon would do is to slow the transition from NSA storage to the telephone company stewardship from the 6 months prescribed in the underlying bill. For those who believe that the underlying bill is the correct policy, I do not know why they would object to a little bit of extra time so we can make sure that this is going to work as intended.

Indeed, the second amendment does relate specifically to that. It would require a certification by the Director of National Intelligence that the software is actually in place that will allow the National Security Agency to query the phone records in the possession of the telephone companies.

Another amendment would provide that the Foreign Intelligence Surveillance Court, which is a group of experienced Federal judges who review the requests from the FBI and other law enforcement authorities, would be able to query these telephone records. It would establish a panel of experts, so to speak, to argue against the government's case in front of the Foreign Intelligence Surveillance Court. As somebody who used to be a judge for some time, this is a rather strange provision because what it does, essentially, is to put a defense attorney in the grand jury room and create an adversarial process at the early stages of an investigation, which may or may not lead up to an indictment in that case.

The final amendment would require the phone companies to notify Congress if they are going to change their policy for retaining customer records. This is a serious concern because it could well be that some telephone companies will start marketing to potential customers that they will not retain any records, thus eliminating an important tool which helps keep Americans safe and has absolutely zero threat to civil liberties.

There has been so much misrepresentation about what this so-called metadata program has done. I think that is one of the reasons we find ourselves here today. Many who believe the program is useful are reluctant to

even talk about it in public because, as we know, so much of what is done to protect our country is classified. So rather than have a public debate and actually correct the misstatements of fact and the demagoguery that unfortunately attends this subject, many people are simply confused about what exactly is going on and what Congress is doing. But I would just point out that oversight of these programs is absolutely rigorous. It is executive, judicial, and legislative oversight. It is not a matter of trust as to whether these programs work the way they are supposed to; it is actually verified on a regular basis, universally verified.

Also, we have to go before these Federal judges known as a FISA Court—a Foreign Intelligence Surveillance Court—in order to make our case. Unless we can make our case to these judges that there is reason to continue the investigation, they will shut it down.

One of the things I think we have forgotten is that we want to treat intelligence gathering and prevention as we do ordinary law enforcement. What I mean by that is that ordinarily, in the criminal law context, government doesn't get involved in a case unless something bad has already happened. If there has been an explosion or a murder or a bank robbery or something like that, it is after the fact that we try to figure out what happened and then, if we can, to identify the perpetrator and to bring them to justice. That satisfies an important need in our society to enforce our criminal law, but that is far different from what our intelligence community is supposed to be doing because they are supposed to be detecting threats and intervening in those ongoing schemes and stopping them before they ultimately occur.

That is the important lesson we learned on 9/11. Unfortunately, it has been so long ago now that many people have simply forgotten or they don't feel as though this is an imminent threat. But when Director Comey says they have open inquiries in all 56 FBI field offices about the potential threat of homegrown terrorists, I take that very seriously. I believe it is absolutely reckless for us to take any unnecessary chances.

There are some who say this underlying bill is important because instead of the National Security Agency collecting these telephone numbers, we are going to leave the data with the telephone companies. But none of the people who are going to be querying these records at the phone companies have security clearances. One can just imagine the potential for abuse at the phone companies of these phone records once they receive some sort of request from the government.

We know the current system as run at the National Security Agency is subject to rigorous oversight, as I mentioned. In addition to the executive, judicial, and legislative oversight, we actually have a private and civil liberties

oversight board which makes sure that we strike the right balance. Nobody wants to see the privacy rights of American citizens undermined, but we all are adult enough to know that there has to be a balance and that in order to provide for security and to avoid terrorist attacks such as occurred on 9/11, we are going to have to take some actions to reach the right balance, and I believe the current law does that.

Unfortunately, we have a traitor such as Edward Snowden who selectively leaked certain portions of this program, and it has created an uproar. I think that unfortunately, as a result of his leaks and the ensuing political environment after that, America is at greater risk, and that is a terrible shame.

So I think it is reckless to take a chance. We have been fortunate that there have been no terrorist attacks on our homeland since 9/11. Well, I take that back. Five years ago, at Fort Hood, MAJ Nidal Hasan killed 13 people and injured 30-something more. Of course, we know now that he had been in constant communication over the Internet with Anwar al-Awlaki, who subsequently was killed in a drone strike—even though he was an American citizen—overseas. He was overseas because he was recruiting people to Islamic extremism, including Nidal Hasan, who killed 13 people at Fort Hood 5 years ago.

It is simply a fact that the Fourth Amendment of the U.S. Constitution involving searches and seizures doesn't apply to foreign terrorists; it applies to Americans. Under the procedures used under current law, all requests for additional information are subject to Federal court supervision and permission.

So we will vote on a number of amendments this afternoon. I can tell my colleagues, after talking to a number of our colleagues, many of them have said they don't really have any disagreement over the content or the policy of these amendments. Actually, these amendments are designed to try to strengthen the underlying House bill.

We all understand that the House is going to prevail in the basic structure of the underlying piece of legislation, but since when did the U.S. Senate outsource its decisionmaking to the other body across the Capitol? We have a bicameral legislature—a Senate and a House—for a reason. We know we make better decisions when we have consultation between the two branches of the legislature—not capitulation but consultation. The Senate should not be a rubberstamp for the House or vice versa.

I have heard some of our colleagues say that if the Senate were to change a period or a comma or a dash in the underlying legislation, it would be a poison pill, that the House would reject it and we would have nothing to show for our efforts. But I have great faith that

if the Senate will do its job and vote to pass these underlying amendments and strengthen this underlying bill, the House will take up the bill and vote on it and it will pass. So if my colleagues feel as though these amendments would actually strengthen the underlying House bill and represent good policy, why in the world would they vote against these amendments because of some fantasy that the House will simply reject any changes at all? Why would they essentially capitulate any of their prerogatives as U.S. Senators to represent their constituents in this body? We all know we make better decisions in consultation with other people.

Certainly I think it is true that the House's bill is not holy writ. It is not something we have to accept in its entirety without any changes. I think where the policy debate should go would be to embrace these amendments and to say that we understand the House wants to change the current custody policy of these phone records and leave them with the phone company, but we sure need to know the new system will actually work. Doesn't that make sense? That is why the certification from the Director of National Intelligence is so important. It makes sense to provide a little bit more time—from 6 months to a year—in order to make sure this transition goes smoothly.

I know no Member of the Senate and no Member of the House and no American wants to look back on our hasty treatment of this underlying legislation and say: If we were just a little more careful, if we had just taken a little bit more time, if we had just been a little more thoughtful, a little more deliberative, and talked about the facts as they are and not some misrepresentation of the facts, we could have actually prevented a terrorist attack on our home soil.

Unfortunately, by increasing the risk to the American people, as I believe this underlying legislation will do, we may not find out about that until it is too late. I hope and pray that is not the case, but why should we take the risk to the homeland? Why should we risk anyone being injured or potentially killed as a result of a homegrown terrorist attack on our own soil because we have simply blinded ourselves in a significant way to the risks? Not that this is a panacea, not that this is some litmus test, but it is one essential piece of information that will help law enforcement make the case to not just prosecute crimes after they occur but to prevent them from occurring in the first place through the good and sound use of constitutional intelligence gathering in a way that respects the privacy of all Americans but lives up to our first and foremost responsibility, and that is to keep the American people safe.

Madam President, I yield to the distinguished ranking member.

The PRESIDING OFFICER. The Senator from Vermont.

Mr. LEAHY. Madam President, nobody disputes that we all want to keep America safe. We all agree on that. We also want to make sure that we keep Americans free and that their constitutional freedoms are protected. None of us would think that we were making the country safer if we were to try to pass a law that said law enforcement or anybody else can walk into our homes at any time they want and go through any files we have, follow us anywhere they wanted just on a whim. We would be totally opposed to that. But some would say that in the aftermath of 9/11, in some of the aspects of the PATRIOT Act, we did just that.

Congressman Armey, who was the Republican leader, the majority leader of the House at the time—a very conservative Republican—he and I joined together after consultation to put into the PATRIOT Act sunset provisions which would require us to have the debate we are having right now.

We talk about consultation. The fact is that there have been hours and days and weeks and months of consultation between the House and the Senate on the USA FREEDOM Act. We had a bill before us last year that was filibustered. It still got 58 votes. That was done in consultation with the House. The majority leader of the House has already said—the Republican leader—he has warned the Senate not to move ahead with planned changes to the House bill because it could bring real challenges in getting the USA FREEDOM Act passed through the House again.

The fact is that we have had so much consultation. Senator LEE, I, Republicans and Democrats have met continuously for months—even a year—with House Republicans and House Democrats to get the bill that is before us now. That is probably why it passed by such a lopsided margin in the House of Representatives.

My distinguished friend from Texas says these are minor changes. Well, actually, they are not. One would weaken the FISA Court amicus authority. We know that for years the FISA Court secretly misinterpreted section 215. As a result, after the program leak, that is the only time the FISA Court finally heard the government's argument. Before that, they only heard the government. Once a legal reason justifying this program became public, challenges were brought, and the Second Circuit last month ruled unanimously that the program was unlawful.

Having amicus in there is not having a defense attorney in a grand jury room at all. Amicus on questions of law can be invited by the court to step in. This could be a relatively rare case, completely in the discretion of the court. It is hard to talk about weakening that further, especially when we are talking about a secret court.

I oppose the amendment to extend the current bulk collection program in place for a full year. We have a 180-day transition period. And the Director of

the NSA said: "We are aware of no technical or security reason why this cannot be tested and brought online within the 180-day period." I think the NSA Director is as knowledgeable about this subject as anybody in this Chamber, and he says we can go forward with it.

I think all of these amendments that are talked about would simply delay passing an excellent piece of legislation, one that has been worked on by Republicans and Democrats for months and even years. Let's pass it today.

We hear about stopping terrorism attacks. We all want to do that. But I remember some of the statements made by a former NSA Director that this had stopped 54 terrorist attacks. When he was pressed on that claim, it came out that the bulk collection program was only important after the fact in one case—and that was not a terrorist attack.

We also know that 9/11 could have been avoided. The evidence was there. The information was there. But the dots had not been connected. Everybody was frantically taking information they already had—recordings they already had after 9/11—and saying: We ought to get around to translating what is in these things. We know that in Minnesota, the FBI warned that people were taking flight lessons and there was no good reason. That warning was ignored. They basically were told: We know better.

I remember the day or so after the attack, at FBI Headquarters, people were calling in with information from different field offices. Somebody would write it down and would hand it to somebody else who would rewrite it and hand it to somebody else who would put it in a file. They would charter planes to bring photographs around to different places so our offices could see them. And I said: Well, why don't we just email the photographs? They would say: Well, we don't have the ability to do that. I said: Well, my 11-year-old neighbor could do it for you if that would help.

The fact of the matter is we had the information prior to our own new laws, and it didn't make us safer—any more safer than when we voted for \$2 to \$3 trillion to go into Iraq because, as the Vice President and others were saying, they were about to attack us with nuclear weapons, and they were implying they were involved in 9/11.

Mr. WYDEN. Will the distinguished ranking member yield?

Mr. LEAHY. Yes.

Mr. WYDEN. I think the ranking member has made a number of very important points here.

The fact of the matter is that we are all here because the majority leader wasn't able to defeat the surveillance reform. So instead, he has chosen to introduce amendments designed to water it down. I am disappointed by this. I will oppose all of these amendments, and I want to have a colloquy briefly with the ranking minority member.

The ranking minority member and our colleague from Connecticut, Senator BLUMENTHAL, have done very good reform work with respect to the FISA Court. In particular, what the distinguished Senator from Vermont has done, with the help of the Senator from Connecticut, is to bring some very important sunshine and transparency to the court. As my two colleagues have pointed out on the Judiciary Committee, we really meet on the major questions—not all of them, as the Senator from Vermont has just said—but what is really needed is to make sure that both sides get a chance to be heard, not just the government side.

So what troubles me—and I am interested in the reaction of my colleague from Vermont, and I want to praise him and my colleague from Connecticut—is that it seems to me that what the Senate majority leader wants to do is basically to take us back to the days of secret law.

What is important, as we get into this, and particularly with this amendment, is that there is a difference between secret operations and secret law. Operations always have to be kept secret.

I see my friend Chairman BURR here. We serve on the Intelligence Committee together. The two of us feel so strongly about making sure secret operations are kept secret because otherwise Americans are going to die. We can't have secret operations played all hither and yon in the public square.

But the law always ought to be public. As Senator LEAHY has pointed out for some time—and I warned about it here on the floor—what we would see is, if you live in Connecticut or Vermont, the PATRIOT Act talked about collecting information relevant to investigation. Nobody thought that meant millions and millions of records on law-abiding people. That decision was made in secret. It was made without the reforms advocated by the Senator from Connecticut and the Senator from Vermont.

So I would be interested in my colleague from Vermont's reaction to the majority leader's amendment to scale back your very constructive reforms on the FISA Court. And my sense is that what the majority leader's approach would do would take us back to the days of secret law. I think that is a mistake, and I would be curious about the reaction of my colleague from Vermont on this.

Mr. LEAHY. I would say to my friend from Oregon that the American people want to know how the laws are being interpreted. They want to know what the courts are doing.

As to secret operations, of course, you have had briefings on those. I have had briefings on those. I have been in places I will not name here. They are places overseas where I was there in the operations center as operations were taking place and being briefed on what they did, where they got the information, and what they were going

to do next. Of course, none of that you want to be reading in the press or seeing in real time.

But I also know that when we are dealing with Americans and with their lives and with their sense of privacy, we have to protect them. The USA FREEDOM Act makes very simple changes to the FISA court. The bill provides the FISA Court with the authority to designate individuals who have security clearances to be able to serve as an amicus or a friend of the court. It is triggered in only relatively rare cases involving a novel or significant issue of law, and the decision of appointment is left entirely up to the court. That is about as narrowly drawn as you can get. But I think we have to have this ability to know what the court is doing because we have known for years that the FISA Court secretly misinterpreted Section 215 to allow for the dragnet collection of Americans' phone records.

I would be happy to yield to the Senator from Connecticut, who has worked so hard on this and is a former attorney general of his own State.

My own experience in getting search warrants for phone records or anything else as a prosecutor—and I realize it is not of the complexity of what we have today, but I realize we had to follow the law—is that, ultimately, that protects us more than anything else. I do not want this administration or any other administration to have the ability just to go anywhere they want. I am not encouraged by those who say this is so carefully maintained. We were given information earlier that just a small number of people can have access to those records. I guess it is one less since Edward Snowden walked out the door with all of it.

I will yield to the Senator from Connecticut if he would like to speak on this subject.

The Senator from Oregon has been such a strong and passionate leader on this, and I know from what I hear from the people of my State and when I am down in his State that people want us to be safe, but they also want their privacy protected.

The PRESIDING OFFICER (Mr. FLAKE). The Senator from Connecticut. Mr. BLUMENTHAL. I thank the Chair.

Mr. President, I am very grateful for the opportunity to follow my distinguished colleague from Vermont and to emphasize some of the points that he has just made. But first let me thank Senator WYDEN for his leadership and his courage on this issue of foreign intelligence surveillance reform. He has helped to lead this effort, long before I was in the Senate, in favor of more transparency and accountability. Those are among the overarching objectives here.

My colleague from Vermont, who shares with me a background as a prosecutor, rightly makes a point that warrants and other means of surveillance when prosecutors seek them are sought

ultimately from judges. I want to speak to some of the myths and misconceptions here that endanger this key reform.

Our colleague from Texas, whom I greatly respect, has argued that the FISA Court is like a grand jury. In fact, he has said that an amicus should not be appointed, in effect, to intervene with a body that is like a grand jury. Well, the Foreign Intelligence Surveillance Court is not a grand jury, as my colleague from Oregon has said very well. The FISA Court makes law. It interprets the law in ways that are binding as legal precedents. Far from being like a grand jury, as a truly investigative tool of the court, the Foreign Intelligence Surveillance Court is a court. In fact, it is composed of article III judges who do as they do on their own district courts or appellate courts; that is, they interpret law and thereby, in effect, make law.

To keep that law secret is a disservice to the American people and to our legal system. To have only one side represented skews and, in effect, impedes the operations of that court because we know that judges make better decisions when they hear both sides and rights are better protected. Even so, the FISA Court needs to hear from that amicus panel only when it chooses to do so, ultimately.

It has the discretion under the statute, as it exists now, to decide to appoint an amicus in any particular matter. It is required to appoint an amicus in novel or significant cases unless—and the word “unless” is in the statute—it issues a finding that the appointment is not appropriate. It can make that finding whenever it wishes to do so. So the discretion is for the FISA Court in whether to hear from an amicus, even under the bill that the USA FREEDOM Act is now. It can permit the amicus to address privacy, technology or any other area relevant to the matter before the court—not just constitutional rights. And that leads to the second misinterpretation, if I may say so, in the remarks made by my colleague from Texas.

The bill does not direct an amicus to oppose intelligence activity or to oppose the government's view or position. In fact, it is to enlighten the court. In some instances it may oppose the government, but it is as part of that process of constructively arriving at the correct legal interpretation—not as a kind of knee-jerk reaction to oppose the government.

Again, I stress, a novel or significant issue in the discretion of the court may be addressed by the amicus. What the amendment does is to deprive the amicus or expert panel of the access it needs to facts and law to be the best that it can be in interpreting, arguing, and protecting rights. It, in effect, bars access to past precedents of the court, to briefings from intelligence experts, to facts that may be known to the Department of Justice or intelligence agencies. That hampering and hobbling

of the amicus in no way serves the cause of justice. It in no way serves the cause of intelligent intelligence activities—in fact, it undermines that activity.

It undermines trust and confidence in the court. This court has operated in secret. It has heard arguments in secret. It has issued opinions in secret. It is the kind of court our Founders would have found an anathema to their vision of democracy and freedom. We may need such a court now to authorize surveillance activities that must be kept secret, but we need to strike a balance that protects very precious constitutional rights and liberties.

After all, what does our surveillance and intelligence system protect if not these fundamental values and rights of privacy and liberties that have lasted and served us well because we respect them?

More than a physical structure that we seek to protect through this system, it is those values and rights that are fundamentally paramount and important. So this FISA Court reform goes to the core of the changes—constructive changes that we seek to make. I hope my colleagues will defeat amendment 1451, along with all of the other amendments, because the practical effect of adopting amendments is it further delays implementation of the USA FREEDOM Act at a time when our country may be at risk from the expiration of the PATRIOT Act. We cannot afford for this country—

Mr. WYDEN. Will my colleague yield for a question on that point?

Mr. BLUMENTHAL. I will be happy to yield.

Mr. WYDEN. Because I think, again, my colleague from Connecticut has spoken to what the stakes are here. For the last decade, intelligence officials have been relying on secret interpretations of their authorities that have been very different from the plain reading of public law. The public has seen the consequences of that, and they are angry because the American people know we can have policies that promote both security and liberty.

I would just like to ask a question of my colleague with the respect to what the implications would be of hollowing out the good work you and Senator LEAHY have done with respect to having more transparency and both sides making a case on key questions with respect to the FISA Court. I would like to note that the majority leader's second amendment delays implementation of other important reforms that you all have dealt with.

For example, one question I was asked about at a townhall meeting just this past weekend in Tillamook, OR, where I was, is people were concerned about what would we do to protect our Nation when there was an emergency. You all, in your good work, have, in effect, said you would strengthen the language to make sure that when there was an emergency—government officials already can issue an emergency

authorization to get the business records and you would then seek court approval, and you all strengthen that.

All of you on the Judiciary Committee said: We are going to provide another measure of security for the American people; in other words, we are going to protect their liberty and we are going to strengthen their security. It looks to me like the combination of the majority leader's two amendments scaling back the reforms, the transparency reforms in the FISA Court, and delaying the strengthening of emergency authorities that can protect the American people without jeopardizing their liberty would really roll back the kind of reforms the American people want.

I would be interested in my colleague's reaction to that.

Mr. BLUMENTHAL. I am happy for that very pertinent and important question from my colleague from Oregon. In fact, the majority leader's amendments would not only scale back and roll back the protections for the American people in the event of exigent or urgent situations, they would also undermine the confidence and trust of the American people in this system to protect the homeland.

Delaying these kinds of reforms undermines the goal of protecting our national security as well as preserving our fundamental constitutional rights. Delay is an enemy here. Uncertainty is an adversary. We owe it to the American people not only to restore their trust and confidence and sustain the faith of the American people in the intelligence agencies but also to make it more transparent, where it can be made so without compromising security and increasing accountability.

That is what the FISA Court reforms do. That is why the Director of National Intelligence as well as the Attorney General, the Privacy and Civil Liberties Oversight Board, the President's Review Group, at least two former FISA Court judges, civil rights advocates, and representatives of many of the most informed and able in our intelligence community all support these reforms.

The Director of National Intelligence and the Attorney General said in 2014, “The appointment of an amicus in selected cases as appropriate need not interfere with the important aspects of the FISA process, including the process of ex parte consultation between the court and the government.”

Ex parte communication, in effect, secret conversation or consultation, can continue to go forward under this bill. The amendment would not alter that fact. The amendment simply makes the amicus less effective by depriving that amicus of access to facts and law that are necessary to do its job. So, in my view, these amendments fundamentally undermine the purpose of reforms that a vast bipartisan majority of this body has already approved today. It is an increasingly large margin that has voted for these

reforms, recognizing what I hear from Connecticut, what my colleagues hear in their States; that people want to believe the Foreign Intelligence Surveillance Court is, in fact, operating as a court, hearing both sides, keeping secrets but at the same time increasing public access to facts and laws that are important to them without compromising our national security.

I hope my colleagues will vote to reject these amendments. As the Senator from Oregon has said, adopting them will simply serve to delay reforms that are necessary.

I yield the floor.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Mr. President, there are always two sides of every picture, two sides of every story. I have tremendous affection for Ranking Member LEAHY. We are friends. We look at this issue differently. I have deep respect for Senator BLUMENTHAL, Senator WYDEN.

The fact is I look at history a little bit differently and I look at the future a little bit differently because I think what the American people want to believe is that America is doing everything possible to keep them safe. I think, at the end of the day, that is the single most important issue: Are we doing everything we can to keep America safe?

Now, Senator WYDEN opposes section 215. He talked about changes. He is opposed to section 215. He is a member of the committee. I know exactly where he stands, and I respect it. The fact is that 215 is a very effective program. My colleagues are right. It was not a public program until Eric Snowden, a traitor to the United States, published a lot of information about what the intelligence community does. This was one small piece. Eric Snowden put the lives of Americans and foreigners at risk in what he released.

You cannot put the genie back in the bottle, but you also cannot hide from the fact that this program enabled us to thwart terrorist attacks here and abroad. I quoted the four of them yesterday. This program itself was what we were able to use post the Boston Marathon bombing to figure out whether the Tsarnaev brothers had an international connection that directed that horrific event at that marathon.

Yes, the FISA Court operates in secret. Why? It is the same reason the Senate sometimes clears the Galleries, shuts the doors, cuts off the TV, and as an institution only cleared people here—classified and top secret information—can make decisions. Therein describes the FISA Court. They always deal with classified and top secret documents. They are called on a minute's notice. No other court in the world responds like that. There is a FISA judge on the bench 24/7, 365 days a year. It rotates. These are the best of the best of the judicial system around the country, picked by the Chief Justice of the Supreme Court.

Could it be open? Sure. But we would then expose either classified and top

secret documents or we could not use the documents to make the case to the FISA Court that we have a suspected individual of terrorism and we need the authority to see who that person is. Well, we have heard a lot about the FISA Court. A lot of it is true.

The people who serve on the bench are heroes because they take the toughest cases America is presented with, and they rule on them in the most judicial way they possibly can, demanding, over 25 percent of the time, that an application be resubmitted after changes because they did not think it had met the threshold.

Much has been focused on the changes to the amicus language or the "friend of the court." This is not a normal court. When the choice is to go to the FISA Court, it is because we are concerned. We are concerned about an imminent threat.

Let me explain, once again, for my colleagues and for the American people what the section 215 program is. It is a program where at the NSA we collect raw telephone numbers from telephone companies—numbers, not names.

We have a number that does not have a person's name with it. They are deidentified. We collect a number, the date the call was made, and the duration of the call. For us to trigger any search or we call it query of that database, we have to have a foreign telephone number that we know is a telephone number used by a terrorist.

Those are all the components of the section 215 program. That is it. We can have a database, but without a foreign terrorist telephone number, we cannot search the database. If we have a foreign terrorist telephone number and no database, which is where we are moving to—I concede this legislation is going to move, and we are going to transition over to hundreds of telephone companies.

Now, rather than have a number of people controlled and supervised within the NSA to carry out these queries, we are going to have telephone company employees carry out a query with a known foreign terrorist's telephone number against all of the numbers in their database. Again, hopefully, they will not tie a person's name to it. We do not even get a person's name at the NSA.

The only people who should be worried are Americans who have actually had a communication with a known terrorist abroad. Now, I think when the American people hear me talk about this, up to this point they are saying: That is a good thing. We want to know if somebody here has talked to a terrorist because we want to be kept safe.

Well, not only are we shifting the database out of the NSA over to the telephone companies, which means our response time is going to be delayed—let me remind everybody that whether we search the meta database at NSA or whether we search the database at the telephone company, we first have to go to the FISA Court and get a court

order that says: You have the authority to do this based upon what you have presented the court.

Now we have to go to the telephone companies, and in a timeframe that is conducive to them, they are going to search their database for a known terrorist's cell phone number, and now we are relying on hundreds of companies to search their database in a timely fashion and get back to us because we are trying to be in front of a threat versus behind a threat. In front of a threat, it is called intelligence; behind a threat, it is called an investigation.

When we thwarted the New York City subway bombing, we were in front of the threat. That was intelligence. When we reacted to the Boston Marathon, that was an investigation led by the FBI, not the NSA.

So when you inject this new requirement for a friend of the court—and I would disagree with my colleagues. This is not a voluntary thing for the FISA Court. It is something that is available to the FISA Court today if they choose to have somebody come in to counsel them on something. This is mandatory. In the legislation, it says "shall." The court shall set up a panel. The court shall choose a friend of the court. A friend of the court is not there to facilitate a timely processing of information.

Let me remind everybody that we are dealing with the safety of the American people. They always stress this at the end of the conversation: We want the confidence and trust to be rebuilt that we are protecting our homeland. If you are moving a database, you are making it slower. Now you are setting up a mechanism inside to slow it down even more.

What we are doing is shifting from intelligence gathering to investigations. Nobody knows how long it is going to take from the time we present the FISA Court with a foreign terrorist's telephone number before we actually complete a search process within this new database.

I happen to be the one behind a 12-month transition versus a 6-month transition, and it was all stimulated off of exactly the same person whom Senator BLUMENTHAL or Senator WYDEN quoted. They said the Director of the NSA said: We think we can do this in 6 months.

Well, I am telling you, if I am the general public in America and I am concerned about my safety and the people who are supposed to be protecting me say "I think I can do this in 6 months"—I would like somebody to say "I am absolutely 100 percent sure I can do it in 6 months." But they think they can do it in 6 months. There is the reason for a year. There is the reason for a longer transition period.

If privacy were really the concern—and everybody has come down and said: I want to protect the privacy of the American people. Let me point out a couple of things.

No. 1, we didn't collect anybody's name in this program. It is hard to intrude on somebody's privacy when you didn't collect their name. We collected the number, the date of the call, and the duration of the call. That is it. Anything else that turns into an investigation is the Federal Bureau of Investigation going to a court and saying: We have to have more information because we know the President of the Senate is a potential threat to us. And then more information can be found out, such as his identity and anything else that might be part of the investigation. But from the standpoint of the NSA, those are the only things we have—a telephone number, a date, and the duration of the call.

If privacy is the concern, I don't think we have breached it. As a matter of fact, since this program has been in existence, there has not been one case of a breach of anybody's privacy—not one.

If they were truly concerned about privacy, they would be on the floor today with a bill abolishing the CFPB, which is a government agency, a government entity that collects every financial transaction of the American people by name, by date, by amount, by transaction. But they are not down here doing that. Why? Because they don't like the fact that the FISA Court operates in secret. They don't think there should be classified or top-secret documents. They believe everything should be transparent.

Well, let me say to my colleagues, my friends, and to the American people that we have done more over the last month to destroy the capacity of this program because of the debate we have had. There is not a terrorist in the world now who doesn't understand that using a cell phone or a land line is probably a pretty bad thing. It probably puts a target on their backs. We have done a great job of chasing people to alternative methods of communication, and I would suggest to you that is not making America any safer. If anything, maybe we should have had this debate in secret simply so we wouldn't give them a roadmap as to what we do.

Therein lies the reason that there are some things on which I think there is a determination made by the executive branch and by the legislative branch and I think in many cases at the dining room tables around America where Americans say: You know, you don't need to share everything with me. I am tired of hearing things on the nightly news that I think shouldn't be discussed.

This probably happens to be one of them because it doesn't make us more safe, it makes us less safe.

I will end the same way Senator BLUMENTHAL did. People want to believe—question mark. I think people want to believe we are doing everything we possibly can to strengthen our national security, to eliminate the threat of terrorism here and abroad. My fear, quite frankly, is that this bill doesn't accomplish that.

Again, I have deep affection for those whose names are on the bill and for what they believe is the intent. But I think that at the end of the day the only responsible thing to do right now is to accept three amendments—one, a substitute, and two, a first-degree and a second-degree amendment.

Let me say briefly that the substitute incorporates two changes. One change is that the telephone companies would be required to notify 6 months in advance of any change in their retention program—in other words, how long they hold the data. I have received calls from both big telecom companies today, and they have both said: We have no problem with that.

The second one would have the Director of National Intelligence certify at the end of the transition period that technologically we can make the transition. I don't find anybody who has really objected to that.

Then there is an amendment that extends the transition period from 6 months to 12 months. There have been people who object to that. I would only tell you we have a difference of opinion. They are willing to trust the NSA on their ability to make the transition in 6 months. I think that is ironic because the reason we are here having this debate is because they have made us believe we can't trust NSA. Yet, they are willing to trust the NSA relative to a transition time that is sufficient to accomplish the transition.

Let's err on the side of caution. Let's do it at 12 months. If they can do it sooner, then let them petition us, Congress can pass it, and we will turn to it sooner. But let's not get to 6 months and be challenged with not being ready to make that transition.

The last one is a change to amicus language. Clearly, that is the biggest difference we have. I would say to my colleagues that you either vote for the amendment or you vote against it. If you vote for it, you will delay the time it will take for us to connect the dots between a foreign terrorist's telephone number and a domestic telephone number they might have talked to. If that doesn't bother Members and it doesn't bother the public, I am all for giving the American people what they want. But I think most American citizens sit at home and say: You know, the faster you do this, the safer I am. I have a responsibility first and foremost to the protection of the American people. It is in our oath.

I also share something with the Presiding Officer and my colleagues who are here—to protect the rights and liberties of the American people. And as the chairman of the Intelligence Committee, I don't think we have in any way infringed on that.

I am now in year 21. I have come a lot closer to the line than I ever dreamed when I came to Congress in 1995. But I also never envisioned an event as horrific as 9/11. I never envisioned an enemy as brutal as ISIL or Al Qaeda or the Houthis. I could go on and on.

What has changed since 9/11? On 9/11, we had one terrorist organization that had America in its crosshairs. Today, we have tens to twenties of organizations that are offshoots of terrorist organizations that would like to commit something right here in the United States. The threat hasn't become less; it has become more. We are on the floor today talking about taking away some of the tools that have been effective in helping us thwart attacks. It is the wrong debate to have, but we are here.

I would only ask my colleagues to show some reason. Extend by 6 months the transition period. Make sure it doesn't take longer to search these databases. Make sure we are ready for the telephone companies to carry out the searches because there is one certainty on which I think I would find agreement from all of my colleagues here: The terrorists aren't going away. America is still their target. No matter what we say on this floor, we are still in the crosshairs of their terrorist acts.

Only by providing the intelligence community and the law enforcement community the tools to carry out their job can they actually fulfill their obligation of making sure America is safe well into the future.

I yield the floor.

The PRESIDING OFFICER (Mr. CRUZ). The Senator from South Dakota.

Mr. THUNE. Mr. President, I hope our colleagues in the Senate and the American people are listening to this discussion because there isn't anything that is more important than defending our country. The debate we are having in the Senate today is really about the tools our intelligence community uses to prevent terrorist attacks.

As we look at and discuss the legislation in front of us, I think it is very important that we not forget we are living in dangerous times. This is the most dangerous time, literally, since 9/11 in terms of the terrorist activity that is out there. As the Senator from North Carolina pointed out, we have a big bull's-eye. The United States and people in this country, the things we believe in—the terrorists would love nothing more than to be able to take out and destroy, through some terrorist act, Americans and American interests. So I think it is very critical.

The Senator from North Carolina did a great job. I know the Senator from Indiana is going to speak here on the subject in a few minutes. But I hope everyone listens carefully because we are on the cusp of doing something that does weaken the very tools that have been used, the very capabilities that have been used to prevent those terrorist attacks.

The ironic thing about it, as you frame this up, you look at the threats that are out there, the dangerous times in which we live, and the success of these programs and how effective they have been in the past at preventing a terrorist attack, and what is being

talked about are potential abuses, hypothetical examples of how these programs could be abused, but they haven't been. The fact is, they haven't been.

We have a long period of time now in which to examine the effectiveness of these tools relative to the arguments that are being made about their abuse. They just don't exist. There isn't a documented case, in the time these tools have been in existence, of anybody's privacy being breached.

So it is very important that we look at these issues in light of what we are up against and what our No. 1 responsibility is; that is, defending Americans and Americans' interests. And this discussion is critical to that.

THE ECONOMY

Mr. President, I wish to speak on another subject this morning, and that has to do with the headline of the New York Times from Friday morning of last week, which I thought was pretty grim, and that is "U.S. Economy Contracted 0.7% in First Quarter." Let me repeat that. Not only did our economy fail to grow in the first quarter of 2015, it actually shrank.

That is pretty discouraging news for millions of Americans still struggling in the Obama economy, and the Obama administration didn't offer them any consolation. Too often the administration has met stories of economic woe with excuses: uncertainty in the eurozone, not enough foreign demand, the Japanese tsunami, too much snow, too many congressional Republicans, and of course the Obama administration's favorite excuse, the Bush administration.

This time, among other things, the administration is blaming the measurements themselves. The administration claims the Bureau of Economic Analysis is not accurately measuring economic growth from quarter to quarter. Now, of course, the Department of Commerce should always be looking for ways to modernize our measurements and adjust for seasonal changes, but no arithmetical sleight of hand can disguise the fact that our underlying economy is so weak that isolated events can shut down economic growth altogether and actually push our economy into the red.

Economic growth has averaged an abysmal 2.2 percent under this administration since the end of the recession. That is one of the weakest economic recoveries in the past 70 years. If the Obama recovery had met the average economic growth experienced in all post-World War II recoveries, our economy would be \$1.9 trillion larger than it is today.

If you look at the President's record, it is easy to see why our economy is still sputtering along: a failed \$1 trillion stimulus, \$1.6 trillion in new taxes, the President's health care law, which raised premiums for families and increased costs for small businesses, 2,222 new regulations costing more than \$653 billion in new compliance costs, a Fed-

eral debt that has doubled on the President's watch, a financial reform bill that has overreached and is stifling community banks and lending across the country, and a runaway EPA that wants to increase electricity rates on families who are already struggling with stagnant wages and now—now—wants to regulate ditches and ponds in farm fields across the country.

All of this has led some economists to wonder if 2 percent growth is the new normal. If it is, it is very bad news for American families who will face a future that is less prosperous with less economic opportunity and mobility.

During the entire postwar period, from 1947 to 2013, our Nation averaged 3.3 percent growth. At that pace, the standard of living in America almost doubles every 30 years. Incomes rise, financial security increases, and more people are able to afford homes, take vacations, and save for higher education. At the pace of growth we have seen since 2007, on the other hand, it will take closer to 99 years for the standard of living to double.

Unfortunately, our recent weak economic growth shows every sign of continuing. The Congressional Budget Office projects our economy will grow at an average pace of 2.5 percent through 2018 and just 2.2 percent from 2020 through 2025.

That is not good news for American families. For generations, individuals have clung to the promise America has always held out: If you work hard, you could build a better life for yourself and an even better one for your children. But after years of economic stagnation, that promise is now in jeopardy.

A survey released last September reported that nearly half of Americans over 18 believe their children will be worse off financially than they are. A similar percentage of Americans no longer believe if you work hard you will get ahead.

Their disillusionment is not surprising. The weak economic growth we have experienced over the past several years has left families struggling to make ends meet. Americans are struggling to make health care costs and to make mortgage payments. They are no longer sure they can put their children through college and retire comfortably. Some have even lost their homes. Good-paying jobs are few and far between.

The U.S. Census Bureau reports that for the time since the government began tracking the number, more businesses are closing each year than are being opened. Think about that. More businesses are closing. There are more business deaths than there are business births in this country today.

Millions of Americans are unemployed, and millions more are being forced to work part time because they can't find full-time work. Forty percent of unemployed Americans have become so disillusioned with the lack of opportunity, they have given up en-

tirely looking for work—40 percent. That is a staggering number. If the unemployment rate were changed to reflect the number of unemployed who have given up looking for work, our current unemployment rate would be well over 9 percent.

The good news is that things don't have to stay that way. We can enact progrowth policies that will return our economy to a more prosperous path in the 21st century. According to former CBO Director Douglas Holtz-Eakin, the differences between 2.5 percent growth and 3.5 percent growth would have a major impact on the quality of life for low- and middle-income families.

If our economy grows at a rate that is just 1 percentage point faster than what is projected, we will have 2½ million more jobs and average incomes will be \$9,000 higher. Average incomes would be \$9,000 higher if we grow just 1 percentage point faster than what is projected. For a lot of Americans, that is the difference between owning your home and renting one. It is the difference between being able to send your kids to college or forcing them to go deeply into debt to pay for their education. It is the difference between a secure retirement and being forced to work well into old age.

Additionally, the CBO estimates that for every additional one-tenth percent increase in economic growth, it reduces our deficits by \$300 billion over the next 10 years. That means an additional percentage point in economic growth will reduce our deficits by \$3 trillion over the next 10 years, and that in turn—reducing deficits—would further enhance economic growth.

Senate Republicans have laid out a number of policies to help grow the economy and open up opportunities for low- and middle-income Americans. We proposed energy policies that will expand domestic energy development which will help drive down energy prices. We are advancing trade policies that will help create more opportunities for American workers here at home by increasing the market for U.S. goods and services abroad. We have proposed tax reform that will simplify our outdated Tax Code and make our businesses more competitive, which will open up new jobs and opportunities for American workers. We have laid out entitlement reforms that will keep our promises to our seniors while protecting our economy by reducing our long-term deficits. We are pushing for regulatory reforms that will rein in the out-of-control government bureaucracies that are stifling economic growth.

Years and years of government overspending, burdensome taxation, massive government programs—many of which don't work—and excessive regulation have taken their toll on our economy, but we can still undo that damage. For generations, America has held out the promise of hope and opportunity, and Republicans are committed to ensuring it does so again. We invite

our colleagues to join us because we can have a better, brighter, and more prosperous future for future generations of Americans by changing directions, changing the policies, doing away with the regulations, the overreaching government that has made it so difficult for so many Americans to get ahead.

Mr. President, I yield the floor.

The PRESIDING OFFICER. The Senator from Indiana.

Mr. COATS. Mr. President, we are fortunately moving forward on this issue of extreme importance to the security of the American people. These are necessary procedures we should take to do everything we can to ensure our safety, to publicly discuss and debate the issue of terrorist threat and the measures the people's government is taking to defend our country and to defend each individual American from being a victim of terrorism.

As Senator BURR, chairman of the Intelligence Committee, just related, the threat to our certain security and to our safety has never been stronger, never been more threatening, with the proliferation of terrorist organizations, the unfortunate proliferation of the inspiration that is being provided through social media to any number of American citizens—and those who may not be citizens but are residing in this country—to take up arms or to create a bomb or bring harm to Americans in the name of support for jihad, in the name of ISIS, in the name of Al Qaeda, in the name of support for the extreme fundamentalist activities of terrorists that are prevailing not only through the Middle East but affecting the world in various places.

We know through intelligence gathering and through public statements, the United States has been put in the crosshairs. "Kill Americans, no matter how you do it, take it up. We will learn today, if we haven't learned already," something that has just come across the wires of someone who was attempting to do just that, and we just see more and more references to these types of attacks.

Unfortunately, we are in a period of time when one of the methods we had to try to detect these threats is no longer in operation. It is not in operation because the authorization for going forward with this program, described as section 215 of the PATRIOT Act—the collection of raw telephone numbers, not anybody's name but raw telephone numbers—that we could use as a base to determine whether, from a foreign source, a known terrorist or someone connected to a terrorist organization is talking to somebody in the United States. That is the program. Unfortunately, that program is dark. It is shut down. It shut down at midnight Sunday.

The program was shut down because we could not achieve support for even a minimum extension of time for which to better understand the program, to better debate and discuss the program,

to make adjustments necessary to ensure that Americans' privacy was not being breached. Several requests were made and, unfortunately, one Member, exercised his right to say no to a unanimous consent request, and we were in a position where we had to ask for consent driven by our procedural process we have to go through to achieve a vote. But, that vote was rejected time after time after time. So on the basis of one Member's objection, we have what I believe, what many believe, and what those who better understand this now that we have been able to disclose what it is believe is a necessary tool that ought to be in place.

This program ought to be in place for the very purpose of doing everything we can to prevent another 9/11, to prevent something much worse than 9/11, which would involve a 9/11 type of action coupled and married with a weapon of mass destruction. Where an attack in New York would not result in 3,000 in casualties—it would potentially result in 3 million casualties or even more or something concocted by a small group of people who would shoot up a shopping mall or rush into an elementary school or just simply take down someone on the subway system or an individual attack by someone with a knife or an ax or a gun.

One of the essential programs we have had that has been successful has been under attack in terms of breaching the privacy of American citizens. I think it has been made clear in the last few days that there has been no abuse of this program and that no one's privacy has been breached. The only allegation that holds true is that it has the potential to breach someone's privacy. Over the years, there has never been documented abuse. No one's privacy has been breached. To shut down a program with that kind of record on the basis that something could happen, that government could use this, I know resonates with a number of people in the United States. I really don't blame them.

This current administration's policies have created great distrust among the American people as to their leadership, as to their operations, as to their policies.

When we look at what has taken place with the IRS, definitely breaching people's privacy for political purposes, when we look at Benghazi and the coverup that has taken place in Benghazi, with the administration refusing to stand up and take responsibility for not responding adequately and changing the narrative and rewriting the intelligence. And when we look at Fast and Furious and the agency responsible there. I fully understand not just the frustration but the anger that American people have and the distrust they have.

One of the most difficult issues those of us in the Intelligence Committee have had to deal with is that when there are descriptions of policies that are implemented in terms of providing

for an intelligence gathering and necessary response to prevent terrorist attacks, that information is classified. So when we see the program being misrepresented and described as something that it isn't, we don't have the ability to respond. We can't go to the press without breaching our oath to secrecy. We do not and cannot release classified material.

So while we now are in a position of having to unclassify this material, we have to understand that everything we say is not only listened to by the American people in an attempt to ensure their privacy is not being breached—and that this is an essential tool to help prevent terrorist attacks. Terrorist groups know everything that is being said and done, and they will make behavioral changes. They will make changes in terms of how they communicate.

So the program is being compromised by the very fact that we have had to come on the floor and publicly address it and release information as to what it is to help assure the American people that, in fact, what has been said about the program is simply false.

I have been on the floor several times raising that issue, using the quotes of what has been said by Members on this floor—particularly one Member. That is blatantly false. It is a blatant misrepresentation of what the program is. Now, I am not questioning their motive. I am not questioning the individual's decision in terms of whether he is for or against or wants to support or not support. All I want to do is clarify so that the public has the facts and they can make their own determination. We make a valid case that privacy is not breached. If someone comes to the conclusion that they don't trust what we say, don't believe what we say or don't agree with what we say, that is their decision. All I want is for them to have the facts in front of them so that when they make that decision, it is based on fact and not based on what has been misrepresented.

That is why I took the actual words stated on this floor relative to the program—which I believe misrepresented the program—and challenged them. I challenged them with the factual information. I am not going to repeat them. That is a matter of record.

We now are at the point, however—because we were not able to achieve any support for any kind of extension to either clarify what the bill does and doesn't do or to clarify with the House of Representatives how we best can coordinate this process and come up with a good solution to the issue—where, procedurally, we only have two options.

One option is essentially to do nothing. The program does not secure the votes to be reauthorized, and that program is taken off the books and is no longer there. In my opinion and in the opinion of many, that makes us more vulnerable. That gives us less access to be able to stop a terrorist attack.

The second option is to support an effort that was passed by the House of Representatives, the USA FREEDOM Act, which I wish I could say addressed the issue and doesn't compromise the program. But it severely goes against what this program attempts to do. It compromises the program to the point where I am not even sure the program can exist under the provisions that have been enacted by the House of Representatives.

Three very experienced and trustworthy individuals who don't have to salute the Commander in Chief and can give their own unbiased opinions on this came before our Intelligence Committee and basically said that with the structure of the USA FREEDOM Act, you might as well not have the program in it because it will take down the program. There are a couple of major issues here that these amendments try to address but don't technically address. I am going to be supporting those amendments. I think they make a bad piece of legislation a little bit better. But I have real questions as to whether it addresses the problems that really render the program inoperable.

The first is retention. There is no mandatory retention among telephone companies that they keep the information—the phone numbers—that we need in order to create a haystack of numbers from which we can identify connections between foreign terrorist organizations and operatives inside the United States. That is not done by somebody looking at anybody's records. Before the NSA can even use a phone number, it needs to have outside approval—legal approval—to query that.

If the telephone companies don't retain those numbers, we can't go out and match them up. And there is no mandatory retention of those numbers. It is simply an amendment now that would basically say they would have to give us notice that they don't retain them. But there is no mandatory retention.

I can just see a lot of companies saying—and I have heard from a lot of companies: We don't want to be responsible for trying to build in the protections and hire the people who have the background checks and the security clearances to put a regulatory process in place to make sure our people don't abuse this or use it for the wrong purpose.

So here we have a program that is accessible only by a very limited number of people at the National Security Agency, overseen by layers and layers of lawyers and legal experts and others to make sure it is not abused in any way. They have been successful because there has not been one case of an abusiveness process against anybody's personal liberties. There are six layers of oversight that are in place before they can even take it to the court and say: We think we have a problem here. We think there is a suspicion—a rea-

sonable suspicion—that a phone number may be associated with a terrorist organization.

Then the court looks at that and says: We think you have something here. But let's check it further before we give you the authority to turn this over to the FBI so they can then look into this in greater detail to determine whether this is a live terrorist act.

As Senator BURR said, it works on the negative side, also, and there are some examples of live situations—as in the Boston bombing and so forth—that proved the negative. It proved there wasn't a conspiracy. It proved that just two people were involved in this. There were no connections. So they didn't have to waste a lot of time trying to query and pull up a bunch of information about whom they had talked to, and the police were then allowed to focus their efforts on Boston and what then took place in Boston and not throw the alarm out to New York City—the allegation was that they were on the way to New York City—and shut down New York City, causing panic and causing scare and alerting police and so forth. They were able to prove the negative of that. So it works both ways. But without that retention, we are not going to be able to accomplish that.

So I don't understand how the USA FREEDOM Act is a better way of protecting privacy and a better way of dealing with the fact that time is of the essence here. Instead of querying one area, we now have to go to multiple telephone companies, and there are 1,400 in the country. Let's say there are 100 major companies or let's say there are 10 major companies. We have to go to all 10 or to all 100 or more in order to find out whether in their database that telephone number exists. Time is of the essence here. If you are detecting a terrorist attempt and you build in all kinds of steps you have to take in order to get to the point where you think you really have something here, the act could have already been undertaken.

So those two issues, I think, are major problems with the FREEDOM Act.

The third is simply to think that the layers of protection and judicial oversight, executive oversight, and congressional oversight that take place to make sure we don't abuse the program through NSA—every telephone company has to insert that same level of oversight, and they simply won't be able to do it. It will take months. It takes months to get background checks and security clearances. Many telephone companies don't have the capacity to do that. They do not have the financial ability to do that. The irony is that individuals' privacy is more at risk by the telephone companies holding the numbers than the NSA holding the numbers, but, of course, we have not been able to convince the American people of that partly because the program has been so distortedly reported.

But this as the saving grace to protect everybody's privacy by turning it over to the phone companies instead of turning it over to NSA just doesn't add up.

It is going to be very difficult for me and I think for many of my colleagues to think—while many of us are going to support these very limited amendments, which we don't even know the House will accept, it does not resolve the issue and does not solve the problem that we are dealing with here and, in effect, could render the program inoperable.

I think when Members are making decisions about which option to choose, it is a devil's choice. Is something better than nothing or is something really nothing and you end up with nothing and nothing? None of us wants our country to be put into that position, but that is where we are. If we are not able to secure passage of these amendments to improve this and the House rejects it—or we reject it or the House rejects it, then the program will stay inoperable.

I think the American people will then be picking up their phones and writing and emailing us and urging us to rethink this program through now that they know more about it, now that they know that much of what has been said irresponsibly by Members of this body and others is not true. Once they learn more about it, I think they will be calling on us to take a new look, and they will take a new look.

The arguments simply do not hold up because they are not factual. Now that we have been able to release some of this classified information and now that people have the ability to understand, if they so choose—to take another look at this and the proof we have provided relative to the success of the program and relative to the need for the program.

That is what is before us. There has been a constitutional argument here regarding the Fourth Amendment, and it is important to note: "The right of the people to be secure in the persons, houses, papers, and effects against unreasonable searches." Unreasonable. I think we have proven this is not an unreasonable search. It does not identify anybody's name. Only after a court approves and gives the NSA the authority to go forward, similar to seeking the authority of a judge for other suspected criminal activity taking place in every jurisdiction across America, every town, every police department going to court. We tune in to "Law & Order" and "CSI" and all these programs and we see exactly how this works. You cannot go barging into a house without a warrant. You cannot collect information without a warrant.

The case being made that there is a violation here of the Fourth Amendment simply has not held up with legal authorities. Secondly—this is interesting. This was just pointed out to me. I am not a constitutional scholar. I took constitutional law in law school

and probably have forgotten half of it. But I do carry it around. I do look at it, but I am not a scholar. But I think it is pretty clear and pretty interesting that article I, section 5, talking about the legislature, says:

Each House shall keep a Journal of its Proceedings, and from time to time publish the same—

It is on our desks here. Every day, our CONGRESSIONAL RECORD, these are our proceedings—

excepting such Parts as may in their Judgment require secrecy.

That is why we have an Intelligence Committee. There are some things that require secrecy. Unfortunately, we have had to unclassify information to try to let the public know that what they have been told by their government, elected members of their government, is breaching their privacy, which is not true. We have a constitutional right as a body to make a decision and a judgment requiring secrecy. On this program, we require secrecy because once our adversaries know what we are doing, they are going to change what they are doing and it will not be worthwhile anymore.

Also, relative to the statements made by the Senator from Connecticut, who opposes the amendment on the amicus issue, it is my understanding that the Administrative Office of the United States Courts, Director Duff, sent a letter to the House asking for their concerns about the amicus issue effect on the court be placed in the bill. That was turned down by the House, unfortunately.

The letter says, “We respectfully request that, if possible, this letter be included with your Committee’s report to the House on the bill.”

It was sent to the chairman of the Permanent Select Committee on Intelligence, United States House of Representatives. It is in regard to H.R. 2048, the USA FREEDOM Act.

Mr. President, I ask unanimous consent that the letter I am referencing be printed in the RECORD.

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

ADMINISTRATIVE OFFICE OF THE
UNITED STATES COURTS
Washington, DC, May 4, 2015.

Hon. DEVIN NUNES,
Chairman, Permanent Select Committee on Intelligence, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: I write regarding H.R. 2048, the “USA Freedom Act,” which was recently ordered reported by the Judiciary Committee, to provide perspectives on the legislation, particularly an assessment that the pending version of the bill could impede the effective operation of the Foreign Intelligence Surveillance Courts.

In letters to the Committee on January 13, 2014 and May 13, 2014, we commented on various proposed changes to the Foreign Intelligence Surveillance Act (FISA). Our comments focused on the operational impact of certain proposed changes on the Judicial Branch, particularly the Foreign Intelligence Surveillance Court (“FISC”) and the Foreign Intelligence Surveillance Court of

Review (collectively “FISA Courts”), but did not express views on core policy choices that the political branches are considering regarding intelligence collection. In keeping with that approach, we offer views on aspects of H.R. 2048 that bear directly on the work of the FISA Courts and how that work is presented to the public. We sincerely appreciate the ongoing efforts of the bipartisan leadership of all the congressional committees of jurisdiction to listen to and attempt to accommodate our perspectives and concerns.

We respectfully request that, if possible, this letter be included with your Committee’s report to the House on the bill.

SUMMARY OF CONCERNS

We have three main concerns. First, H.R. 2048 proposes a “panel of experts” for the FISA Courts which could, in our assessment, impair the courts’ ability to protect civil liberties by impeding their receipt of complete and accurate information from the government (in contrast to the helpful amicus curiae approach contained in the FISA Improvements Act of 2013 (“FIA”), which was approved in similar form by the House in 2014). Second, we continue to have concerns with the prospect of public “summaries” of FISA Courts’ opinions when the opinions themselves are not released to the public. Third, we have a few other specific technical concerns with H.R. 2048 as drafted.

NATURE OF THE FISA COURTS

With the advent of a new Congress and newly proposed legislation, it seems helpful to restate briefly some key attributes of the work of the FISA Courts.

The vast majority of the work of the FISC involves individual applications in which experienced judges apply well-established law to a set of facts presented by the government—a process not dissimilar to the *ex parte* consideration of ordinary criminal search warrant applications. Review of entire programs of collection and applications involving bulk collection are a relatively small part of the docket, and applications involving novel legal questions, though obviously important, are rare.

In all matters, the FISA Courts currently depend on—and will always depend on—prompt and complete candor from the government in providing the courts with all relevant information because the government is typically the only source of such information.

A “read copy” practice—similar to the practices employed in some federal district courts for Title III wiretap applications—wherein the government provides the FISC with an advance draft of each planned application, is the major avenue for court modification of government-sought surveillance. About a quarter of “read copies” are modified or withdrawn at the instigation of the FISC before the government presents a final application—in contrast to the overwhelming majority of formal applications that are approved by the Court because modifications at the “read copy” stage have addressed the Court’s concerns in cases where final applications are submitted.

The FISC typically operates in an environment where, for national security reasons and because of statutory requirements, time is of the essence, and collateral litigation, including for discovery, would generally be completely impractical.

At times, the FISA Courts are presented with challenging issues regarding how existing law applies to novel technologies. In these instances, the FISA Courts could benefit from a conveniently available explanation or evaluation of the technology from an informed non-government source. Congress could assist in this regard by clarifying

the law to provide mechanisms for this to occur easily (e.g., by providing for pre-cleared experts with whom the Court can share and receive information to the extent it deems necessary).

THE “PANEL OF EXPERTS” APPROACH OF H.R. 2048 COULD IMPEDE THE FISA COURTS’ WORK

H.R. 2048 provides for what proponents have referred to as a “panel of experts” and what in the bill is referred to as a group of at least five individuals who may serve as an “amicus curiae” in a particular matter. However, unlike a true amicus curiae, the FISA Courts would be required to appoint such an individual to participate in any case involving a “novel or significant interpretation of law” (emphasis added)—unless the court “issues a finding” that appointment is not appropriate. Once appointed, such amici are required to present to the court, “as appropriate,” legal arguments in favor of privacy, information about technology, or other “relevant” information. Designated amici are required to have access to “all relevant” legal precedent, as well as certain other materials “the court determines are relevant.”

Our assessment is that this “panel of experts” approach could impede the FISA Courts’ role in protecting the civil liberties of Americans. We recognize this may not be the intent of the drafters, but nonetheless it is our concern. As we have indicated, the full cooperation of rank- and-file government personnel in promptly conveying to the FISA Courts complete and candid factual information is critical. A perception on their part that the FISA process involves a “panel of experts” officially charged with opposing the government’s efforts could risk deterring the necessary and critical cooperation and candor. Specifically, our concern is that imposing the mandatory “duties”—contained in subparagraph (i)(4) of proposed section 401 (in combination with a quasi-mandatory appointment process)—could create such a perception within the government that a standing body exists to oppose intelligence activities.

Simply put, delays and difficulties in receiving full and accurate information from Executive Branch agencies (including, but not limited to, cases involving non-compliance) present greater challenges to the FISA Courts’ role in protecting civil liberties than does the lack of a non-governmental perspective on novel legal issues or technological developments. To be sure, we would welcome a means of facilitating the FISA Courts’ obtaining assistance from non-governmental experts in unusual cases, but it is critically important that the means chosen to achieve that end do not impair the timely receipt of complete and accurate information from the government.

It is on this point especially that we believe the “panel of experts” system in H.R. 2048 may prove counterproductive. The information that the FISA Courts need to examine probable cause, evaluate minimization and targeting procedures, and determine and enforce compliance with court authorizations and orders is exclusively in the hands of the government—specifically, in the first instance, intelligence agency personnel. If disclosure of sensitive or adverse information to the FISA Courts came to be seen as a prelude to disclosure to a third party whose mission is to oppose or curtail the agency’s work, then the prompt receipt of complete and accurate information from the government would likely be impaired—ultimately to the detriment of the national security interest in expeditious action and the effective protection of privacy and civil liberties.

In contrast, a “true” amicus curiae approach, as adopted, for example, in the FIA,

facilitates appointment of experts outside the government to serve as *amici curiae* and render any form of assistance needed by the court, without any implication that such experts are expected to oppose the intelligence activities proposed by the government. For that reason, we do not believe the FIA approach poses any similar risk to the courts' obtaining relevant information.

"SUMMARIES" OF UNRELEASED FISA COURT
OPINIONS COULD MISLEAD THE PUBLIC

In our May 13, 2014, letter to the Committee on H.R. 3361, we shared the nature of our concerns regarding the creation of public "summaries" of court opinions that are not themselves released. The provisions in H.R. 2048 are similar and so are our concerns. To be clear, the FISA Courts have never objected to their opinions—whether in full or in redacted form—being released to the public to the maximum extent permitted by the Executive's assessment of national security concerns. Likewise, the FISA Courts have always facilitated the provision of their full opinions to Congress. See, e.g., FISC Rule of Procedure 62(c). Thus, we have no objection to the provisions in H.R. 2048 that call for maximum public release of court opinions. However, a formal practice of creating summaries of court opinions without the underlying opinion being available is unprecedented in American legal administration. Summaries of court opinions can be inadvertently incorrect or misleading, and may omit key considerations that can prove critical for those seeking to understand the import of the court's full opinion. This is particularly likely to be a problem in the fact-focused area of FISA practice, under circumstances where the government has already decided that it cannot release the underlying opinion even in redacted form, presumably because the opinion's legal analysis is inextricably intertwined with classified facts.

ADDITIONAL TECHNICAL COMMENTS ON H.R. 2048

The Judiciary, like the public, did not participate in the discussions between the Administration and congressional leaders that led to H.R. 2048 (publicly released on April 28, 2015 and reported by the Judiciary Committee without changes on April 30). In the few days we have had to review the bill, we have noted a few technical concerns that we hope can be addressed prior to finalization of the legislation, should Congress choose to enact it. These concerns (all in the *amicus curiae* subsection) include:

Proposed subparagraph (9) appears inadvertently to omit the ability of the FISA Courts to train and administer *amici* between the time they are designated and the time they are appointed.

Proposed subparagraph (6) does not make any provision for a "true *amicus*" appointed under subparagraph (2)(B) to receive necessary information.

We are concerned that a lack of parallel construction in proposed clause (6)(A)(i) (apparently differentiating between access to legal precedent as opposed to access to other materials) could lead to confusion in its application.

We recommend adding additional language to clarify that the exercise of the duties under proposed subparagraph (4) would occur in the context of Court rules (for example, deadlines and service requirements).

We believe that slightly greater clarity could be provided regarding the nature of the obligations referred to in proposed subparagraph (10).

These concerns would generally be avoided or addressed by substituting the FIA approach. Furthermore, it bears emphasis that, even if H.R. 2048 were amended to address all of these technical points, our more funda-

mental concerns about the "panel of experts" approach would not be fully assuaged. Nonetheless, our staff stands ready to work with your staff to provide suggested textual changes to address each of these concerns.

Finally, although we have no particular objection to the requirement in this legislation of a report by the Director of the AO, Congress should be aware that the AO's role would be to receive information from the FISA Courts and then simply transmit the report as directed by law.

For the sake of brevity, we are not restating here all the comments in our previous correspondence to Congress on proposed legislation similar to H.R. 2048. However, the issues raised in those letters continue to be of importance to us.

We hope these comments are helpful to the House of Representatives in its consideration of this legislation. If we may be of further assistance in this or any other matter, please contact me or our Office of Legislative Affairs at 202-502-1700.

Sincerely,

JAMES C. DUFF,
Director.

Mr. COATS. There is a lot more that could be said. We will shortly be voting on the amendments here. I probably said more than I should.

Mr. ISAKSON. Will the Senator from Indiana yield?

Mr. COATS. I will be happy to yield. This is one of the most important issues I have had to deal with during my times of service on behalf of our State and our country. I think getting the facts out has been necessary. It is a momentous decision that has momentous consequences. I hope each of us will take very seriously all that has been said and weigh that in their own judgment and hopefully make the right decisions for the future of this country.

I will be happy to yield to my colleague.

Mr. ISAKSON. I know we are about to adjourn for lunch, but I have to come to the floor and pay the Senator a great compliment. For the last 6 days, the Senator has tried to illuminate some misperceptions and, quite frankly, half-truths that have been talked about in terms of the NSA program. You have provided great information to the Senate and to the people of the United States of America, and I think it is ironic—and I do not believe the Senator from Indiana knows this—but today in the Finance Committee at 10:30 we had a hearing before the IRS Commissioner, Mr. Koskinen, who was trying to explain what the IRS was doing with the 104,000 identities that were stolen from the IRS, which included the Social Security numbers, church contributions, home residences, rent payments, debts, obligations, the entire amount of information of 104,000 American citizens. Nobody is talking about giving the IRS to the phone companies. Nobody is talking about the amount of information the IRS has and whether the government abuses or uses it. And here we are worried about 41 individuals who have the ability to know 2 telephone numbers, the origination of a call and the duration of that call, without its association to a name, unless a judge says it is OK.

I think there has been a lot of misdirection this week. The American people are starting to listen. I think the Senator from Indiana has done a great job of illuminating the truth behind this issue. We have a great country. You do not find anybody trying to break out of the United States of America. They are all trying to break in. They are because we are safe and secure. I commend the Senator for fighting for the safety, the security, and the rights of the American people.

I yield back.

Mr. COATS. I thank the Senator for those words. I think this is a fight for all of us. How I wish we had been putting our time and our passion into what the Senator from Georgia just mentioned—a clear breach of people's privacy on the record and a clear defense effort by this administration to not have us go forward and examine this. If we had been putting half of the passion into that, we would really be servicing the American people and the breaches of their privacy that are just apparent.

Here we have a program that has never had a case of a breach of privacy, that has more oversight than any other program in the entire U.S. Government, that involves all three branches of our government—the judicial, the legislative, and the executive—all with the intent of having something in place that can stop Americans from being killed by terrorists, and we have to spend weeks arguing just to correct the record, when so clearly in front of us are abuses by this administration that we are not putting attention to—the irony of that and the irony of the fact that every day we have more information about the scope of these potential terrorist attacks against Americans. Here we are releasing five known terrorist leaders from Guantanamo to a country. We are combing the world to see if somebody will take them because we do not want to retain them here, and we know they are going to go back. They are not going back to be baristas at Starbucks. They are not going back to do lawn work back home or start a microbusiness. They are going back to join the enemy attack against us. They are going back to the Taliban. They are going back to Al Qaeda. They are going back to do what they were arrested for in the first place.

How ironic and how uncertain our situation here is relative to our security, and we are arguing over a tool that can help protect us instead of focusing on the real threat.

Anyway, I got worked up during the 6 days a number of times. I appreciate the opportunity to, once again, try to clarify where we are. Hopefully, the American people are listening.

We have a momentous decision to make coming up here very shortly. I hope each of us will use not polls and not what the public perception is, I hope each of us will use the judgment that we have had and the access to information that we have had to make a

decision on the basis of what is best for the American people, not about what is best politically, not what gets us past the next election, not what is pleasing to people who want to hear things back at home, not on any other basis than what is necessary to do everything we can to keep us safe from known terrorist attacks that are multiplying faster than we can keep up with across the world, and Americans are in the crosshairs. Our decision should be based on that and that alone.

I yield the floor.

RECESS

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

Thereupon, the Senate, at 12:59 p.m., recessed until 2:15 p.m. and reassembled when called to order by the Presiding Officer (Mr. PORTMAN).

USA FREEDOM ACT OF 2015— Continued

The PRESIDING OFFICER. The Senator from Oklahoma.

Mr. INHOFE. Mr. President, I would like to inquire as to the order.

The PRESIDING OFFICER. The Senate is considering H.R. 2048 postcloture.

Mr. INHOFE. Mr. President, I ask that I be recognized.

The PRESIDING OFFICER. The Senator is recognized.

Mr. INHOFE. Mr. President, I know we have all had a chance to talk about this and the seriousness of what is now before us at this time. I look at the seriousness of this, and I listened to a lot of people standing on the floor and saying things that sound popular to people back home, and I have heard from some of the people in my State of Oklahoma, saying: They talk about the privacy problems and all these things that might be existing. Then I always think about my 20 kids and grandkids and think that they are the ones who are at stake.

This world we have right now is a much more dangerous world than it has ever been before. I look wistfully back at the good old days of the Cold War when we had a couple superpowers. We knew what they had—mutual assured destruction. It really meant something at that time. Now we have crazy people with capabilities, people in countries who have the ability to use weapons of mass destruction.

So right after 9/11 we formed the NSA. We have been talking about that down here. It is not perfect, but I think it is important at this last moment to point out the fact that a lot of lies have been told down here. I heard one person—I think two or three different ones talking about and making the statement that since the NSA procedure was set up after 9/11, that has not stopped one attack on America. I would like to suggest to you that a good friend of mine and a good friend of

the Chair's, General Alexander, who is a very knowledgeable person and ran that program for a while, said—and this was way back 2 years ago, 2013—information “gathered from these programs provided government with critical leads to prevent over 50 potential terrorist events in more than 20 countries around the world” and that the phone database played a role in stopping 10 terrorist acts since the 9/11 attacks.

I was very pleased to hear from my good friend, Senator SESSIONS, a few minutes ago that a brand new poll that just came out of the field shows that almost two-thirds of the people in America want to go back and give back to the NSA those tools we took away 2 days ago.

Now we have a situation where we can talk about a few of the cases where major attacks on this country were stopped by the process we put in place after 9/11.

One was a planned attack in 2009. Najibullah Zazi was going to bomb the New York City subway system. The plan was for him and two high school friends to conduct coordinated suicide bombings, detonating backpack bombs on New York City subway trains near New York's two busiest subway stations; that is, Grand Central Station and Times Square.

Sean Joyce, the Deputy FBI Director, said that the NSA intercepted an email from a suspected terrorist in Pakistan communicating with someone in the United States “about perfecting a recipe for explosives.”

On September 9, 2009, Afghan-American Zazi drove from his home in Aurora, CO, to New York City, after he emailed Ahmed—that was his Al Qaeda facilitator in Pakistan—that “the marriage is ready.” That was a code that meant “We are ready now to perform our task.” The FBI followed Zazi to New York and broke up the plan of attack, and they stated it was because of the email that was intercepted by the NSA that allowed them to do that.

How big of a deal is that? People do not stop and think about the fact that if you look at the New York City subway stations down there, we know that the average ridership of the New York City subway during peak hours averages just under 900,000 people—that is 900,000 people, Americans who are living in New York City.

What we do know is that when they came to New York City to perform their plan at Grand Central Station and Times Square, it was the NSA using the very tools we took away from them 2 days ago, and you wonder, how many lives would have been lost? If there are 900,000 riders on the subway and they are ready to do this at two stations, are we talking about 100,000 lives, 100,000 Americans being buried alive? That attack was precluded by the tools that were used by the NSA that we took away from them just 2 days ago. Many more have not been declassified.

GEN Michael Hayden and GEN Keith Alexander, who are both former Directors of the NSA, and others have confirmed to me personally that at least one of the three terrorist attacks on 9/11 could have been avoided, and perhaps all three could have been avoided if we had had the tools we gave the NSA right after 9/11, and also the attack on the USS Cole could have been prevented entirely.

So you have to stop and think, it is a dangerous thing to stand on the floor and say we have formed this thing in this dangerous world and it has not stopped any attacks on America. That is what we are faced with today.

I voted against the program the House passed that is going to be considered in just a few minutes. I felt it was better to leave it as we had it. Now that is gone. I look at it this way: I do support the amendments that are coming up. I do think the last opportunity we will have will be the program we will be voting on in just a few minutes.

So let's think about this, take a deep breath, and go ahead and pass something so we at least have some capability to stop these attacks and to gather information from those who would perpetrate these attacks and then have time to put together a program that will be very workable and make some changes if necessary.

With that, Mr. President, I yield the floor.

EXTENDING FISA PROVISIONS

Mr. LEAHY. It is unfortunate that we were unable to pass the USA FREEDOM Act before the June 1, 2015, sunset of sections 206 and 215 of the USA PATRIOT Act and the so-called “lone wolf” provision of the Intelligence Reform and Terrorism Prevention Act. Senator LEE and I both sought to bring up the USA FREEDOM Act well before the sunset date to avoid just this situation. Now that the roving wiretap, business records, and so-called “lone wolf” provisions have lapsed, it is important that we make clear our intent in passing the USA FREEDOM Act this week—albeit a few days after the sunset. Could the Senator comment on the intent of the Senate in passing the USA FREEDOM Act after June 1, 2015?

Mr. LEE. Although we have gone past the June 1 sunset date by a few days, our intent in passing the USA FREEDOM Act is that the expired provisions be restored in their entirety just as they were on May 31, 2015, except to the extent that they have been amended by the USA FREEDOM Act. Specifically, it is both the intent and the effect of the USA FREEDOM Act that the now-expired provisions of the Foreign Intelligence Surveillance Act, FISA, will, upon enactment of the USA FREEDOM Act, read as those provisions read on May 31, 2015, except insofar as those provisions are modified by the USA FREEDOM Act, and that they will continue in that form until December 15, 2019. Extending the effect of those provisions for 4 years is the reason section 705 is part of the act.