That doesn't satisfy them, Mr. Speaker. They even want to legalize the people that have been deported and sent to their home countries and bring them back to the United States. If that occurs, 11 million to 20 million becomes at least 30 million people.

Because we have what they call a ''de facto'' amnesty now, it is, in fact, literally amnesty now, and making that promise is going to start another rush over our borders.

We must restore the rule of law.

IMMIGRATION REFORM

(Mr. PAYNE asked and was given permission to address the House for 1 minute.)

Mr. PAYNE. Mr. Speaker, creating an immigration process for new American immigrants is not just an issue that will shape the future for one group.

So much is at stake for 3 million African and Caribbean immigrants that live and work here. They're a vital part of our future as hardworking, upstanding individuals in search of freedom and a better life. They also deserve a fair system that works, and they are more than just a number on a page.

Last week, a young lady came to my office who was born in America to Haitian parents. Her name is Natalie. Natalie is a graduate student who has job offers lined up. She is ready to work and commits herself to this country. But Natalie can't do those things because of our broken immigration system. She is neither recognized as a citizen here nor in Haiti. While in tears, she said she has no home. She can't see her family. She's scared and feels alone. Natalie is one of those 11 million people that are looking for a pathway to citizenship.

It is time to pass commonsense legislation that fixes our immigration system once and for all, one that serves our interests and reflects our values for Natalie and the 11 million other Natalies who call America home.

AMERICA'S ECONOMY CAN THRIVE AGAIN

(Mr. ROTHFUS asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. ROTHFUS. Mr. Speaker, the solution to our economic challenges is one simple word: growth. Unfortunately, the only place really growing in our country today is Washington, D.C.

As I travel my district, workers, job seekers, and small business owners tell me they're concerned about jobs and economic security.

Washington must unleash their economic potential by spending less, taxing less, and regulating less. Washington has to stop growing so the rest of the country can start to grow.

Small business owners this year spent upwards of 2 billion hours trying to comply with our Tax Code. Simplifying the Tax Code will help them save time and money that they can then put towards growing their businesses, hiring new employees and raising wages.

Washington must also streamline regulations that are strangling growth. The REINS Act would require that any regulation with an annual impact of $100 million or more be subject to a vote of this House.

With the right tax and regulatory policies, America's economy can thrive again.

□ 1240

CLOSE GUANTANAMO BAY

(Mr. MORAN asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. MORAN. Mr. Speaker, about 12 years ago, 779 people were gathered initially and sent to the prison at Guantanamo Bay, Cuba. About 85 percent of them had never actually engaged in direct combat against the United States. A report was issued by an independent, authoritative commission yesterday that I want to bring attention to. It was headed by Asa Hutchinson, a former Republican colleague of ours, and 4 star General Jim Jones, who was head of the National Security Council in the Obama administration.

It concluded that the United States engaged in the practice of torture at Guantanamo Bay. It concluded that the methods we used, like waterboarding, slamming prisoners into walls, chaining them in stress positions for hours, violated international legal obligations with ''no firm or persuasive evidence that they produced valuable information that could not have been obtained by other means.'' It also concluded that what we did had ''no justification'' and ''damaged the standing of our Nation, reduced our capacity to convey moral censure when necessary, and potentially increased the danger to U.S. military personnel taken captive.''

It concluded that President Bush and Vice President Cheney were directly involved in condoning such tactics and that their legal advisors engaged in ''acrobatic'' legal analysis to attempt to establish legal justification.

There was no legal precedent. Guantanamo Bay should be closed—now.

TAX REFORM

(Mr. SOUTHERLAND asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. SOUTHERLAND. Mr. Speaker, it's tax week. As you know, that means that Americans' heads are chock-full of all kinds of numbers. We've done all kinds of itemizations, deductions, and calculations in our personal finances just to make sure that we know how much we are going to hand over to Uncle Sam. Let me share with you some more numbers.

How about $168 billion? That's how much our fellow Americans spend each year just to make sure they comply with our overcomplicated Tax Code. Just how complicated are the tax rules in this country? Well, here is another number—4 million. That's how many words there are in the U.S. Tax Code. There are 4,500 words in the U.S. Constitution. There are 775,000 words in the Bible. Yet there are 4 million in our Tax Code.

What does this all add up to?

It means that our current tax system is broken. We need fundamental, comprehensive tax reform to make our Tax Code fairer and simpler for all Americans. That is the House Republican plan.

PROVIDING FOR CONSIDERATION OF H.R. 624, CYBER INTELLIGENCE SHARING AND PROTECTION ACT

Mr. WOODALL. Mr. Speaker, by direction of the Committee on Rules, I call up House Resolution 164 and ask for its immediate consideration.

The Clerk read the resolution, as follows:

H. RES. 164

Resolved, That at any time after the adoption of this resolution the Speaker may, pursuant to clause 2(b) of rule XVIII, declare the House resolved into the Committee of the Whole House on the state of the Union for consideration of the bill (H.R. 624) to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes. The first reading of the bill shall be dispensed with. All points of order against consideration of the bill are waived. General debate shall be confined to the bill and shall not exceed one hour equally divided and controlled by the chair and ranking minority member of the Permanent Select Committee on Intelligence. After general debate the bill shall be considered for amendment under the five-minute rule. In lieu of the amendment in the nature of a substitute recommended by the Permanent Select Committee on Intelligence now printed in the bill, it shall be in order to consider as an original bill for the purpose of amendment under the five-minute rule an amendment in the nature of a substitute consisting of the text of Rules Committee Print 113-7. That amendment in the nature of a substitute shall be considered as read. All points of order against that amendment in the nature of a substitute are waived. No amendment to that amendment in the nature of a substitute shall be in order except those printed in the report of the Committee on Rules accompanying this resolution. Each such amendment may be offered only in the order printed in the report, may be offered only by a Member designated in the report, shall be considered as read, shall be debatable for the time specified in the report equally divided and controlled by the proponent and an opponent, shall not be subject to amendment, and shall not be subject to a demand for division of the question in the House or in the Committee of the Whole. All points of order against such amendments are waived. At the conclusion of consideration of the bill for amendment the Committee shall rise and report the bill to the House with such amendments as may have been adopted. Any Member may demand a separate vote in the House on any

amendment adopted in the Committee of the Whole to the bill or to the amendment in the nature of a substitute made in order as original text. The previous question shall be considered as ordered on the bill and amendments thereto to final passage without intervening motion except one motion to recommit with or without instructions.

The SPEAKER pro tempore. The gentleman from Georgia is recognized for 1 hour.

Mr. WOODALL. Mr. Speaker, for the purpose of debate only, I yield the customary 30 minutes to my friend, the gentleman from Florida (Mr. HASTINGS), pending which I yield myself such time as I may consume. During consideration of this resolution, all time yielded is for the purpose of debate only.

GENERAL LEAVE

Mr. WOODALL. I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Georgia?

There was no objection.

Mr. WOODALL. Mr. Speaker, I always enjoy the reading of the resolution. There are a lot of readings that you can waive on the floor of this House, but not so with a Rules resolution because this resolution is framing the nature of the debate we are going to have perhaps on the most important issue that we've taken up so far in this Congress.

The underlying bill is H.R. 624. It's the Cyber Intelligence Sharing and Protection Act.

Whenever we start talking about cyber intelligence sharing and protection, folks often think that sharing and protection are oxymorons—you can't have protected sharing, and you can't have shared protection. It's not an easy nut to crack, Mr. Speaker. I don't sit on the Intelligence Committee, but I've been down to the classified briefings where folks are sharing details of the amazing successes that our teams, both domestically and abroad, are having and combating in cyber threats; but it's getting harder and harder every day, and we have to balance the national security implications of failing to address these threats with what we, as all Americans, love, which is our liberty here at home—our liberty here at home, our privacy here at home.

In order to try to crack that, Mr. Speaker, you'll know that we brought this bill to the floor in the last Congress, and it has been changed and improved since that time. Today, this rule makes in order an additional 12 amendments. Now, of course we'll have the traditional 1 hour of debate on the underlying bill, but there will be another 12 amendments, each debated—2 hours of total additional time—so that Members can have their voices heard. Of these additional 12 amendments, four of them were offered by Republican Members; seven of them were offered by Democratic Members; and one of them is a bipartisan amendment. But the rule is designed to allow that further discussion because of the very important nature of the underlying bill.

I rise, of course, in support of the rule to allow for that debate, and I rise in support for the underlying bill. In today's world, you don't have to have a battlefield full of tanks to wage war on your enemy. A nation-state can have a roomful of young computer scientists and a couple of computers and begin to be a threat to the largest, most democratically controlled country in the world.

How do we stop that, Mr. Speaker? Because we don't want to close our borders. We don't want to have Federal control over the Internet. In so many of these nation-states, the government does control the Internet. That's never going to happen here in America. That's not who we are. That's not what we're about. In fact, 10 private sector providers control about 80 percent of the networks here in America—as it should be.

But what can we do to make ourselves safer tomorrow than we are today? Here is what the underlying bill does, Mr. Speaker: it enables, for the very first time, businesses and governments to share information about the threats that they are facing.

If you go up the road to Maryland, where the NSA is operating today, there are some smart, smart folks there, and I'm glad we have every single one of them on the front lines of cyber warfare—protecting America, protecting American enterprise. Yet today, when they are aware of threats that are impending threats to our financial system, threats to our economic system, they can't share that information with the private sector.

Back in my home district, Mr. Speaker, we're home to UPS—the United Parcel Service—Delta, Home Depot. If those companies come under attack today, Delta can't share that information with American Airlines and say, Look at what has just happened to us. Be on the lookout. It might happen to you. Home Depot can't share with Lowe's today, This is what has happened to us. We want you to be on the lookout. Don't let it happen to you.

□ 1250

This bill changes that. This bill, for the first time, says in the name of defending America and American interests against cyber threats around the globe, you can begin to share with one another what your experiences are and opportunities to protect yourself from having that happen to you again in the future.

Now, the real important thing to me about this bill, and I will just hold it up for you, Mr. Speaker, the Cyber Intelligence Sharing and Protection aspect of this bill, it's the important part. It's the meat of this bill. It's what's going to allow us to be safer tomorrow than we are today, but the bulk of the words in this bill don't speak to the sharing in terms of enabling it. It speaks to the sharing in terms of restricting it. Page after page after page after page of this short, 24-page bill talks about how we as citizens must, must, must continue to be safe and secure in the privacy of our own information.

It's a four-step process the bill lays out, Mr. Speaker, in terms of how we can ensure that no personally identifiable information is being shared from Home Depot or Delta or UPS or any of the other folks who are out there on the Internet when they're sharing that with the government or with one another in order to prevent threats to American security or economic prosperity, to ensure that personally identifiable information is not a part of that information that's shared, because privacy is paramount.

I've been tremendously impressed through this process, Mr. Speaker, because I'm one of the folks who is most likely to be suspect when we start talking about sharing information with the government. I'm a big lover of liberty. There's not many things I'm willing to give liberty up for. In fact, I dare say there's not a one that I'm willing to give liberty up for.

But the Intelligence Committee, from which this bill came, has worked with Members month after month after month after month to ensure that privacy is protected, that we as citizens can be secure. At the same time that we're fighting threats that perhaps we're not allowed to talk about on this floor, we're protected from threats that each and every one of us experiences in our day-to-day lives—a threat to privacy.

It's not been easy to craft this bill, and it has been an incredible bipartisan effort throughout, Mr. Speaker, in order to put this language together. Again, we have four Republican amendments made in order by this rule, seven Democratic amendments made in order by this rule, and one bipartisan amendment made in order by this rule. It is my great hope that we can move forward today with this rule, with debate on the underlying bill, and move forward with something that is far, far, far overdue, Mr. Speaker, and that's protecting America—American business and American individuals, American citizens—from the threats posed by nation states through cyber warfare from abroad.

With that, I reserve the balance of my time.

Mr. HASTINGS of Florida. Mr. Speaker, I thank my friend from Georgia for yielding me the customary 30 minutes, and I yield myself such time as I may consume.

Before I begin, I would like to take a moment, as have almost all of our colleagues that have spoken here today, to offer my sincerest condolences to the people of Boston, Massachusetts, following the deadly explosions at

Monday's marathon. I can't speak for everyone here, but I believe that most of us would say that the thoughts and prayers of the United States Congress are with the victims, their families and friends at this most difficult time. Those responsible for this act of terror will be brought to justice.

Mr. Speaker, while I rise today in support of H.R. 624, the Cyber Intelligence Sharing and Protection Act, better known as CISPA, I do not support the rule. My friend from Georgia spoke about how important it is that we have the reading of the rule, and one of the particular efforts of Congress that allows for there not to be any abridgement of that, but I do believe that we would be better served if this were an open rule.

Last night, during our Rules Committee hearing, the majority blocked several germane Democratic amendments which would have further helped to balance cybersecurity concerns with smart policies that protect our citizens. I spoke to those issues last night, and I raise them again, particularly the two amendments offered by our colleagues, Ms. SCHAKOWSKY and Mr. SCHIFF, and others.

However, the underlying CISPA legislation is, as my friend from Georgia said, a bipartisan bill that aims to safeguard our Nation's computer networks and critical infrastructure by allowing for two-way cyber threat information sharing on an entirely voluntary basis, both between the private sector and the Federal Government, and within the private sector itself.

In his March 12, 2013, testimony before the Senate Intelligence Committee, the Director of National Intelligence, James Clapper, stated for the first time that cyber attacks and cyber espionage have supplanted terrorism as the top security threat facing the United States.

In recent months, media reports have highlighted cyber attacks on several major U.S. companies, including Facebook, Google, and the network security firm RSA, as well as The New York Times, Bloomberg News, and The Washington Post newspapers.

Furthermore, government networks such as those of the Central Intelligence Agency and the United States Senate have also been targeted by hackers. Waves of cyber attacks have sought to disrupt operations at financial institutions and service providers, including American Express, JPMorgan Chase, Citigroup, Wells Fargo, Bank of America, MasterCard, PayPal, and Visa.

The fact of the matter is that state actors, terrorist organizations, criminal groups, individuals, and countless persons that describe themselves as hackers attack our public and private computer networks thousands of times every day. Many foreign hackers seek to steal valuable trade secrets, which results in the loss of countless American jobs. There are estimates that have been quoted of loss from economic espionage that range as high as $400 billion a year.

Unfortunately, the same vulnerabilities used to steal trade secrets can be used to attack the critical infrastructure we depend on every day. Our economy, our power grids, and our defenses are increasingly reliant on computers and network integration. These networks power our homes, provide our clean water, protect our bank accounts, defend our intellectual property, guard our national security information, and manage other critical services. In addition to intellectual property and national security intelligence, personal finance, health care, and other private records are prime targets for hackers to steal.

According to the Information Technology Industry Council, 18 adults become victims to cyber crime—including identity theft and phishing campaigns—every second. This adds up to 1.5 million cyber crime victims each day.

□ 1300

Cyber attacks present a very real and dangerous threat to the United States. However, the government currently does not have the authority to share classified cyber intelligence information with the private sector.

While private companies have taken considerable measures to protect their networks, they often have limited information and can only respond to known threats.

Cyber threats evolve at the speed of technology, and CISPA, this measure, helps the private sector protect against cyber attacks by providing companies with the latest cyber threat information from the intelligence community, which has timely, classified information about destructive malware. This cyber threat intelligence is the information that companies and the government need to protect and defend their networks.

The so-called ''signatures'' are primarily made up of numerical codes consisting of zeros and ones, without any personal information attached.

CISPA is the product of close cooperation between the intelligence community, the private sector companies, and trade groups and, to a certain degree, the White House, as it pertains to many of the measures that are included in this legislation.

During their efforts to improve the bill, they also maintained a dialogue with privacy advocates in an effort to strengthen civil liberties protections and oversight.

I add a personal note here for the reason that, over a period of 10 years, I served 8 of those years on the Intelligence Committee, and the now-chairman of the Intelligence Committee and ranking member were both junior members of the committee that I served on. They have risen to the position that they are in and have acted in an extremely responsible way, over a 2-year period of time, trying to bring a measure as complicated as this one, contemplating all of the factors that I've identified and more, including the members of the committee.

I would urge Members of the House of Representatives—many of them continue to have concerns, not only about this particular legislation, but about other intelligence matters, and rightly so are they concerned. But let me remind them that they are Members of a body that allows, if they wish to go into the spaces of the Intelligence Committee and to be briefed by staff and Members there on classified information, upon appropriate undertakings, they too can gain the information and insight that's needed in order to make an intelligent determination when they are voting, rather than come out here and criticize the people that do that hard work. They get no benefits, no concerns from the Members, and yet, cannot say all of the things that are needed to say or be said to the American public.

The same holds for ADAM SCHIFF and JAN SCHAKOWSKY and others that I won't mention that I served on that committee with. These are conscientious people who spend more time than almost any Member of Congress on any matter that he or she is attending to, and I have great respect for them. I don't agree with everything that either or all of them say, but I know they put their heart and time, both in the amendments that are offered, as well as in this bill and the particulars that are being put forward to this body.

As a result of their work, 19 improvements to enhance privacy and protect Americans have been adopted. Chief among them, this CISPA measure that requires the government to eliminate any personal information it receives that is not necessary to understand the cyber threat.

It creates no new authorities for any agency, and I can't say that enough. It creates no new authorities for any agency.

It gives companies the flexibility to choose which agency within the intelligence community they would like to work with to protect the cyber networks. It requires an annual review and report by the intelligence community's inspector general of the government's use of any information shared by the private sector.

And I would urge Members, when we increase the responsibilities of the inspector general that we also give the inspector general the resources in order to be able to do the necessary oversight that is required in this legislation.

It includes something that I very much support, and that is a 5-year sunset provision. I've supported other 5-year sunset provisions in the intelligence community and would have preferred, in this instance, that it be a 3-year provision. But the fact of the matter is, it's 5, and we will learn an awful lot during that period of time, and we will be back here dealing with

this same subject at some point in the future.

Allowing for the appropriate sharing of cyber threat information between the government and private sector is key to protecting our Nation from those who would do us harm. CISPA balances the critical need to strengthen our cyber defenses while protecting Americans' individual privacy.

I reserve the balance of my time.

Mr. WOODALL. Mr. Speaker, at this time it's my great pleasure to yield 3 minutes to the gentleman from Texas (Mr. CONAWAY), one of those Members on the Intelligence Committee my friend from Florida spoke of, a gentleman who serves us all.

Mr. CONAWAY. Mr. Speaker, I appreciate the opportunity to speak.

I rise in strong support of the rule and the underlying legislation that is before us this afternoon.

I also want to congratulate my colleague from Florida. I agree wholeheartedly with his reasons why this is important. He walked through those very eloquently.

I'd like to speak quickly as to what this bill does not do. It does not create a government surveillance program. It does not give the government the authority to monitor private networks or communications like email or other activities.

And it is strictly voluntary. It does not create a mandate on the private sector that they participate. In fact, these activities, monitoring and surveillance, are specifically excluded from being an activity that would be authorized under this bill.

There are four purposes for which this activity can be conducted, and whatever gets done has to fit within one of these four. One is cybersecurity. Two is investigating and prosecuting cybersecurity crimes. Three would be preventing death and physical injury, and four would be protecting minors from physical and psychological harm. So whatever gets done under this bill has to fit within those narrow categories specifically to make that happen.

As both speakers have said already, great work has been done in trying to protect the privacy and the civil liberties that all of us have. Those who have a grave concern that we've not fixed those, I would ask them to simply go review the contract they have with their Internet service provider. They have ceded immense personal liberties and privacies under that contract to simply sign up with that Internet service provider.

So as they look at what we're trying to do with this bill, I would argue that they may have already gone past that with respect to those guys.

This bill does nothing like that whatsoever. No personal information can be shared. There's a mandate that the government put in place filters so that, as that data's coming in at the speed of light, no one's reading this information. This is machine-to-machine. That personal information is scrubbed from that as it comes in.

There are immense reporting requirements for this system to be put in place, so that if there are occasional breaches, and there may be, that those breaches are reported on a timely basis to the committee, not at the end of some arbitrary period but as quickly as the system can report it to the oversight committees that have jurisdiction.

There is no ambiguity in this bill. It says what can be done and what cannot be done, and it outlines the consequences for breaking the law.

Let me also agree with my colleague from Florida. It has a sunset provision. Five years from now, future Congresses will have to either deal with this or it goes away. And so unlike many of our bills that just simply go on unless we actually do something, this has the protection of allowing those who disagree with it to know that there will be another bite at this apple 5 years from now if, in fact, there are things we've learned about that intervening 5-year period.

But this is critical for America to have this. If this were a physical attack on this country, there would be no question that the Federal Government, through its military, would stand in the breach and protect this country. There are no less dangerous attacks conducted against infrastructure, banks, airlines, other things every single day that we weren't able to help protect the private sector from, and this bill goes a long way toward doing that.

I urge my colleagues to support the rule and the underlying bill.

Mr. HASTINGS of Florida. Mr. Speaker, I'm privileged to yield 5 minutes to the distinguished gentleman from Colorado (Mr. POLIS), my colleague on the Rules Committee.

Mr. POLIS. Mr. Speaker, where to begin?

Let's start with process. This, as has been indicated by everyone who spoke thus far, is a critical issue for our country, getting the balance right between protecting American infrastructure and our way of life, with our civil liberties and confidence in the Internet ecosystem. And yet, this rule only allows 1 hour of debate in the House of Representatives on this bill.

□ 1310

I might add, the amendments that were talked about in the Rules Committee last night, the amendments that actually address some of the deficiencies which I'll be getting into about this bill, are not allowed under this rule. In fact, out of the 12 amendments allowed, two of them are actually the same. The same exact amendment allowed twice. And yet a number of other amendments are not even allowed to be debated or voted on here on the floor of the House.

I hold in my hands many, many amendments that were brought forward by Members of both parties and under this rule were prevented from being debated upon here on the floor of the House, which is why I strongly encourage my colleagues to vote ''no'' on the rule and ''no'' on the underlying bill in its present form.

There's no disagreement that cybersecurity is a very real and important issue. Threats come from criminal enterprises, they come from nation states, they come from corporations, they come from 16-year-olds. There's a variety of threats to both the public and private sector both here and abroad. The question is, What's the solution?

One of the first fallacies with the premise of this bill at the 20,000-foot level is, Who helps who? Frankly, it is the government that needs to learn and the private sector that leads the way. I've talked to a number of technology executives, having been a technology executive before I got here, and they are frequently ahead of the government. Because everyday they're fighting hacking attempts and they're on the front lines of cybersecurity.

Now it's not a doubt whether they want free help. Who wouldn't want free help? Should we in fact as taxpayers subsidize the defense of those who have not invested in their own cybersecurity? Should this be a bailout of companies with poor cybersecurity? But the truth of the matter is most of the learning that needs to occur is from the private sector to the government. And, in fact, we're taking some of those steps. The government and the NSA are using private contractors who are in the forefront of this issue every day, and that's more of the direction we need to go.

The notion that somehow the government would be of assistance to companies is laughable to many of the technology executives that I talk to; nor would they expect to call the government for help when they themselves are so far ahead. But to the extent we want to get the government involved with information and with the private sector here, we need to be very careful how this information is used, not just from a civil liberties perspective, which we'll be talking about, but because this is an economic issue; it's a confidence issue.

The Internet has been a tremendous engine of innovation and economic growth. And we should be concerned for the Internet ecosystem, concerned for the millions of jobs, concerned for the great value that's been created, the benefits to consumers across the country, the way it's touched our lives in so many ways.

What's fundamentally flawed in this approach is it trumps privacy agreements in terms of use that Internet companies enter with their users. So you could sign up for a service on the Internet, it could say explicitly we will not share this information with the government unless required by law, in terms of use—and frequently there are

statements analogous to that in there—and the minute you click send and complete it, if this bill were law, the company you gave that information to could then turn around, in violation of their own terms of use, and provide all that information to the government.

The limitations on what the government would do with that information are completely inadequate. There is a section of the bill on pages 10 and 11 that deals with those limitations. First, it says that information can be used for cybersecurity purposes. Okay, that's the purpose of the bill: investigation and prosecution of cybersecurity crimes. That's okay. Then it goes far afield into pretty much everything. It talks about bodily harm, danger of death. When we look at bodily harm and bodily injury, that includes things under USC section 18, 365: cuts, abrasions, bruises, disfigurement, including mental pain.

So this is anything the government wants to use the information for. Paper that can cause paper cuts. The government can collect who's buying paper, who's buying scissors, who's playing football, who's organizing gun shows, who's a Tea Party enthusiast.

The SPEAKER pro tempore. The time of the gentleman has expired.

Mr. HASTINGS of Florida. I yield the gentleman 1 additional minute.

Mr. POLIS. And there are absolutely no protections with regard to what is done with that information.

There are a number of improvements that could make this bill viable, and these are not allowed under this rule. My colleague, Mr. SCHIFF, has put forward an amendment that would have simply required that reasonable precautions were taken to ensure privacy was protected. That would be a strong step forward. Real limitations about actually tying the use of this information to cybersecurity would be an important step forward with the bill.

What's at danger is, yes, civil liberties; but the danger is the confidence in the Internet ecosystem that has driven our economic growth over the last decade. There will be great harm if that confidence is shaken, great harm if people know that the information that they provide and sign up for can immediately be turned over to a government agency—indeed, a secretive government agency—with no recourse and completely exempt from any liability for the company that's done it.

It's been noted that this program is voluntary. It may be voluntary for the corporations. It's not voluntary for the individual. It's not voluntary for the citizens of the country who provide that information.

Mr. WOODALL. Mr. Speaker, I yield myself 1 minute to say I know my friend from Colorado's concerns are heartfelt, and he shared those last night in the Rules Committee. The gentleman has a great deal of experience in this industry. And as heartfelt as his concerns are, I know, too, equally heartfelt are his concerns to national security if we fail to come together and address this issue.

I would like to be able to say, Mr. Speaker, that when we pass this bill today, it's going directly to the President's desk for signature. I don't actually believe that to be true. I think it's a long process between now and getting it to the President's desk for signature. And I know the gentleman will be raising these concerns throughout that process.

But I just cannot emphasize enough, Mr. Speaker, the dangers to the liberties of the American people of failing to begin this process today. I'm very proud we're allowing 12 amendments today to work through the concerns that the gentleman has, among others. But the importance of beginning this process today cannot be overstated.

I reserve the balance of my time.

Mr. HASTINGS of Florida. Mr. Speaker, I am very pleased at this time to yield 3 minutes to the gentleman from California (Mr. SCHIFF), my friend and a distinguished member of the Intelligence Committee.

Mr. SCHIFF. I thank the gentleman for yielding.

Mr. Speaker, I rise in opposition to the rule. At the outset, let me say that the cyber threat is real and its damage already devastating. And I very much appreciate the work that the chair and ranking member of the Intelligence Committee have done on this bill, and I appreciate that we have made and are continuing to make improvements.

But as the bill currently stands and as it will stand even after the amendments allowed by the rule are adopted, the bill simply does not do enough to protect the private information of Americans. Most importantly, I'm disappointed that the proposed rule does not allow an amendment that I offered with Ms. SCHAKOWSKY, Ms. ESHOO, Mr. HOLT, and Mr. THOMPSON of Mississippi. My amendment would fix an issue specifically cited by the White House in its Statement of Administration Policy in explaining why the President's advisers would recommend a veto of CISPA without important change. It would require the companies that share cyber threat information either with the government or with another private company to make reasonable efforts to remove personally identifiable information.

As the administration stated in its veto threat, the administration remains concerned that the bill does not require private entities to take reasonable steps to remove irrelevant personal information when sending cybersecurity data to the government or other private sector entities. Citizens have a right to know that corporations will be held accountable—and not granted immunity—for failing to safeguard personal information adequately.

The requirement of government-alone efforts to safeguard or minimize personal information is simply not enough. This is most apparent when, under the immunized conduct in the bill, private entities can share information with each other without ever going through the government. In those circumstances, how can the government minimize what it never possesses? So government-side minimization alone, which is all this bill includes, is not enough.

We have responded to the concerns of industry by making sure that when we ask them to take reasonable efforts to remove personal information, they can do so in real-time through automated processes. The witnesses who testified before the Intelligence Committee said that often the private parties are in the best position to anonymize the data. This is something they're doing anyway. And it's more than reasonable to require them to do that, particularly if we want to give them a broad grant of immunity.

□ 1320

Mr. Speaker, without an amendment to ensure that companies remove private information when they can do so—when they can do so through reasonable efforts—I cannot support the underlying bill. I believe that Members of both parties who support this change deserve the chance to vote on it. I suspect that because that issue would have gathered broad support, it is not being brought up for a vote here on the floor, and that is very disappointing. Accordingly, I urge a ''no'' vote on the rule, and I thank the gentleman for yielding.

Mr. WOODALL. Mr. Speaker, I yield myself 60 seconds to say I agree with my friend, that the private sector is often in the best position to get the work done that we're talking about in this bill.

I would refer my colleague, Mr. Speaker, to the Intelligence Committee's Web site—it's intelligence.house.gov—where you can see the long list of those private sector actors who are supporting this bill here today, that long list of folks in the private sector responsible for the security of their firms, of the information that Americans have entrusted to them, asking this body to move forward with this bill today.

There's no question, Mr. Speaker, when you're dealing with something of the magnitude of the national security threats posed by cyber warfare and the privacy protections that everyone in this body is committed to, that you're going to end up with conscientious men and women on both sides of this issue. But it is important to note that the private sector—which is being bombarded each and every day with threats from nation-state actors overseas—is asking, pleading with this body to move forward with this bill.

I reserve the balance of my time.

Mr. HASTINGS of Florida. Mr. Speaker, may I inquire about how much time remains on both sides?

The SPEAKER pro tempore. The gentleman from Florida has 9 minutes remaining. The gentleman from Georgia has 17 minutes remaining.

Mr. HASTINGS of Florida. With that, Mr. Speaker, in an effort to respond to my colleague and friend from Georgia, I yield 1 additional minute at this time to the gentleman from California (Mr. SCHIFF).

Mr. SCHIFF. I thank the gentleman for yielding the additional time.

And just to respond to my colleague, I'd be interested to know if there is anything you can point to in those 17 amendments that governs or requires the private sector, when it shares information with other private sector entities, to remove personally identifiable information. Because under the bill, the only minimization that's required is being done by the government; and in the case of private-to-private sector sharing, there is no government role. So this is the big hole.

While there are many private sector companies that may support the bill because it gives them broad immunity without any responsibility, that doesn't mean it's good policy, particularly when private companies have said they would make reasonable efforts. They're willing to do it; they can do it; they have the capacity to do it; we're just not asking them to do it or requiring them to do it. And we're giving something of great value to them, and that is we're giving them broad immunity. I think with that immunity ought to come some responsibility; and it shouldn't be too much to ask that that responsibility take the form of a reasonable effort, not a herculean one, not an impossible one, but a reasonable effort to ensure that Americans' privacy interests are observed and they take out that information when they can.

Mr. WOODALL. Mr. Speaker, I reserve the balance of my time.

Mr. HASTINGS of Florida. Mr. Speaker, again, for purposes of clarity, I yield 1 additional minute to my colleague from Colorado (Mr. POLIS).

Mr. POLIS. Mr. Speaker, I have three documents to submit to the RECORD: one from former Representative Bob Barr, one Statement of Administration Policy, and a letter from several tech companies and others opposed to the bill.

I quote, in part:

Developments over the last year make CISPA's approach even more questionable than before.

Former Representative Bob Barr:

Congress must take the civil liberties threats created by this bill just as seriously as it takes the cyber threats the legislation purports to address.

Mr. Speaker, we should not hurt the Internet to save the Internet; and this bill, in its current form, leaves the language wide open with potential abuse. Again, when we talk about bodily harm, I have learned that in a California statute that includes dog bites. Essentially, anything is included in this information without limitation with regard to how the government can use it. This is a backdoor attack on the Fourth Amendment against unreasonable search and seizures.

We have criminal procedures and processes around how information can and can't be used. This is the biggest government takeover of personal information that I've seen during my time here in Congress. Again, I believe, on the balance, it harms what it purports to protect.

''JUST SAY NO'' TO CYBERSECURITY BILL

(By Former Rep. Bob Barr (R–Ga.), Apr. 16, 2013)

Anyone who has read or watched any news source over the past year knows President Obama, numerous Administration officials, and many leaders in Congress agree that addressing the threat of cyber attacks is a critical national priority. Based on this threat analysis, the administration and many members of Congress continue to push for passage of cybersecurity legislation that would clarify and expand the government's powers to receive and process traffic from American computer networks.

It would, however, be a mistake for Congress to rush to enact legislation that could militarize our computer networks, and pave the way for private companies to share vast quantities of sensitive and highly personal information with the government, all in the name of ''cybersecurity.'' Although a carefully-crafted ''information sharing'' program that includes robust protections for civil liberties could be an effective approach to cybersecurity, the bill about to come up for a vote in the House clearly fails this test.

The Cyber Intelligence Sharing and Protection Act (CISPA), H.R. 624, is set to be considered by the full House of Representatives later this month. Although the bill that emerged from markup by the House Permanent Select Committee on Intelligence (HPSCI) includes some improvements in privacy safeguards over the earlier version, CISPA's proponents have overstated the protections incorporated into the bill. As a result, members of Congress should vote against CISPA when it comes to the House floor.

Last year, The Constitution Project's bipartisan Liberty and Security Committee, on which I serve, prepared a detailed report on ways that Congress could protect our nation's computer networks from cyber threats, while at the same time preserving the constitutionally-guaranteed rights of Americans. Unfortunately, the drafters of CISPA failed to incorporate the robust safeguards we recommended.

Most critical, CISPA's sponsors have resisted all efforts to ensure that the new cybersecurity program would maintain civilian control of our nation's computer networks. CISPA would allow private companies, cloaked with broad immunity from legal liability, to share sensitive information such as internet records or the content of emails, with any agency in the government, including military and intelligence agencies. Sensitive personal information from private computer networks should not be shared directly with the military or the National Security Agency (NSA), the agency that gained widespread public notoriety seven years ago for its warrantless wiretapping program—hardly the agency we want to see tasked with receiving private internet traffic.

Sadly, the members of HPSCI voted down an amendment that would have ensured civilian control of computer networks, by specifying that when private companies share information with the federal government, they should not provide it to the NSA or any other military agency or department. This amendment would still have permitted the NSA to share its own expertise on cyber threats with the private sector, but would have protected the information flowing into the government.

A second critical flaw with CISPA is that it fails to include meaningful limits on the extent of private sensitive information that companies can send into the government. The HPSCI also voted down an amendment requiring that before sharing cyber threat information with the government, companies must ''make reasonable efforts'' to remove ''any information that can be used to identify a specific person unrelated to the cyber threat.'' A similar provision was included in last year's Senate cybersecurity bill, and witnesses at a hearing before HPSCI earlier this year testified that companies can easily strip out personally identifiably information that is not necessary to address cyber threats. Yet CISPA still lacks any such safeguard.

It is true that from a privacy perspective, this version of CISPA is an improvement over last year's bill. Most notably, the bill no longer permits private information to be used for broad 'national security uses'' unrelated to cybersecurity. But it clearly is not sufficient. Congress must take the civil liberties threats created by this bill just as seriously as it takes the cyber threats the legislation purports to address. CISPA does not meet this test, and members of the House should just say no.

STATEMENT OF ADMINISTRATION POLICY

H.R. 624—VYBER INTELLIGENCE SHARING AND PROTECTION ACT

(Rep. Rogers, R–MI, and Rep. Ruppersberger, D–MD), Apr. 16, 2013)

Both government and private companies need cyber threat information to allow them to identify, prevent, and respond to malicious activity that can disrupt networks and could potentially damage critical infrastructure. The Administration believes that carefully updating laws to facilitate cybersecurity information sharing is one of several legislative changes essential to protect individuals' privacy and improve the Nation's cybersecurity. While there is bipartisan consensus on the need for such legislation, it should adhere to the following priorities: (1) carefully safeguard privacy and civil liberties; (2) preserve the long-standing, respective roles and missions of civilian and intelligence agencies; and (3) provide for appropriate sharing with targeted liability protections.

The Administration recognizes and appreciates that the House Permanent Select Committee on Intelligence (HPSCI) adopted several amendments to H.R. 624 in an effort to incorporate the Administration's important substantive concerns. However, the Administration still seeks additional improvements and if the bill, as currently crafted, were presented to the President, his senior advisors would recommend that he veto the bill. The Administration seeks to build upon the continuing dialogue with the HPSCI and stands ready to work with members of Congress to incorporate our core priorities to produce cybersecurity information sharing legislation that addresses these critical issues.

H.R. 624 appropriately requires the Federal Government to protect privacy when handling cybersecurity information. Importantly, the Committee removed the broad national security exemption, which significantly weakened the restrictions on how this information could be used by the government. The Administration, however, remains concerned that the bill does not require private entities to take reasonable steps to remove irrelevant personal information when sending cybersecurity data to the government or other private sector entities. Citizens have a right to know that corporations

will be held accountable—and not granted immunity—for failing to safeguard personal information adequately. The Administration is committed to working with all stakeholders to find a workable solution to this challenge. Moreover, the Administration is confident that such measures can be crafted in a way that is not overly onerous or cost prohibitive on the businesses sending the information. Further, the legislation should also explicitly ensure that cyber crime victims continue to report such crimes directly to Federal law enforcement agencies, and continue to receive the same protections that they do today.

The Administration supports the longstanding tradition to treat the Internet and cyberspace as civilian spheres, while recognizing that the Nation's cybersecurity requires shared responsibility from individual users, private sector network owners and operators, and the appropriate collaboration of civilian, law enforcement, and national security entities in government. H.R. 624 appropriately seeks to make clear that existing public-private relationships—whether voluntary, contractual, or regulatory—should be preserved and uninterrupted by this newly authorized information sharing. However, newly authorized information sharing for cybersecurity purposes from the private sector to the government should enter the government through a civilian agency, the Department of Homeland Security.

Recognizing that the government will continue to receive cybersecurity information through a range of civilian, law enforcement, and national security agencies, legislation must promote appropriate sharing within the government. As stated above, this sharing must be consistent with cybersecurity use restrictions, the cybersecurity responsibilities of the agencies involved, as well as privacy and civil liberties protections and transparent oversight. Such intra-governmental sharing and use should not be subject to undue restrictions by the private sector companies that originally share the information. To be successful in addressing the range of cyber threats the Nation faces, it is vital that intra-governmental sharing be accomplished in as near real-time as possible.

The Administration agrees with the need to clarify the application of existing laws to remove legal barriers to the private sector sharing appropriate, well-defined, cybersecurity information. Further, the Administration supports incentivizing industry to share appropriate cybersecurity information by providing the private sector with targeted liability protections. However, the Administration is concerned about the broad scope of liability limitations in H.R. 624. Specifically, even if there is no clear intent to do harm, the law should not immunize a failure to take reasonable measures, such as the sharing of information, to prevent harm when and if the entity knows that such inaction will cause damage or otherwise injure or endanger other entities or individuals.

Information sharing is one piece of larger set of legislative requirements to provide the private sector, the Federal Government, and law enforcement with the necessary tools to combat the current and emerging cyber threats facing the Nation. In addition to updating information sharing statutes, the Congress should incorporate privacy and civil liberties safeguards into all aspects of cybersecurity and enact legislation that: (1) strengthens the Nation's critical infrastructure's cybersecurity by promoting the establishment and adoption of standards for critical infrastructure; (2) updates laws guiding Federal agency network security; (3) gives law enforcement the tools to fight crime in the digital age; and (4) creates a National Data Breach Reporting requirement.

APRIL 15, 2013.

DEAR REPRESENTATIVE: Earlier this year, many of our organizations wrote to state our opposition to H.R. 624, the Cyber Intelligence Sharing and Protection Act of 2013 (CISPA). We write today to express our continued opposition to this bill following its markup by the House Permanent Select Committee on Intelligence (HPSCI). Although some amendments were adopted in markup to improve the bill's privacy safeguards, these amendments were woefully inadequate to cure the civil liberties threats posed by this bill. In particular, we remain gravely concerned that despite the amendments, this bill will allow companies that hold very sensitive and personal information to liberally share it with the government, including with military agencies.

CISPA creates an exception to all privacy laws to permit companies to share our information with each other and with the government in the name of cybersecurity. Although a carefully-crafted information sharing program that strictly limits the information to be shared and includes robust privacy safeguards could be an effective approach to cybersecurity, CISPA lacks such protections for individual rights. CISPA's information sharing regime allows the transfer of vast amounts of data, including sensitive information like internet records or the content of emails, to any agency in the government including military and intelligence agencies like the National Security Agency or the Department of Defense Cyber Command.

Developments over the last year make CISPA's approach even more questionable than before First, the President recently signed Executive Order 13636, which will increase information sharing from the government to the private sector. Information sharing in this direction is often cited as a substantial justification for CISPA and will proceed without legislation. Second, the cybersecurity legislation the Senate considered last year, S. 3414, included privacy protections for information sharing that are entirely absent from CISPA, and the Obama administration, including the intelligence community, has confirmed that those protections would not inhibit cybersecurity programs. These included provisions to ensure that private companies send cyber threat information only to civilian agencies, and a requirement that companies make ''reasonable efforts'' to remove personal information that is unrelated to the cyber threat when sharing data with the government. Finally, witnesses at a hearing before the House Permanent Select Committee on Intelligence confirmed earlier this year that companies can strip out personally identifiably information that is not necessary to address cyber threats, and CISPA omits any requirement that reasonable efforts be undertaken to do so.

We continue to oppose CISPA and encourage you to vote 'no.'

Sincerely,

Access; Advocacy for Principled Action in Government; American Arab Anti-Discrimination Committee; American Association of Law Libraries; American Civil Liberties Union; American Library Association; Amicus; Association of Research Libraries; Bill of Rights Defense Committee; Breadpig.com; Center for Democracy & Technology; Center for National Security Studies; Center for Rights; Competitive Enterprise Institute; The Constitution Project; Council on American-Islamic Relations; CREDO Action; Daily Kos; Defending Dissent Foundation; Demand Progress.

DownsizeDC.org, Inc.; Electronic Frontier Foundation; Fight for the Future; Free Press Action Fund; Government Accountability Project; Liberty Coalition; Mozilla; National Association of Criminal Defense Lawyers; New American Foundation's Open Technology Institute; OpenMedia.org; PolitiHacks; Reddit; RootsAction.org; Tech Freedom.

Mr. WOODALL. Mr. Speaker, I yield myself 60 seconds again to say to my friend from Colorado that I know his concerns are heartfelt; but he knows, as I do, there's nothing that we can do in statute here today that would trump any of our civil liberties that are protected under the Constitution of the United States of America. The Constitution of the United States of America trumps all.

What we're doing here today, Mr. Speaker, is responding to a very serious national security threat, and we're doing so in a way that can give Americans great comfort that their civil liberties are every bit as protected today as they were yesterday. In fact, Mr. Speaker, in that these nation-states are hacking into these accounts and accessing our personal information every single day, I would tell you that we will actually have our privacy more protected in the presence of a secure Internet than we do today, as nation-states are frequently eroding our cybersecurity border here in the United States of America.

With that, I reserve the balance of my time.

Mr. HASTINGS of Florida. Mr. Speaker, I would advise my friend from Georgia that I'm the last speaker. If he is prepared to close, I am prepared to close.

Mr. WOODALL. I thank my friend. I have one speaker remaining.

Mr. HASTINGS of Florida. I reserve the balance of my time.

Mr. WOODALL. Mr. Speaker, at this time it is my great pleasure to yield as much time as he may consume to the chairman of the Rules Committee, the gentleman from Texas (Mr. SESSIONS).

Mr. SESSIONS. Mr. Speaker, I want to thank the gentleman, my dear friend from Georgia (Mr. WOODALL), not only for managing his rule, but for the time that he has invested not into just this issue, but the issues that come before the Rules Committee, and I want to thank him for his service.

I also want to thank, if I can, the gentleman from Florida (Mr. HASTINGS)—welcome back to the committee after a couple of days of being out with surgery—and for the vigorous hearing that we had yesterday at the Rules Committee.

Mr. Speaker, we had an opportunity to have Mr. RUPPERSBERGER, the leader for the Democrats from the Intelligence Committee, as well as MIKE ROGERS from Michigan, the chairman of the committee. Both came and vigorously talked about the things which are aimed at our country—cyber threats, nation-states, nations such as China, North Korea, and others who are trying to invade our Internet here in the United States and to steal not only information and data, but also thoughts, ideas, and money. So it gave

us an opportunity yesterday to have a great hearing, one which was full of detail, one which really offered intrigue by our Members and a lot of thought process by all those who came before the committee.

However, I would like to advise, if I can, that following the closing statements on the rule before us, the gentleman from Georgia (Mr. WOODALL) will be offering an amendment to the rule that seeks to address concerns with the role of civilian Federal agencies in receiving the cyber information that would be transmitted from the private sector that is included in the underlying bill. This amendment was in negotiation yesterday and submitted for consideration to the Rules Committee, but the final compromise was not ready at the time that the committee finished its work product yesterday evening, so negotiations continued all last night and through this morning until today.

On a bipartisan basis, these negotiations have given us what I consider to be a good amendment with good merits and should be considered under this rule. The amendment has been vetted thoroughly by the five committees which share jurisdiction in this matter, including Ranking Members THOMPSON and RUPPERSBERGER, and, by the way, my colleague, the ranking member of the Rules Committee, Ms. SLAUGHTER.

If the rule is amended, the language would be offered by Mr. MCCAUL, the chairman of the House Committee on Homeland Security. I'm confident that this work product and the work which we are bringing to this floor will continue to support not just the rule, but the legislation that would be before this House tomorrow by the Rules Committee.

So I believe that this helps not just the underlying bill, but really is a testament to the work on a bipartisan basis among our committees, among a lot of people who had a chance to look at not just jurisdictional issues, but the actual substance of trying to make protecting this country, its assets, and its people a reality now in law that the United States House of Representatives will fully debate tomorrow, vote on, and support.

Part of the role of the Rules Committee about this process has been to make sure that the final product that came to the floor of the House of Representatives was well vetted, received the attention that was necessary, and, perhaps more importantly, was leading-edge.

□ 1330

And, lastly, the most important thing is that we know what we've agreed to; that we know what we've agreed to where we're very clear about what the law is and the expectations of that performance.

I thank the gentleman for yielding.

Mr. HASTINGS of Florida. Mr. Speaker, I yield myself such time as I may consume.

I thank the distinguished chairman of the Rules Committee, my good friend, Mr. SESSIONS, for his explanation of the measure going forward. I certainly do not anticipate that my side will oppose the measure as offered.

In addition thereto, I would highlight what he did eloquently point out, and that is the bipartisan effort that has been put into this, including all of the negotiations leading up to now what will be the McCaul amendment offered by Mr. WOODALL.

CISPA, Mr. Speaker, provides the government and private sector with the tools they need to secure our networks and prevent future cyber attacks, while respecting the privacy of individuals.

In bringing private companies and trade groups to the table, as well as taking into consideration the concerns expressed by civil liberties organizations, CISPA has been improved to better address the growing cybersecurity risks faced by the Federal Government and private sector, provide greater oversight, and protect Americans' privacy. We can take significant steps to reduce our vulnerability to cyber threats today.

I have had the honor and privilege of meeting many of our intelligence professionals when I served as a member of the Intelligence Committee; and since that time, I cannot overstate how much I appreciate, and am humbled by, their service.

Furthermore, I want to take this moment of personal privilege to thank my good friends, Chairman ROGERS and Ranking Member RUPPERSBERGER, and to underscore one of the unnoticed and hardworking staffs' efforts, and that would be the House Intelligence Committee staff, for their hard work and dedication in helping to see this and other measures having to do with the intelligence of this committee to the House floor, as well as in cooperation with their colleagues and ours at the United States Senate.

I urge my colleagues to vote ''no'' on the rule and ''yes'' on the underlying bill, and I yield back the balance of my time.

Mr. WOODALL. Mr. Speaker, I yield myself the balance of my time.

I thank my friend from Florida for his service on the Rules Committee and his service on the Intelligence Committee.

The work that goes on in the Intelligence Committee, Mr. Speaker, is work that so many Members of Congress do not involve themselves in. It goes on deep in the bowels of the Capitol Complex. It's under great security, all electronic devices left outside the door, so that they can discuss things within the four walls of that committee that we're not allowed to discuss here on the House floor.

In fact, when they asked me to handle the rule today, Mr. Speaker, I was a little concerned because throughout this process of developing CISPA, I traveled down to that committee room time and time again in order to understand the threats that this Nation is facing, understand the challenges that this community of intelligence professionals is grappling with around the globe, and I don't want to be the one who shares those stories here on the House floor by mistake. I don't envy the gentleman from Florida having to balance being in that committee every single day, trying to protect the security of every single citizen, and not being able to come out of that committee room and share with, not just your colleagues here in the House, but your constituents back home, why it is you're doing the things that you do.

Can you imagine, Mr. Speaker, what would have happened in World War II if we had to keep the bombing of Pearl Harbor a secret? It's a secret. Nobody knows. What do you think the support would have been, Mr. Speaker, for taking affirmative action in World War II? It would have been hard to generate that support. I would have voted ''no.''

There are things going on in this Nation and in this world today, Mr. Speaker, that our Intelligence Committee grapples with, that our intelligence professionals grapple with, things that are frightening, and things that threaten the liberty of this country and the economic security of this country. Now, I don't want to be a fearmonger, Mr. Speaker. What I love about this country is no matter what the challenge is, we are great enough collectively to rise to meet it.

In this case, we happen to need to rise to meet it in a subject matter that is near and dear to the heart of every American, which is my Internet privacy. I care a lot about Internet privacy, Mr. Speaker. I've got a VPN system set up so nobody is listening in on my Wi-Fi. I change my password about every 10 days to make sure nobody is making any progress towards hacking my system. I'll occasionally go on the Internet and use one of those anonymizers to make sure my IP address isn't being tracked when I'm looking at things that perhaps my friends in Congress, I'm trying to get a bill done, I don't want you to know I'm getting that bill done. Who knows what those people down in HIR, House Information Resources, what they're tracking that we do here? We have tools available to us in that way, Mr. Speaker.

But do you know who I can't outsmart? Perhaps I can outsmart my next-door neighbor who wants to piggyback on my Wi-Fi system. Perhaps I can outsmart the guy at the hotel who is trying to piggyback on my information there in the hotel room. Perhaps I can even outsmart the U.S. House of Representatives. But what I can't outsmart is that team of cyber warriors gathered by nation-states around the globe who are hacking my information and your information every single day, stealing our intellectual property, stealing our military technology, threatening the privacies that we've

talked so much about here on the floor today.

I'm very glad, Mr. Speaker, that as you page through this bill, you will find line after line after line aimed at protecting your and my privacy. I think we do a good job of finding that balance. We even will offer amendments today on the floor to do even better. But without security at the Internet border, I have no protection of my privacy because those agents of the state of China, North Korea, and beyond are accessing that information today.

Mr. Speaker, it's been 18 months that we've been working to craft that balance of privacy and security. We'll continue to work on that throughout 12 amendments here today. I urge my colleagues, look through this resolution, look through H.R. 624 to see the efforts that have gone into crafting this bipartisan piece of legislation; and look at those 12 amendments, look at those 12 amendments that we'll have an opportunity to vote on over the next 2 days to make this bill even better. But the time for delay, Mr. Speaker, has passed us, and the cost of delay is most certainly measured in dollars, and I fear it is measured in lives.

Let's move forward with this bill today, Mr. Speaker. I urge strong support for the rule, and I urge strong support after the debate of these 12 amendments on the underlying legislation.

AMENDMENT OFFERED BY MR. WOODALL

Mr. WOODALL. Mr. Speaker, at this time, I offer an amendment to the resolution.

The SPEAKER pro tempore. The Clerk will report the amendment.

The Clerk read as follows:

At the end of the resolution, add the following:

SEC. 2. Notwithstanding any other provision of this resolution, the amendment specified in section 3 shall be in order as though printed as the last amendment in House Report 113–41 if offered by Representative McCaul of Texas or his designee. That amendment shall be debatable for 10 minutes equally divided and controlled by the proponent and an opponent.

SEC. 3. The amendment referred to in section 2 is as follows: After section 1, insert the following new section (and renumber subsequent sections accordingly):

"SEC. 2. FEDERAL GOVERNMENT COORDINATION WITH RESPECT TO CYBERSECURITY.

''(a) COORDINATED ACTIVITIES.—The Federal Government shall conduct cybersecurity activities to provide shared situational awareness that enables integrated operational actions to protect, prevent, mitigate, respond to, and recover from cyber incidents.

''(b) COORDINATED INFORMATION SHARING.—

''(1) DESIGNATION OF COORDINATING ENTITY FOR CYBER THREAT INFORMATION.—The President shall designate an entity within the Department of Homeland Security as the civilian Federal entity to receive cyber threat information that is shared by a cybersecurity provider or self-protected entity in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, except as provided in paragraph (2) and subject to the procedures established under paragraph (4).

''(2) DESIGNATION OF A COORDINATING ENTITY FOR CYBERSECURITY CRIMES.—The President shall designate an entity within the Department of Justice as the civilian Federal entity to receive cyber threat information related to cybersecurity crimes that is shared by a cybersecurity provider or self-protected entity in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, subject to the procedures under paragraph (4).

''(3) SHARING BY COORDINATING ENTITIES.—The entities designated under paragraphs (1) and (2) shall share cyber threat information shared with such entities in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, consistent with the procedures established under paragraphs (4) and (5).

''(4) PROCEDURES.—Each department or agency of the Federal Government receiving cyber threat information shared in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act, shall establish procedures to—

''(A) ensure that cyber threat information shared with departments or agencies of the Federal Government in accordance with such section 1104(b) is also shared with appropriate departments and agencies of the Federal Government with a national security mission in real time;

''(B) ensure the distribution to other departments and agencies of the Federal Government of cyber threat information in real time; and

''(C) facilitate information sharing, interaction, and collaboration among and between the Federal Government; State, local, tribal, and territorial governments; and cybersecurity providers and self-protected entities.

''(5) PRIVACY AND CIVIL LIBERTIES.—

''(A) POLICIES AND PROCEDURES.—The Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the Secretary of Defense shall jointly establish and periodically review policies and procedures governing the receipt, retention, use, and disclosure of nonpublicly available cyber threat information shared with the Federal Government in accordance with section 1104(b) of the National Security Act of 1947, as added by section 3(a) of this Act. Such policies and procedures shall, consistent with the need to protect systems and networks from cyber threats and mitigate cyber threats in a timely manner—

''(i) minimize the impact on privacy and civil liberties;

''(ii) reasonably limit the receipt, retention, use, and disclosure of cyber threat information associated with specific persons that is not necessary to protect systems or networks from cyber threats or mitigate cyber threats in a timely manner;

''(iii) include requirements to safeguard non-publicly available cyber threat information that may be used to identify specific persons from unauthorized access or acquisition;

''(iv) protect the confidentiality of cyber threat information associated with specific persons to the greatest extent practicable; and

''(v) not delay or impede the flow of cyber threat information necessary to defend against or mitigate a cyber threat.

''(B) SUBMISSION TO CONGRESS.—The Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the Secretary of Defense shall, consistent with the need to protect sources and methods, jointly submit to Congress the policies and procedures required under subparagraph (A) and any updates to such policies and procedures.

''(C) IMPLEMENTATION.—The head of each department or agency of the Federal Government receiving cyber threat information shared with the Federal Government under such section 1104(b) shall—

''(i) implement the policies and procedures established under subparagraph (A); and

''(ii) promptly notify the Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, the Secretary of Defense, and the appropriate congressional committees of any significant violations of such policies and procedures.

''(D) OVERSIGHT.—The Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the Secretary of Defense shall jointly establish a program to monitor and oversee compliance with the policies and procedures established under subparagraph (A).

''(6) INFORMATION SHARING RELATIONSHIPS.—Nothing in this section shall be construed to—

''(A) alter existing agreements or prohibit new agreements with respect to the sharing of cyber threat information between the Department of Defense and an entity that is part of the defense industrial base;

''(B) alter existing information-sharing relationships between a cybersecurity provider, protected entity, or self-protected entity and the Federal Government;

''(C) prohibit the sharing of cyber threat information directly with a department or agency of the Federal Government for criminal investigative purposes related to crimes described in section 1104(c)(1) of the National Security Act of 1947, as added by section 3(a) of this Act; or

''(D) alter existing agreements or prohibit new agreements with respect to the sharing of cyber threat information between the Department of Treasury and an entity that is part of the financial services sector.

''(7) TECHNICAL ASSISTANCE.—

''(A) DISCUSSIONS AND ASSISTANCE.—Nothing in this section shall be construed to prohibit any department or agency of the Federal Government from engaging in formal or informal technical discussion regarding cyber threat information with a cybersecurity provider or self-protected entity or from providing technical assistance to address vulnerabilities or mitigate threats at the request of such a provider or such an entity.

''(B) COORDINATION.—Any department or agency of the Federal Government engaging in an activity referred to in subparagraph (A) shall coordinate such activity with the entity of the Department of Homeland Security designated under paragraph (1) and share all significant information resulting from such activity with such entity and all other appropriate departments and agencies of the Federal Government.

''(C) SHARING BY DESIGNATED ENTITY.—Consistent with the policies and procedures established under paragraph (5), the entity of the Department of Homeland Security designated under paragraph (1) shall share with all appropriate departments and agencies of the Federal Government all significant information resulting from—

''(i) formal or informal technical discussions between such entity of the Department of Homeland Security and a cybersecurity provider or self-protected entity about cyber threat information; or

''(ii) any technical assistance such entity of the Department of Homeland Security provides to such cybersecurity provider or such self-protected entity to address vulnerabilities or mitigate threats.

''(c) REPORTS ON INFORMATION SHARING.—

''(1) INSPECTOR GENERAL OF THE DEPARTMENT OF HOMELAND SECURITY REPORT.—The Inspector General of the Department of Homeland Security, in consultation with the

Inspector General of the Department of Justice, the Inspector General of the Intelligence Community, the Inspector General of the Department of Defense, and the Privacy and Civil Liberties Oversight Board, shall annually submit to the appropriate congressional committees a report containing a review of the use of information shared with the Federal Government under subsection (b) of section 1104 of the National Security Act of 1947, as added by section 3(a) of this Act, including—

''(A) a review of the use by the Federal Government of such information for a purpose other than a cybersecurity purpose;

''(B) a review of the type of information shared with the Federal Government under such subsection;

''(C) a review of the actions taken by the Federal Government based on such information;

''(D) appropriate metrics to determine the impact of the sharing of such information with the Federal Government on privacy and civil liberties, if any;

''(E) a list of the departments or agencies receiving such information;

''(F) a review of the sharing of such information within the Federal Government to identify inappropriate stovepiping of shared information; and

''(G) any recommendations of the Inspector General of the Department of Homeland Security for improvements or modifications to the authorities under such section.

''(2) PRIVACY AND CIVIL LIBERTIES OFFICERS REPORT.—The Officer for Civil Rights and Civil Liberties of the Department of Homeland Security, in consultation with the Privacy and Civil Liberties Oversight Board, the Inspector General of the Intelligence Community, and the senior privacy and civil liberties officer of each department or agency of the Federal Government that receives cyber threat information shared with the Federal Government under such subsection (b), shall annually and jointly submit to Congress a report assessing the privacy and civil liberties impact of the activities conducted by the Federal Government under such section 1104. Such report shall include any recommendations the Civil Liberties Protection Officer and Chief Privacy and Civil Liberties Officer consider appropriate to minimize or mitigate the privacy and civil liberties impact of the sharing of cyber threat information under such section 1104.

''(3) FORM.—Each report required under paragraph (1) or (2) shall be submitted in unclassified form, but may include a classified annex.

''(d) DEFINITIONS.—In this section:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security, the Committee on the Judiciary, the Permanent Select Committee on Intelligence, and the Committee on Armed Services of the House of Representatives; and

''(B) the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Select Committee on Intelligence, and the Committee on Armed Services of the Senate.

''(2) CYBER THREAT INFORMATION, CYBER THREAT INTELLIGENCE, CYBERSECURITY CRIMES, CYBERSECURITY PROVIDER, CYBERSECURITY PURPOSE, AND SELF-PROTECTED ENTITY.—The terms 'cyber threat information', 'cyber threat intelligence', 'cybersecurity crimes', 'cybersecurity provider', 'cybersecurity purpose', and 'self-protected entity' have the meaning given those terms in section 1104 of the National Security Act of 1947, as added by section 3(a) of this Act.

''(3) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

''(4) SHARED SITUATIONAL AWARENESS.—The term 'shared situational awareness' means an environment where cyber threat information is shared in real time between all designated Federal cyber operations centers to provide actionable information about all known cyber threats.''.

Page 5, strike line 6 and all that follows through page 6, line 7.

Page 7, beginning on line 17, strike ''by the department or agency of the Federal Government receiving such cyber threat information''.

Page 13, strike line 13 and all that follows through page 15, line 23.

Page 17, strike line 15 and all that follows through page 19, line 19.

Mr. WOODALL. Mr. Speaker, I yield back the balance of my time, and I move the previous question on the amendment and on the resolution.

The previous question was ordered.

The SPEAKER pro tempore. The question is on the amendment.

The amendment was agreed to.

The SPEAKER pro tempore. The question is on the resolution, as amended.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. HASTINGS of Florida. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The vote was taken by electronic device, and there were—yeas 227, nays 192, not voting 13, as follows:

[Roll No. 109]

YEAS—227

Aderholt
Alexander
Amash
Amodei
Bachus
Barber
Barletta
Barr
Barton
Benishek
Bentivolio
Bilirakis
Bishop (UT)
Black
Bonner
Boustany
Brady (TX)
Bridenstine
Brooks (AL)
Brooks (IN)
Broun (GA)
Buchanan
Bucshon
Burgess
Calvert
Camp
Campbell
Cantor
Capito
Carter
Cassidy
Chabot
Chaffetz
Coble
Coffman
Cole
Collins (GA)
Collins (NY)
Conaway
Cook
Costa
Cotton
Cramer
Crawford
Crenshaw
Culberson
Daines
Davis, Rodney
Denham
Dent
DeSantis
DesJarlais
Diaz-Balart
Duffy
Duncan (SC)
Duncan (TN)
Ellmers
Farenthold
Fincher
Fitzpatrick
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Franks (AZ)
Frelinghuysen
Gardner
Garrett
Gerlach
Gibbs
Gibson
Gingrey (GA)
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (MO)
Griffin (AR)
Griffith (VA)
Grimm
Guthrie
Gutierrez
Hall
Hanna
Harper
Harris
Hartzler
Hastings (WA)
Heck (NV)
Hensarling
Herrera Beutler
Hudson
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Issa
Jenkins
Johnson (OH)
Johnson, Sam
Jordan
Joyce
Kelly (PA)
King (IA)
King (NY)
Kingston
Kinzinger (IL)
Kline
Labrador
LaMalfa
Lamborn
Lance
Lankford
Latham
Latta
LoBiondo
Long
Lucas
Luetkemeyer
Lummis
Marchant
Marino
Massie
Matheson
McCarthy (CA)
McCaul
McHenry
McIntyre
McKeon
McKinley
McMorris Rodgers
Meadows
Meehan
Messer
Mica
Miller (FL)
Miller (MI)
Mullin
Mulvaney
Murphy (PA)
Neugebauer
Noem
Nugent
Nunes
Nunnelee
Olson
Owens
Palazzo
Paulsen
Pearce
Perry
Petri
Pittenger
Pitts
Poe (TX)
Pompeo
Posey
Price (GA)
Radel
Reed
Reichert
Renacci
Ribble
Rice (SC)
Rigell
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rogers (MI)
Rokita
Rooney
Ros-Lehtinen
Roskam
Ross
Rothfus
Royce
Runyan
Ruppersberger
Ryan (WI)
Salmon
Scalise
Schneider
Schock
Schweikert
Scott, Austin
Sensenbrenner
Sessions
Shuster
Simpson
Smith (NE)
Smith (NJ)
Smith (TX)
Southerland
Stewart
Stivers
Stutzman
Terry
Thompson (PA)
Thornberry
Tiberi
Tipton
Turner
Upton
Valadao
Wagner
Walberg
Walden
Walorski
Weber (TX)
Webster (FL)
Wenstrup
Whitfield
Williams
Wilson (SC)
Wittman
Wolf
Womack
Woodall
Yoder
Yoho
Young (AK)
Young (FL)
Young (IN)

NAYS—192

Andrews
Barrow (GA)
Bass
Beatty
Becerra
Bera (CA)
Bishop (GA)
Bishop (NY)
Blumenauer
Bonamici
Brady (PA)
Braley (IA)
Brown (FL)
Brownley (CA)
Bustos
Butterfield
Capps
Capuano
Cárdenas
Carney
Carson (IN)
Cartwright
Castor (FL)
Castro (TX)
Chu
Cicilline
Clarke
Clay
Cleaver
Clyburn
Cohen
Connolly
Conyers
Cooper
Courtney
Crowley
Cuellar
Cummings
Davis (CA)
Davis, Danny
DeFazio
DeGette
Delaney
DeLauro
DelBene
Deutch
Dingell
Doggett
Doyle
Duckworth
Edwards
Ellison
Engel
Enyart
Eshoo
Esty
Farr
Fattah
Foster
Frankel (FL)
Fudge
Gabbard
Gallego
Garamendi
Garcia
Grayson
Green, Al
Green, Gene
Grijalva
Hahn
Hanabusa
Hastings (FL)
Heck (WA)
Higgins
Himes
Hinojosa
Holt
Honda
Horsford
Hoyer
Huffman
Israel
Jackson Lee
Jeffries
Johnson (GA)
Johnson, E. B.
Jones
Kaptur
Keating
Kelly (IL)
Kildee
Kilmer
Kind
Kirkpatrick
Kuster
Langevin
Larsen (WA)
Larson (CT)
Lee (CA)
Levin
Lewis
Lipinski
Loebsack
Lofgren
Lowenthal
Lowey
Lujan Grisham (NM)
Luján, Ben Ray (NM)
Maffei
Maloney, Carolyn
Maloney, Sean
Matsui
McCarthy (NY)
McClintock
McCollum
McDermott
McGovern
McNerney
Meeks
Meng
Michaud
Miller, George
Moore
Moran
Murphy (FL)
Nadler
Napolitano
Negrete McLeod
Nolan
O'Rourke
Pallone
Pascrell
Pastor (AZ)
Payne
Pelosi
Perlmutter
Peters (CA)
Peters (MI)
Peterson
Pingree (ME)
Pocan
Polis
Price (NC)
Quigley
Rahall
Richmond
Rohrabacher
Roybal-Allard
Ruiz
Rush
Ryan (OH)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Schakowsky
Schiff
Schrader
Schwartz
Scott (VA)
Scott, David
Serrano
Sewell (AL)
Shea-Porter
Sherman
Sinema
Sires
Slaughter
Smith (WA)
Speier
Stockman
Swalwell (CA)
Takano
Thompson (CA)
Thompson (MS)
Tierney
Titus
Tonko
Tsongas
Van Hollen
Vargas
Veasey
Vela
Velázquez
Visclosky
Walz
Wasserman Schultz
Waters
Watt
Waxman
Welch
Wilson (FL)
Yarmuth

NOT VOTING—13

Bachmann	Kennedy	Rangel
Blackburn	Lynch	Shimkus
Gohmert	Markey	Westmoreland
Holding	Miller, Gary	
Hurt	Neal	

□ 1418

Mr. RAHALL, Ms. PELOSI, Ms. BROWNLEY of California, Mr. CÁRDENAS and Ms. WILSON of Florida changed their vote from ''yea'' to ''nay.''

Messrs. KING of New York, YOHO and AMASH changed their vote from ''nay'' to ''yea.''

So the resolution was agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

APPOINTMENT OF MEMBERS TO THE BOARD OF VISITORS TO THE UNITED STATES COAST GUARD ACADEMY

The SPEAKER pro tempore (Mr. RODNEY DAVIS of Illinois). The Chair announces the Speaker's appointment, pursuant to 14 U.S.C. 194, and the order of the House of January 3, 2013, of the following Members on the part of the House to the Board of Visitors to the United States Coast Guard Academy:

Mr. COBLE, North Carolina

Mr. COURTNEY, Connecticut

□ 1420

CYBER INTELLIGENCE SHARING AND PROTECTION ACT

GENERAL LEAVE

Mr. ROGERS of Michigan. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and include extraneous material on the bill H.R. 624.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Michigan?

There was no objection.

The SPEAKER pro tempore. Pursuant to House Resolution 164 and rule XVIII, the Chair declares the House in the Committee of the Whole House on the state of the Union for the consideration of the bill, H.R. 624.

The Chair appoints the gentlewoman from Florida (Ms. ROS-LEHTINEN) to preside over the Committee of the Whole.

□ 1422

IN THE COMMITTEE OF THE WHOLE

Accordingly, the House resolved itself into the Committee of the Whole House on the state of the Union for the consideration of the bill (H.R. 624) to provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes, with Ms. ROS-LEHTINEN in the chair.

The Clerk read the title of the bill.

The CHAIR. Pursuant to the rule, the bill is considered read the first time.

The gentleman from Michigan (Mr. ROGERS) and the gentleman from Maryland (Mr. RUPPERSBERGER) each will control 30 minutes.

The Chair recognizes the gentleman from Michigan.

Mr. ROGERS of Michigan. I yield myself such time as I may consume.

I want to thank my ranking member and both the Republican and Democratic staffs and the Republican and Democratic members of the Intelligence Committee for 2 years of long hours in negotiated efforts to reach the point that we are.

I want to back up just a little bit and tell you how we got to where we are today. We sat down some 2 years ago when the ranking member and I assumed the leadership of the Intelligence Committee and we looked at the one threat that we knew existed but we were not prepared to handle as Americans, both the private sector and the government. And we knew that we had to do something about this new and growing and misunderstood cyber threat and what it was doing to our intellectual property across the country, what it was doing to the freedom and open Internet that we so enjoy and are increasingly dependent on and the commercial value of our growing economy. And it was at risk. The private sector was at risk because people were stealing their identities, their accounts, their intellectual property, and subsequent to that, their jobs, and people began to question the value of getting on the Internet and using it for commercial purposes. Their trust in the free and open Internet the way we've embraced it in the United States really was at risk.

How do we solve that problem? We knew that nation states were investing millions and billions of dollars to generate cyber warriors to go in and crack your computer network. I don't care if you had intellectual property—those blueprints that made your business successful, or maybe it was your bank account, or your ability to have a transaction. If they could interrupt that, they could do great harm to our economy and to the United States.

We saw nation-states like Russia and China and now Iran and North Korea and others developing military-style attacks to actually do harm to the U.S. economy, to hurt the very men and women who get up every day and play by the rules and think that the Internet would be a safe place for them to interact when it comes to commerce. We want that to continue.

So we sat down and we talked to industry folks, people who are in the business, high-tech industry folks from Silicon Valley, financial services folks from New York City, manufacturers from across the Midwest, who were losing intellectual property due to theft from nation-states like China. We talked to privacy groups. We talked to the executive branch. And over the last 2 years, there were some 19 adjustments to this bill on privacy.

We believe this: this bill will not work if Americans don't have confidence that it will protect your privacy and civil liberties while allowing one very simple thing to happen: cyber threat material, that malware that goes on your computer and does bad things, allows somebody else to take over your computer to attack a bank, allows them to go on your computer and steal your personally identifiable information and use it in a crime, allows them to go into your network at work and steal your most valuable company secrets that keep you alive and build great products here in the United States—could we allow the government to share what they know with the private sector and allow the private sector to share when it comes to just that cyber threat, those zeros and ones in a pattern that equates to malicious code traveling at hundreds of millions of times a second the speed of light, can we share that in a way to stop them from getting in and stealing your private information?

And the good news is the answer is, yes, we can do this. We can protect privacy and civil liberties, and we can allow this sharing arrangement, but not of your identity, not of your personally identifiable information. As a matter of fact, if that's what's happening, it won't work. But at the speed of light, from machine to machine, from your Internet service provider before it ever gets into your network they bounce out the nastiest stuff that's in there that's going to take over your computer, steal your money, steal your personally identifiable information, steal your company secrets. And they can identify that by a pattern and kick it out. They'll say, Something looks bad about that. Can the government take a look at that and say, you know what? This is a Chinese attack, it's an Iranian attack, it's a North Korean attack—let's defend our networks. It's really very simple.

Today, what you see is a collaborative effort. This isn't a bill by DUTCH RUPPERSBERGER and MIKE ROGERS and this is the only way it has to be. We have taken suggestions from all the groups I just talked about, from privacy to the executive branch to industry to other trade associations. And this is the bill that mutually all of those people, representing tens of millions of employees around this country, said this is the way you do this and protect the free and open Internet and you protect civil liberties. And you finally raise that big red sign that tells people like China and Iran and Russia, stop. We're going to prevent you from stealing America's prosperity.

I heard a lot of debate earlier on the rule. I've heard a lot of misinformation. There are people who don't like it for whatever reason, maybe it's conviction, maybe it's politics, maybe it's political theater. And I have a feeling there's a little bit of all of that when they talk about this bill.

This bill does none of the things I've heard talked about in the rule—that