know, there is no place to see a game like Cameron.

Mr. Speaker, I ask my colleagues to join me today in recognizing the outstanding achievement of the 2015 Duke University men's basketball team and Coach Mike Krzyzewski on winning the 2015 NCAA Tournament championship.

DEBT-FREE COLLEGE

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

Mr. GALLEGO. Mr. Speaker, a college education should be accessible to all Americans.

Currently, 40 million Americans have student loans, with an average balance of $29,000. This impacts our entire economy, as it prevents young people from buying homes, starting a family, and even buying a car.

Mr. Speaker, we provide a high school education for all students because we recognize the advantages for our children and our society of having a good education.

But a high school education is no longer enough if you want to get a good-paying job. A college education is necessary and essential in today's society in order to move ahead. It is an essential step to getting a good-paying job and joining the middle class.

Mr. Speaker, we are stacking the deck against our young people. The cost of higher education is through the roof, and student loans are weighing on our youth at one of the most vulnerable points in their lives.

Mr. Speaker, our parents and grandparents didn't have to take on this level of debt just to get an education. It is our responsibility to ensure that future generations have the same opportunities that our parents and grandparents had to access higher education without the burdensome student loan debt that we now carry.

VACCINATE YOUR CHILDREN

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

Mr. COHEN. Mr. Speaker, there was a story in today's Washington Post about the Salk vaccine being approved for usage in this country 50 years ago, on April 12, 1955. There was a picture of a second-grade student getting a shot as a test case in 1954. It brought back memories to me that I wanted to relate here.

My father was a physician. In 1954, he gave shots to second-grade children as part of the testing of the Salk vaccine. I had a brother in the second grade. My father gave him the shot that he gave all other second-graders.

I was in kindergarten. My father's mission was not to give shots beyond the second grade. So while the vaccine was in my home, he thought about giving it to me but didn't.

In the spring of 1954, I came down with polio. My father never forgave himself for not giving me that vaccination. I have suffered for it ever since and will continue for the rest of my life.

I relate this story to tell the American people: Vaccinate your children. Don't listen to the hysteria. Science has given us ways to stop children from getting diseases that have threatened society for generations. Do vaccinate. It is safe.

ANNIVERSARY OF ARMENIAN GENOCIDE

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

Mr. POLIS. Mr. Speaker, I rise today in solemn recognition of the 100-year anniversary of the genocide of over 1 million Armenians at the hands of the Ottoman Turks.

The Armenian genocide began April 24, 1915, when 250 Armenian intellectuals and community leaders were arrested. By 1918, between 800,000 and 1.5 million Armenians had disappeared, been killed through massacres, or subjected to forced labor and death marches in the desert.

The Armenian genocide joins other great human tragedies of the 20th century, including the Holocaust perpetuated by Nazi Germany against Jews, Gypsies, homosexuals, Christians, and political opponents; the massacre of the Tutsis in the Rwandan genocide; the Khmer Rouge; and Joseph Stalin's mass murders.

I rise today to remember those whose lives perished in the Armenian genocide and to recognize the Armenian Americans in their ongoing quest to ensure that those who perished are remembered for their loss of life in one of the most tragic genocides of the 20th century.

PROVIDING FOR CONSIDERATION OF H.R. 1560, PROTECTING CYBER NETWORKS ACT, AND PROVIDING FOR CONSIDERATION OF H.R. 1731, NATIONAL CYBERSECURITY PROTECTION ADVANCEMENT ACT OF 2015

Mr. COLLINS of Georgia. Mr. Speaker, by direction of the Committee on Rules, I call up House Resolution 212 and ask for its immediate consideration.

The Clerk read the resolution, as follows:

H. RES. 212

Resolved, That at any time after 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. 1560) to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, 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. It shall be in order to consider as an original bill for the purpose of amendment under the five-minute rule the amendment in the nature of a substitute recommended by the Permanent Select Committee on Intelligence now printed in the bill. The committee amendment in the nature of a substitute shall be considered as read. All points of order against the committee amendment in the nature of a substitute are waived. No amendment to the committee amendment in the nature of a substitute shall be in order except those printed in part A of 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 committee amendment in the nature of a substitute. 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.

SEC. 2. At any time after 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. 1731) to amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections, 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 amendments specified in this section and shall not exceed one hour equally divided and controlled by the chair and ranking minority member of the Committee on Homeland Security. 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 Committee on Homeland Security 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 114-12. 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 part B of 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.

SEC. 3. (a) In the engrossment of H.R. 1560 the Clerk shall—

(1) add the text of H.R. 1731, as passed by the House, as new matter at the end of H.R. 1560;

(2) conform the title of H.R. 1560 to reflect the addition of H.R. 1731, as passed by the House, to the engrossment;

(3) assign appropriate designations to provisions within the engrossment; and

(4) conform cross-references and provisions for short titles within the engrossment.

(b) Upon the addition of the text of H.R. 1731, as passed by the House, to the engrossment of H.R. 1560, H.R. 1731 shall be laid on the table.

□ 1230

The SPEAKER pro tempore. The gentleman from Georgia (Mr. COLLINS) is recognized for 1 hour.

Mr. COLLINS of Georgia. Mr. Speaker, for the purpose of debate only, I yield the customary 30 minutes to the gentleman from Colorado (Mr. POLIS), 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. COLLINS of Georgia. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and to include extraneous materials on H. Res. 212, currently under consideration.

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

There was no objection.

Mr. COLLINS of Georgia. Mr. Speaker, I am pleased to bring this rule forward on behalf of the Rules Committee. It is a rule that respects the legislative process and reflects the responsibility of Congress to address a critical deficit in the infrastructure of our Nation.

This rule provides for consideration of both cybersecurity measures under a structured amendment process. As a result of a thorough and deliberative committee hearing yesterday evening, there are five amendments to H.R. 1560 and 11 amendments to H.R. 1731 that this body will have the opportunity to debate and ultimately vote for or against.

The bipartisan nature of these bills speaks to the critical need for this legislation. Both bills passed their respective committees with bipartisan support, and I am hopeful this rule will enjoy similar overwhelming support.

For each bill, amendments offered by Democrats exceeded those offered by Republicans. I would like to thank Chairman NUNES and also Chairman MCCAUL for their work, both within our conference and across the aisle, to ultimately bring forward two bills that reflect compromise, consistency, and a deep understanding of the dangers that cyber attacks pose every day.

If both bills are adopted, this rule combines the bills and sends them to the Senate as a package in an effort to work with the other Chamber, go to conference, and to produce a product that will be signed into law. This is a fair rule that respects this body, the importance of this issue, and the legislative process as a whole.

The world has changed greatly since this body last discussed cybersecurity. The ''Internet of Things'' has created unforeseen risks and exposed vulnerabilities and defects in the ability of companies to even simply talk to each other without fear of frivolous litigation.

Our enemy is adapting, growing bolder and more sophisticated. North Korea, Iran, Russia, and China seek to exploit and devastate our economic security as a nation and our data security as individuals through cyber attacks that we cannot adequately anticipate, respond, or even communicate about.

Foreign governments aren't the only ones who wish to do Americans harm. Terrorists and criminal enterprises have also recognized that American companies are crippled by the ambiguity in our law as it relates to sharing cyber threat information.

The cyber attack surface has expanded. Wearables, connected vehicles, and embedded devices have made it possible for cyber attacks to literally be driven into the parking lot or walked through doors.

The traditional ways of responding to cyber threats and recovering from them are not sufficient to safeguard the data privacy of Americans and the economic security of our Nation. The scope of these attacks and devastating damages are increasing as rapidly as the attackers are themselves.

These bills are not a magic pill. They will not render inoperable the scores of foreign countries and enterprises that want to see American exceptionalism brought to its knees; but they do give clear, positive legal authority to American companies to allow them to protect their own and to appropriately share cyber threats with other countries and, in certain cases, Federal agencies.

Let me be clear. These are not surveillance bills. These are not data collection bills. This is not the PATRIOT Act or FISA. This body will debate intelligence gathering, collecting, sharing, and using at some point in the future, but today is not that day.

I know those rightly concerned with government surveillance, like myself, would like to use this rule for that purpose and the underlying measures as a platform to debate that, but I urge them to refrain. We will have that debate.

Today's focus is on the perpetrating of the thousands of cyber threats American businesses face every single day. Let the attention be on North Korea. Let it be on Iran. Let it be on the countless enemies of the United States who want to destroy this Nation. For today, we speak with a united voice that they will fail.

We declare with one voice that American companies have the right to protect their own, to protect and defend their own networks, to share technical information with the appropriate agencies on a voluntary basis if they so choose.

I thank the Intelligence and Homeland Security Committees and their staff for their tireless work they have done to ensure that we can protect our economy, our infrastructure, and our private information.

I know detractors of the legislation may attempt to paint this rule and underlying measures in a different light, so let's allow the facts to speak for themselves.

These bills have three key components. First, they provide for completely voluntary participation by private companies in a program with positive legal authority. This program allows three kinds of sharing—private company to private company, government to private company, and private company to government—but this sharing of information is limited only to cyber threat indicators.

Second, they require the removal of all unrelated personal information. It is the technical cyber threat information that is being shared, zeros and ones. In fact, there is a requirement that both the government and the private entity remove personally identifiable information when the information is shared and also when it is received.

Third, the legislation expressly prohibits the cyber threat indicators from being used for surveillance.

These bills will benefit all Americans by helping businesses better protect sensitive information. Attacks against our network often seek to steal Americans' personal information. This can include credit and debit card information, medical records, or even Social Security numbers.

Many of the recent attacks that we have all read about in the news were specifically aimed at stealing the personal information of Americans. Cyber attackers are also increasingly targeting small businesses. In fact, in 2014, 60 percent of all targeted attacks struck at small- and medium-sized businesses.

The underlying legislation will also help protect American jobs by protecting the intellectual property of American businesses. It is estimated that cyber attacks cost Americans roughly 500,000 jobs a year. Foreign companies often use cyber attacks to target the trade secrets of U.S. companies and then use the information to produce their own competing product.

The threat is real, both to our economic security as a nation and our personal information as individuals. If we fail to act and pass this rule and the underlying bills, our Nation and our personal privacy is more at risk than ever before.

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

Mr. POLIS. Mr. Speaker, I thank the gentleman from Georgia for yielding me the customary 30 minutes, and I yield myself such time as I may consume.

Mr. Speaker, I rise in opposition to the rule and the underlying legislation.

Today, the House is convening to debate a matter that we all agree is critical for our national security, our economic competitiveness, our prosperity, and the success of our private sector.

The recent cyber attacks on Sony and Anthem are but two prominent examples of cases in which American businesses or government entities have come under attack by hackers, among many other instances that haven't even been reported.

I want to recognize the work that the House Intelligence and Homeland Security Committees did on these pieces of legislation and their attempts to address these issues. Unfortunately, in spite of their hard work and the work of those that went into crafting these two bills, I regret that they fall short of their goals and would likely do more harm than good.

Not only do both bills, particularly the Protecting Cyber Networks Act, raise enormous concerns about inappropriate sharing of personal information and surveillance on Americans' private lives, but they are built on the premise that many security experts have warned is fundamentally flawed, that sharing information with the Federal Government should be the central focus of our efforts to protect American cyber networks, rather than simply one aspect to a multipronged strategy to defeat hackers, foreign and domestic.

Now, before I address the substance of these two bills, I want to discuss this unusual rule before us and how it treats two bills which contradict each other in significant ways.

Ordinarily, when two committees share jurisdiction over a matter—in this case, the Homeland Security Committee and the Intelligence Committee—they collaborate. One committee handles one portion of the bill, reports it out; the other committee handles the other portion, reports it out, and they work together to bring a single piece of legislation to the floor for Members to debate, amend, and vote for or against.

This is what happened, for example, with the recent SGR repeal legislation, which had components under the jurisdiction of no less than six different committees in this body, but was presented before us as a single bill.

In this case, however, because there seems to be some kind of turf war between the Intelligence Committee and the Homeland Security Committee, we are actually voting on two overlapping bills that, in several respects, contradict one another.

For instance, the bills have drastically different determinations of what kind of information may be shared, what purposes the government may use the information for, and what hacking countermeasures companies are allowed to take to protect their networks.

Instead of having a meaningful debate on the merits of each bill's approach, this body, if this rule passes, would forego that, and we would simply debate and vote on each bill separately, and if they both pass, the rule directs the Clerk to mesh them together through something called conforming amendments.

Not only would this leave businesses to wade their way through two separate, contradictory regulatory schemes, but it leaves it unclear which bill's provisions would actually prevail in practice and under which circumstances. It actually would create more uncertainty in the marketplace, rather than less.

I don't think anybody could reasonably call this an open process. We shouldn't be depriving our constituents of an open debate on important issues. The major amendments of this bill that would have restored privacy, many of which I was a cosponsor, are not even allowed to be debated on the floor of the House, not for 10 minutes, not for 5 minutes, not even for 1 minute.

My colleagues and I on both sides of the aisle are being denied a vote on the very amendments that we feel could address the concerns we have with the cybersecurity legislation and make sure that we keep American networks safe.

Mr. Speaker, in the 2 years since the NSA's shockingly broad data collection program PRISM came to light, we have heard from many of our constituents. The American people want an end to unwarranted surveillance. They want Congress to restore desperately needed accountability and transparency to our Nation's often out-of-control intelligence-gathering apparatus.

It is bewildering to many people that, at the very time the American people have spoken out that we want more safeguards, instead, we are bringing forward two bills whose central objective is to facilitate the flow of more personal information to the Federal Government, when we continue to put off the question of surveillance reform and bringing an end to the NSA's bulk data collection without warrants.

It is especially disappointing in light of the fact that several PATRIOT Act provisions will sunset at the end of next month, giving Congress a crucial opportunity to reexamine and rein in Federal surveillance programs.

By putting off that issue and bringing mass information sharing to the floor, Congress is asking the American people for a blank check. Congress is saying: Trust the President. No President would allow this information sharing to infringe on your civil liberties, even though we have utterly failed to pass a single piece of legislation to end the privacy abuses that we know have occurred under this administration and the prior administration.

The problem with these bills is that they go far beyond, and they open up additional loopholes and potential abuses with regard to privacy abuses, particularly H.R. 1560, the so-called Protecting Cyber Networks Act. Both bills open up Americans' private information to inappropriate scrutiny by the Federal Government.

Now, I expect we will hear proponents of both bills argue at length that the protections against sharing personal information are sufficiently robust.

For instance, under both bills, they will cite that cyber threat data is scrubbed twice for personal information, once by private entities before they transmit it to the government and once by government entities before they store the information or share it with anybody else.

Now, that sounds good, but, unfortunately, the devil is in the details, and a close reading of the bill shows that there is an enormous loophole in the information-scrubbing component and that it fails to offer Americans safeguards for the personal information.

□ 1245

Under both bills, any Federal entity in receipt of cyber data threat information may store and share personal information it receives—unscrubbed information—if they believe that it is related to a cybersecurity threat.

Now, this standard isn't too vague, considering that information ''related'' to a cybersecurity threat could be interpreted to mean just about anything, but it is also incredibly broad. It includes an implicit assumption that Americans' personal information should be shared, unless Federal officials have information that it is not related to a cybersecurity threat. In many cases, the burden is to show that the personal information is not related to a cybersecurity threat for it to be scrubbed, rather than the other way around.

So, yes, companies and Federal entities are required to scrub the data for information that can be used to identify a specific person. But the loophole then calls on them not to remove any personally identifiable information unless they can show that it is not related to cybersecurity. Even if there is an off chance that something at some point might be pertinent to some kind of investigation, it puts Americans' personal information—without warrants, without due process, including information about patterns of Internet use, location, content of online communications—at great risk.

We have seen before that the Federal Government has a poor track record of

safeguarding our personal information when they are entrusted with it. The last thing we should be doing is empowering Federal agencies even more with a broad discretion to look at personal information unless there is clear evidence that doing so would combat a cybersecurity threat.

I introduced, along with my colleagues on both sides of the aisle, a number of amendments to both bills—one with the gentlewoman from California, Representative ZOE LOFGREN, and one with Representative ZOE LOFGREN and the gentleman from Michigan, Representative JUSTIN AMASH—to impose a higher standard on Federal entities who are entrusted with this personal information. Our proposal would simply require the Federal Government to remove personally identifiable information unless it is directly necessary to identify or mitigate a cybersecurity threat—the purported purpose of this bill.

These amendments would have imposed no additional burdens on private companies, but they would have given our Nation's technology companies and the customers who keep them globally competitive more confidence that private information shared under these bills would not be subjected to inappropriate mass scrutiny by the government.

Sadly, our amendments met the same fate as nearly two dozen others put forth to add in important privacy safeguards.

The potential for abuse of private information under H.R. 1560 is even more far-reaching. The Homeland Security bill at least makes clear that the information companies transmit to DHS should be shared specifically with other agencies that need it to protect critical infrastructure. But the circumstances under which information can be shared under the Intelligence bill—and who it can be shared with—are fuzzier and broader.

Under the approach taken by H.R. 1560, every cyber threat indicator shared with a civilian agency of the Federal Government is immediately shared with a host of other government agencies, including the NSA. This increases the threat to cybersecurity by having repositories of information replicated across numerous government agencies, creating additional avenues for attack by malicious hackers. That means that private sector companies will not be able to participate in the program and promise their users they will not share information with NSA or other government agencies unless required by law.

Furthermore, it is true that the Homeland Security bill includes some troubling provisions that allow the government to use cybersecurity threat information for criminal investigations unrelated to cybersecurity. Fortunately, the Rules Committee made in order an amendment by Representatives JOHN KATKO, ZOE LOFGREN, and ANNA ESHOO that would address this problem in the Homeland Security bill. I hope that my colleagues adopt this amendment.

Unfortunately, no such amendment is being considered to address this issue within the Intelligence bill, H.R. 1560, where the problem actually runs much deeper. H.R. 1560 permits cyber threat data, including Americans' private information, that is shared with the Federal Government to be stored and used for a raft of unrelated purposes, unconstrained by congressional directive, including investigations and potential prosecution of crimes completely unrelated to cybersecurity.

Obviously, all of us want law enforcement agencies to be equipped to prevent and prosecute violent crime, but the inclusion of these matters completely unrelated to cybersecurity broadens the scope of the measure far beyond what it is purported to be: a cybersecurity bill. In fact, it reduces the focus of our efforts on combating cybersecurity when you open it up to everything under the sun.

By including a vast array of other reasons the government can invoke to store and share personal information, the authors of the bill essentially transformed the information-sharing initiative into a broad new surveillance program.

Yes. Rather than a cybersecurity measure, effectively, these bills are a stalking horse for broad new surveillance authority by multiple agencies of the Federal Government without warrants, without oversight.

H.R. 1560 empowers Federal entities to hold onto any information about an individual that may be ''related to'' any of the many law enforcement purposes lumped into the bill. That gives the Federal Government enormous incentive to retain and scrutinize personal information, even if it is unrelated to a cybersecurity threat.

The scope of the use authorizations also undermines due process protections that exist to protect Americans against unwarranted search and seizure. Private information about a person that was transmitted warrantlessly to the NSA under a program that was purportedly designed to combat hackers should not be admissible or used in court against them on an unrelated offense—not related to cybersecurity, not related to hacking. It would render all of our due process protections invalid simply because of the medium of the information that is used with regard to these matters in this case: Internet and cyber-related mediums and communications through them.

I joined Representatives ZOE LOFGREN, DARRELL ISSA, and BLAKE FARENTHOLD on an amendment to make clear that information sharing may only be used for the purpose of mitigating cybersecurity threats, again, the purported purpose of this bill. If the proponents of this bill are serious about combating cybersecurity, why did the Rules Committee deny Members the opportunity to limit the provisions of this bill to cybersecurity rather than a whole host of unrelated offenses?

I also joined the gentleman from Kansas, Representative KEVIN YODER, to sponsor an amendment to address a longstanding due process issue that has plagued our Nation's legal system and our privacy rights.

While the government is required to get a warrant if it wants to search through a person's physical mail, it is not required to get a warrant to search through somebody's old emails, provided the emails are older than 6 months. That contradiction and loophole was based on a 1986 law that was written before most people knew what email was.

Representative YODER and I sponsor a bipartisan bill that has 261 cosponsors, and yet when we offered a provision on this bill, we were not given a chance to vote on it and pass it in spite of the grave due process implications that the underlying legislation has.

In addition to these privacy and due process concerns, I am alarmed by the prospect that H.R. 1560 will actually invite attempts by both private and public entities to deliberately weaken the integrity of software systems in the name of cybersecurity.

H.R. 1560, for instance, authorizes companies to deploy countermeasures that are called defensive measures in the form of hack backs that would otherwise be illegal. A countermeasure operated on one network should never cause harm to another that is prohibited by the Federal antihacking statute, the Computer Fraud and Abuse Act. But that is precisely what can happen when a company places malware on its own network, because if that data gets stolen along with other valuable data, it can harm or lead to unauthorized or backdoor access of other proprietary networks or information.

The gentleman from Virginia, Representative GERRY CONNOLLY, put forward two amendments to address this issue in a very thoughtful manner. Regrettably, neither one will be allowed to be debated or receive a vote on the floor of the House unless we can defeat this rule.

Furthermore, both bills present the risk that Federal entities will use the threat information they receive from private companies to circumvent the security protections safeguarding those same private companies' information systems, effectively creating their own back doors which could later be exploited by malicious hackers.

As a matter of routine, our intelligence apparatus already demands that private companies include defects in their encryption system for the purported purpose of conducting backdoor surveillance. Today's legislation only makes it easier for the NSA to find and exploit more of these back doors and, therefore, easier—not harder—for hackers to find and exploit these very same security weaknesses.

Once again, Representative LOFGREN put forward an amendment that would actually improve cybersecurity by making it clear that Federal entities could not use data obtained through information sharing to demand that private entities create new encryption weaknesses to enable backdoor hacking. Sadly, once again, her amendment will not be heard on the floor of the House, and this bill will encourage and allow additional venues for the illicit hacking it purports to combat.

Mr. Speaker, I don't doubt the intentions and the goals of my colleagues on the Intelligence and Homeland Security Committees, but these bills simply represent a step backwards rather than a step forward, present risks on too many fronts, from privacy, to due process, to the threats that they add to the integrity of the very networks that these bills are designed to safeguard.

In addition, the bills' focus on information sharing negates an important conversation about more important mechanisms Congress should be looking at to protect cyber systems, mechanisms that are not as fraught with risks to our civil liberties and are more effective at protecting our networks. We should be doing more, for instance, to educate businesses and governments about basic network security.

Even here in Congress, we have seen evidence of how woefully lacking even elementary knowledge about cyber threats is. Helping businesses prevent cyber attacks doesn't have to mean that the government vacuums up endless amounts of personal data about how individual Americans are using the Internet and their personal communications.

In fact, if we stop allowing the NSA to demand that U.S. businesses deliberately weaken their own networks for the purpose of government surveillance, that, in itself, would be a big step forward to strengthening our national cybersecurity.

Sadly, today's rule doesn't even allow for a debate or for a vote on the most significant concerns surrounding this legislation and denies Members the opportunity to consider changes that would address the issues that we have raised and improve cybersecurity under this bill. For these reasons, I hope my colleagues join me in opposing the rule and the underlying legislation.

I reserve the balance of my time.

Mr. COLLINS of Georgia. Mr. Speaker, again, I want to focus this debate. There are many things my friend from Colorado brought up that will be debated, that are coming up, I think, as early, frankly, as tomorrow in some committees and will be debated on this floor. This is about sharing. This is about information protection.

And with that, I am pleased to yield 3 minutes to the distinguished gentleman from New York (Mr. KING), who is a member of both the Homeland Security and the Intelligence Committees. He is the chairman of the Homeland Subcommittee on Counterterrorism, and he is also the former chairman of the full committee.

Mr. KING of New York. I thank the gentleman for yielding.

Mr. Speaker, I rise in strong support of the rule and also of the underlying bills, H.R. 1731 and H.R. 1560.

As was pointed out, I am the only Member of Congress who is on the Homeland Security Committee and the Intelligence Committee; and I was able to both take part and also to observe closely the extent to which the gentleman from Texas, Chairman MCCAUL, and the gentleman from California, Chairman NUNES, worked with Members on both sides of the aisle, worked with privacy groups, worked with Federal officials, government officials, and administration officials to try to make this as bipartisan a bill as possible, to ensure that privacy would be protected, but also to ensure that everything possible can be done to protect our Nation against cyber intrusions.

Now, every day there are attacks upon our infrastructure. The critical infrastructure—mostly in private hands—is being targeted; and Federal networks, databases that are vital to our national security, are under assault every second of every day.

Cyberterrorism, whether it is carried out by a nation-state, such as Iran or Russia or China, or carried out by terrorist organizations, such as ISIS or al Qaeda, is extremely damaging and threatening to our national security; and it is essential that we, especially since so much of our critical infrastructure is in the hands of the private sector, allow for sharing, that we allow companies to share information with the government, that there is mutual sharing with the government, with the private sector, so that these companies can do it without fear of being sued, without fear of liability—they act in good faith; they do what has to be done.

Every measure that was put in there—I know the gentleman from Colorado disagrees, but every measure is in there to ensure that individual rights will not be violated, that privacy will not be violated. And again, we have to look at, for instance, if the gentleman from Colorado is wrong, what this could mean to our country, how this could devastate—devastate—our infrastructure, devastate our national security, devastate our financial system.

So again, this was not something that was rushed into. And when you have both bills passing out of committee with, as far as I recall, not one dissenting vote—not that everyone was in full agreement with the bills. But the fact is this is probably as close to a consensus as you can come in the Halls of Congress on such a critical and, in some ways, such a controversial issue, to find that type of unanimity on the two committees that deal with this most significantly.

□ 1300

H.R. 1731 is the Homeland Security Committee bill that allows this information to be shared. The port will be the Department of Homeland Security, and that was done, again, working with privacy groups and working with those who are concerned with civil liberties, at the same time working with those who realize how absolutely essential to our security passage of this legislation is and how we have to have this type of cooperation, this type of sharing, this information sharing, and being done with the government and with the private sector working together to combat these enemies which can come at us from all directions. Again, every second of every day these attacks are being attempted and carried out.

That is the crisis that faces us as a nation. It is not as obvious as a bomb going off in Times Square, and it is not as obvious as a bomb going off at the Boston Marathon, but it is just as critical.

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

Mr. COLLINS of Georgia. Mr. Speaker, I yield the gentleman an additional 1 minute.

Mr. KING of New York. It is just as critical and just as vital, in some ways more so, in that the ultimate result could be so devastating to our Nation.

So, Mr. Speaker, I would ask, again, passage of the rule, which I believe is obviously essential, but also passage of the underlying bills because, again, our Congress has been criticized, with some validity, for not being able to work together and for not being able to get things done. But to have such a vital, controversial issue as this, to have both committees who deal with it most closely, to have them come together, all the effort and work that went into it, to have them come together to come up with this package of legislation, this shows Congress works. It shows we take this issue seriously, and it means we are going to go forward in all we can to combat terrorism in all its forms. Right now, probably the most lethal are the cybersecurity attacks being made on us.

Mr. Speaker, I urge strong support of the rule and the underlying bill.

Mr. POLIS. Mr. Speaker, I would just add that demanding that private companies deliberately include defects in their own encryption systems for the purpose of allowing the NSA to conduct backdoor surveillance only increases the risk of our cybersecurity networks rather than decreases it, which is exactly what the bill does.

Mr. Speaker, I yield 2 minutes to the distinguished gentleman from Mississippi (Mr. THOMPSON), the ranking member of the Committee on Homeland Security.

Mr. THOMPSON of Mississippi. Mr. Speaker, I thank the gentleman from Colorado for yielding the time.

Mr. Speaker, though I support H.R. 1731, the National Cybersecurity Protection Advancement Act, as approved by voice vote in my committee, I rise to express my disappointment with the rule.

Yesterday the White House announced support for House passage of H.R. 1731 but said that ''improvements to the bill are needed to ensure that its liability protections are appropriately targeted to encourage responsible cybersecurity practices.'' The White House was referring to the language that was inserted at the direction of the Judiciary majority.

Instead of providing a targeted safe harbor for companies to share timely cyber threat information, it establishes an unduly complicated legal framework that runs the risk of providing liability relief to companies that act negligently. Moreover, it explicitly immunizes companies from not acting on timely cyber information. This language runs counter to the fundamental goal of the legislation: to get companies timely, actionable information to use to protect their networks.

Yet when H.R. 1731 is considered tomorrow, Members will not be allowed to vote on a single amendment to fix the liability provision that the White House has called ''sweeping'' and said may weaken cybersecurity overall. Remarkably, none of the seven amendments that were filed to fix it are being allowed.

I would also like to register my disappointment that the rule calls for H.R. 1731, upon passage, to be attached to the Intelligence Committee bill. From my conversation with Members, I know that there is a great deal of support for authorizing cyber information sharing with the Federal civilian lead, the Department of Homeland Security. As such, I would argue that the rule should have called for H.R. 1560 to be folded into our bill.

Mr. COLLINS of Georgia. At this point, Mr. Speaker, I am pleased to yield 1 minute to the distinguished gentleman from California (Mr. ISSA), the chairman of the Judiciary Committee's Subcommittee on Courts, Intellectual Property, and the Internet.

Mr. ISSA. Mr. Speaker, I thank the gentleman.

Mr. Speaker, I will be supporting the rule, but not without trepidation. I will be opposing the underlying bill, but not without regret. The underlying bill could have done what we wanted it to do. It could have allowed for the exchange of information while protecting individuals' privacy. It could have limited that information to preventing a cyberterrorist attack. But, in fact, amendments that were offered on a bipartisan basis, a number of them, that could have limited this would have, in fact, allowed us to have the confidence that this information would be used only for what it was intended.

Mr. Speaker, since 9/11, the government has begun to know more and more about what we are doing, who we are, where we live, where we sleep, whom we love, whom we do business with, and where we travel. And we have known less and less. Just a few days ago, the Ninth Circuit in northern California had to rule that the government had to turn over information in a usable format. It took a Federal court order to do so.

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

Mr. COLLINS of Georgia. Mr. Speaker, I yield the gentleman an additional 1 minute.

Mr. ISSA. I thank the gentleman.

Mr. Speaker, this bill should mandate our knowing more and the government not knowing. It should have ensured that the government only had what it needed. It should have protected private companies who wanted to exchange appropriate information between each other. It should not have created a vast treasure trove here in Washington or somewhere in the hinterland where the government now and in the future can dig in for any purpose—criminal background investigations or perhaps simply checking to see if you paid your taxes. The fact is, this is a data vault that is not narrowly construed, and, therefore, sadly, without the amendments that were not allowed, I am not in a position to vote for this bill. I thank the chairman, and I thank Mr. POLIS for his kind remarks also.

Mr. POLIS. Mr. Speaker, if we defeat the previous question, we will offer an amendment to the rule that will allow the House to consider the Department of Veterans Affairs Cybersecurity Protection Act.

Mr. Speaker, I yield 2 minutes to the gentlewoman from Arizona (Mrs. KIRKPATRICK) to discuss our proposal.

Mrs. KIRKPATRICK. Mr. Speaker, I thank my colleague for giving me a couple of minutes to talk about the importance of protecting our veterans from cyber attack.

Mr. Speaker, I rise in support of H.R. 1128, the Department of Veterans Affairs Cyber Security Protection Act. My bill will protect veterans' personal and sensitive information from cyber attacks without compromising the VA's ability to provide the health care, benefits, and services our veterans have earned.

This legislation will do primarily three things. First, it will require the VA to develop an information security strategic plan that protects current veterans' information and anticipates future cybersecurity threats. Second, it mandates a report on VA actions to hold employees accountable for data breaches. Third, it requires the VA to propose a reorganization of the VA's information-security infrastructure to protect veterans and provide greater levels of accountability and responsibility in the VA.

My bill will also require the VA to report employee violations of its policy and report any incidents involving the compromise of veterans' personal information by the VA or from outside cyber attacks.

Mr. Speaker, this bill is one commonsense way that we can hold the VA accountable and protect veterans' private and personal information from cyber threats, and I urge all of my colleagues to support H.R. 1128.

Mr. COLLINS of Georgia. Mr. Speaker, at this time I am pleased to yield 5 minutes to the gentleman from Georgia (Mr. CARTER), a member of the Homeland Security Committee and a colleague of mine from Georgia.

Mr. CARTER of Georgia. I thank the gentleman.

Mr. Speaker, national cybersecurity will be an issue this House will have to constantly address for the foreseeable future. To achieve a system that will protect our Nation's citizens and its infrastructure, we must create a public-private partnership between Federal agencies and American businesses. This partnership will allow Federal agencies and American businesses to share cyber threat information, vulnerabilities within our cyber network, and the creation of new systems to protect consumer information. However, private businesses need to be provided protections and incentives to ensure they are protected from government abuse and private legal proceedings meant to gain access to private security information.

Mr. Speaker, one of our top priorities with these two bills should be to clearly acknowledge protections given to companies that engage in penetration testing and clearly state that company proprietary information is protected from nefarious legal proceedings and exempted from Freedom of Information Act requests. It is reasonable to think that individuals would actively pursue this sort of proprietary information for the sole purpose of accessing the vulnerabilities of private cyber networks if we do not clearly state that this information is protected and exempt from those actions.

I believe we should consider these possibilities and ensure that protections are provided so our country and its citizens can fully benefit from these laws.

Mr. COLLINS of Georgia. Will the gentleman yield?

Mr. CARTER of Georgia. I yield to the gentleman.

Mr. COLLINS of Georgia. I want to thank my colleague from Georgia who sits on the Homeland Security Committee for his passion and his commitment to addressing these critical defects in the laws governing this voluntary sharing of cyber threat information. The legislation before us today is good policy reflective of the hard work of the committees on which you sit, Homeland Security and the Intelligence Committee, as well as input from a vast array of stakeholders. It is important to know that the legislation is supported by every sector of the economy.

As my friend so eloquently noted, the legislative process will rightly continue after these bills are considered by the full House this week and for years to come as we revisit and reassess the needs of Americans' privacy and also the laws governing cybersecurity.

Mr. Speaker, I agree with my friend that if there is a conference committee on this bill, we should encourage them to seek additional clarification language as needed to ensure that companies are appropriately incentivized to share cyber threat information.

I just want to say personally that I appreciate all the hard work that you have done on this issue bringing this forward and continuing to work for not only the companies in Georgia but across this Nation who depend on a safe and secure cyber network.

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

Mr. Speaker, it is ironic that on this very day, leaders on the Judiciary Committee will introduce legislation designed to reform and rein in the Federal Government's surveillance programs. I haven't had the opportunity to review those bills yet, so I can't speak to their merits. But I hope that if it is a strong bill, it will make its way through both Chambers and become law.

But, today, this body is considering a rule that would take us in the wrong direction. Recent history has shown that this body shares the American people's concerns that we don't take the threat of unwarranted surveillance seriously enough and that Congress needs to pass meaningful reforms that balance our liberties, our freedoms, and our privacy with the need to keep America safe.

Senate Majority Leader MITCH MCCONNELL introduced legislation yesterday that would extend the NSA's surveillance program without any of the reforms that many of us on both sides of the aisle have advocated to rein them in. This is despite the national outcry and, indeed, international embarrassment that has been counterproductive to the very American security goals that these provisions are designed to advance.

This makes me fear that Congress is not learning from the mistakes of the past, mistakes of overly broad surveillance authorities, but instead is about to repeat them. So before we approve faster, broader, and easier sharing of vast amounts of personal information from innocent Americans with the Federal Government, Congress should be taking up legislation to prove that we have the ability to curb abuse and the Federal Government's penchant for abusing its access to this kind of data.

So far Congress has not shown its aptitude for preventing this kind of abuse. Yet today we ask the American people to trust us, to trust the President, yet again, by opening up even more information to the NSA and other surveillance agencies.

Our experience with the NSA has shown us that to protect American civil liberties from an overzealous surveillance apparatus, the authorities to review and share Americans' personal information need to be construed as narrowly, as unambiguously, and as specifically as possible by the United States Congress. We need to limit very specifically to a specific set of circumstances under which sharing data and information is necessary for mitigating a security threat.

We offered to do that through bipartisan amendments, working with Representative LOFGREN, Representative ISSA, and others, but none of those amendments are allowed to be discussed or debated under this rule.

Both the Protecting Cyber Networks Act and the National Cybersecurity Protection Advancement Act fall well short of the standard—and in the case of the Protecting Cyber Networks Act can even be counterproductive and falls woefully short.

□ 1315

These pieces of legislation would enable Federal agencies to store and share Americans' private information, such as Internet usage patterns, even the content of online communications, based on a vague or broad standard that doing so is not unrelated to a cybersecurity threat.

Again, not affirmatively, they don't have to prove that it is related to a cybersecurity threat; the burden of proof is to show that it is not unrelated to a cybersecurity threat. How can you demonstrably show that about anything?

It would make it easier for government agencies to deliberately weaken software systems for the purpose of creating new surveillance back doors that foreign nation-states and hackers can presumably also exploit.

It would leave the door wide open to more NSA surveillance by allowing the sharing of personal information for a raft of purposes unrelated to cybersecurity. We can do better.

By rejecting this rule, Members of Congress will show that, yes, we take cybersecurity seriously, so seriously that we want to take the time to get it right. Whether that takes another week or 2 weeks or 3 weeks, getting it right means allowing Members of this body input into the formulation of the final bill meaningfully through the kinds of amendments that have been rejected outright under this rule without discussion, without debate, without a vote.

Unfortunately, the rule before us today denies us the ability to consider amendments that would have addressed many of the concerns with the bill.

Mr. Speaker, I ask unanimous consent to insert the text of the amendment in the RECORD, along with extraneous material, immediately prior to the vote on the previous question.

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

There was no objection.

Mr. POLIS. Mr. Speaker, I urge my colleagues on both sides of the aisle to vote ''no'' and defeat the previous question.

I urge a ''no'' vote on this bizarre rule that combines two, at times, contradictory bills and rejects bipartisan amendments that would have addressed the concerns that many of us have with the underlying legislation.

I urge a ''no'' vote on the previous question and the rule.

Mr. Speaker, I yield back the balance of my time.

Mr. COLLINS of Georgia. Mr. Speaker, I yield myself such time as I may consume.

As we move forward, I think one of the things—and there are many things that are going to be discussed, and I encourage all Members to vote for this rule. As we move into general debate, there will be a lot of discussion that talks about what we are moving forward; but, also, I want to bring forward that we are—as is seemingly not discussed bringing forth, there are amendments being brought forth on both of these bills.

There also were 20-something amendments in Homeland Security; there was also an amendment in Intelligence. These are vetted bills. This is a proper role with what we are doing in Congress in bringing these to the floor.

Are there times that someone may want others? Yes; but, at this point, we are going to have that debate here on the floor. That is why voting for this rule and moving this forward is the proper thing to do.

Before we also move back from this, I want to talk about this need and why we are here even to start with. Most Americans recognize and understand that the growing attacks against our cyber networks and critical infrastructure and our laws fail to provide proper legal authority for information regarding cyber threats to be shared.

In fact, when I am back home in the Ninth District of Georgia discussing this, most people don't realize there is this barrier, and especially everything that is going on, they don't understand why some of these impediments were put into place that keeps companies from protecting their own, but also protecting their own personal information.

One of the things that is missing in this debate is the discussion of what has actually happened and the personal information that is shared by these hackers who are getting into our system.

Some of the latest attacks perpetrated by North Korea and other criminal enterprises on Sony Pictures and health insurance providers Anthem and Blue Cross Blue Shield speak to the type of attacks that occur on a daily basis that target the backbone of American business and the privacy of America's most sensitive data.

As we look to constrain this, as we look to put in proper safeguards, we have to realize that doing nothing exposes more and more of our American citizens to personal information being shared. If we don't believe it, just read the headlines from Sony, Anthem, and these others that have come out recently.

According to the Department of Homeland Security, in 2014 alone, they

received almost 100,000 cyber incident reports and detected 64,000 cyber vulnerabilities, and these numbers are just based on information given to DHS and does not reflect the full scope of the attacks on our Nation.

When we look at this and we talk about the personal information, the FBI Director James Comey said:

There are two kinds of big companies in the United States. There are those who have been hacked . . . and those who don't know they have been hacked.

A recent survey by the Ponemon Institute showed an average cost of a cyber crime for U.S. retail stores more than doubled from 2013 to an annual average of 8.6 million per company in 2014.

The annual average cost for a company of a successful cyber attack in 2014 increased to 20.8 million in financial services, 14.5 million in the technology sector, and 12.7 million in the communications industry.

The scope of many attacks are not fully known. For example, in July of 2014, the U.S. Computer Emergency Readiness Team issued an advisory that more than 1,000 U.S. businesses have been affected by the Backoff malware, which targets point-of-sale systems used by most retail industries. These attacks targeted administrative and customer data and, in many cases, financial data. Most companies encounter multiple cyber attacks every day, many unknown to the public and many unknown to the companies themselves even.

Again, as we look back over the attacks of just the past year, Target announced an additional 70 million individual contact information was taken during the December 2013 breach in which 40 million customers' credit and debit information was stolen.

Between May 2013 and January 2014, the payment cards of 2.6 million Michaels customers were affected. Attackers targeted the Michaels POS system to gain access to their systems.

The email service Yahoo! Mail was reportedly hacked in for 273 million users, although the specific number of accounts affected was not released.

For 2 weeks, AT&T was hacked from the inside by personnel who accessed user information, including Social Security information.

Foreign nationals from China have been indicted for computer hacking and economic espionage. We have seen these attacks all over the board.

Looking at this, the real issue that comes to mind is if we sit back and are not productive and not proactive as the Intelligence Committee and the Homeland Security Committee have been here, we are putting in danger more personal information being exposed in ways that no American needs to have their personal information exposed and are being targeted in the process.

This is good legislation that needs to stay on the floor, and that is why we are here today to support this rule and to look forward to that debate that has already happened and will continue to happen.

I appreciate the discussion we have had over the past hour. Although we may have some differences, our unity should be clear against the cyber attacks and our resolve to prevent them and show their success is strong.

This rule provides for ample debate on the floor, the opportunity to debate and to vote on 16 amendments, and a smooth and deliberative process for sending one bill to the Senate. These bills will help protect American consumers, jobs, and small businesses.

Allowing companies, again, to voluntarily share cyber threat indicators with other companies and government agencies will help bring awareness to new threats and vulnerabilities.

If businesses can learn about a new threat from another business or from the government before they are targeted themselves, they can better act to protect their customers' personal information from a similar attack.

I would like to thank Intel, Homeland Security, Judiciary, and Rules Committee members and staff for the thoughtful and involved processes that have brought us to this point.

I urge my colleagues to support the rule and these two cybersecurity bills.

Ms. JACKSON LEE. Mr. Speaker, I rise to speak on the Rule governing debate on H.R. 1731 and H.R. 1560.

I support the Rule for H.R. 1731 and H.R. 1569 because it: 1. provides for consideration of important improvements to both bills; 2. makes clear the role of the Department of Homeland Security in securing civil government networks; and 3. the responsibilities of DHS in assist private sector entities in improving overall cybersecurity for themselves and their customers.

The bipartisan process that the Homeland Security Committee followed through the leadership of Chairman MCCAUL and Ranking Member THOMPSON is an example of what can be accomplished when partisanship is removed from the policymaking equation.

I would also like to thank Chairman SESSIONS and Ranking Member SLAUGHTER as well as members of the Rules Committee for making 4 of my amendments in order.

I join my colleagues in the work to secure our nation's cybersecurity, while preserving the privacy and civil liberties of our citizens.

The road to today began in 2011, when President Obama took several steps to move the issue of cybersecurity to the forefront by: 1. releasing a cybersecurity legislative proposal; 2. calling on Congress to take urgent action to give the private sector and government the tools needed to combat cyber threats at home and abroad; and 3. issuing the International Strategy for Cyberspace to make clear to nations abroad that the United States was firmly committed to improving cybersecurity and combating cyber terrorism.

I will be offering several amendments as the two bills are considered.

The Jackson Lee amendments are simple and will improve the privacy protections already in the bills and allow the Department of Homeland Security to become a better partner with the private sector in its work to improve domestic cybersecurity.

One of the Jackson Lee amendments that will be offered to the both bills will improve privacy and civil liberties by providing the public with a report from the Government Accountability Office that their privacy and civil liberties are not being compromised by the programs established by this bill.

Other Jackson Lee Amendments to H.R. 1731 will include an assurance that DHS's remains current on innovations: 1. on data security that can improve privacy and civil liberties protections; 2. in industrial control systems to keep pace with industry adoption of new technologies; and industry best practices; and 3. that can aid DHS in aligning federally funded cybersecurity research and development with private sector efforts to protect privacy and civil liberties.

These amendments will make sure that technology and equipment purchased with taxpayer dollars provided to ensure cybersecurity will remain current and focused on real-world applications that reflect constitutional values and how businesses and industry function.

An important building block for improving the Nation's cybersecurity is ensuring that private entities can collaborate to share timely cyber threat information with each other and the Federal Government.

The Administration is expressing concerns with H.R. 1560's broad liability protections offered to companies that sharing information with federal government programs established under this bill.

Appropriate liability protections should be established that incentivize good cybersecurity practices and would not grant immunity to a private company for failing to act on information it receives about the security of its networks.

The important component of cybersecurity is that computer network owners and managers will act to improve cyber defense of their systems when provided with information that vulnerabilities in their computer networks exist.

Legislation should not provide incentives for companies not to act when presented with evidence of network cyber security vulnerabilities.

Electronic data breaches involving Sony, Target, Home Depot, Neiman Marcus, JPMorgan Chase, and Athem are only a few of the cyber incidents that have plagued private sector networks.

These data breaches also are a reminder that the Internet is not yet what it must become to continue to meet the remote communication needs of a global marketplace.

As with other threats this nation has faced in the past and overcome we must create the resources and the institutional responses to protect our nation while preserving our liberties and freedoms.

We cannot accomplish the task of better cybersecurity without the cooperation and full support of citizens; the private sector; local state and federal government; computing research community; and academia.

This level of cooperation requires the trust and confidence of the American people that the actions taken by government to combat cyber threats will not threaten our way of life nor our hard fought Constitutional rights.

H.R. 1731 makes clear that the Department of Homeland Security will be the federal government agency responsible for securing civilian government networks and supporting voluntary efforts by private sector companies and institutions to improve coordination and response to cyber security threats.

The issues regarding liability protection related to cybersecurity must be addressed in order for H.R. 1560 and H.R. 1731 to have any chance of succeeding.

It is my understanding that Chairman MCCAUL and Ranking Member THOMPSON have reached agreement on language that addresses concerns that have been raised regarding liability.

There are talented and resourceful people outside and inside of government who can inform Congress on approaches to information sharing that will yield the desired results without compromising privacy or civil liberties.

Mr. RICHMOND. Mr. Speaker, I rise in opposition to the Rule for H.R. 1560 and H.R. 1731. Members from both parties have a shared goal of bolstering cybersecurity and improving the quality of information that the private sector receives about timely cyber threats so that they can protect their systems. I am greatly disappointed that the Rules Committee failed to make in order any of the several amendments submitted by both Democrats and Republicans to refine what the White House has called ''sweeping'' liability protections, as they appear in both cyber information sharing bills to be considered this week.

Extending liability protection to a company that ''fails to act'' on timely threat information could encourage companies to simply do nothing despite receiving information critical to the security of its systems. Appropriate liability protection does not grant immunity to companies for failing to act on such cybersecurity threat information, but rather incentivizes sound cybersecurity practices. The provision also effectively preempts state laws—including those in California, Massachusetts, and Maryland—that hold businesses liable for failing to maintain reasonable security of their systems, thereby undermining important protections for consumers and their sensitive data.

Instead, my Democratic colleagues on the Homeland Security Committee and I support President Obama's straightforward, tailored approach to addressing what some in industry have identified as a major barrier to the sharing of cyber threat information—the risk that sharing such information would expose companies to legal liability. Unfortunately, the liability protection provision included in the bill puts in place an unduly complicated structure that runs the risk of providing liability relief to companies that fail to act on timely cyber information. I submitted two amendments to address the liability protection problems that exist in both information sharing bills to be considered this week. The first would have struck the provision immunizing companies that fail to act on timely threat information and clarified that the Act has no impact on a duty to act on shared cybersecurity threat information. The second would have removed all potential liability exemptions for willful misconduct by government actors.

These provisions would have improved both bills greatly, and at a minimum they deserved to be debated on the House floor today. The effectiveness of information sharing legislation and efforts to improve the security of companies' systems depends on getting liability protection right. I look forward to continuing the discussion on liability protection with Members from both sides of the aisle as the bill moves forward.

Mr. COLLINS of Georgia. Mr. Speaker, House Report 114–88, the report to accompany H. Res. 212, the special rule governing consideration of H.R. 1731, does not reflect a request by Mr. MULVANEY of South Carolina to add Mr. THOMPSON of Mississippi as a cosponsor of his amendment, number 8 printed in part B of the report.

The material previously referred to by Mr. POLIS is as follows:

AN AMENDMENT TO H. RES. 212 OFFERED BY MR. POLIS OF COLORADO

At the end of the resolution, add the following new sections:

SEC. 4. Immediately upon adoption of this resolution the Speaker shall, 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. 1128) to amend title 38, United States Code, to make certain improvements in the information security of the Department of Veterans Affairs, and for other purposes. 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 Committee on Veterans' Affairs. After general debate the bill shall be considered for amendment under the five-minute rule. All points of order against provisions in the bill 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. 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. If the Committee of the Whole rises and reports that it has come to no resolution on the bill, then on the next legislative day the House shall, immediately after the third daily order of business under clause 1 of rule XIV, resolve into the Committee of the Whole for further consideration of the bill.

SEC. 5. Clause 1(c) of rule XIX shall not apply to the consideration of H.R. 1128.

THE VOTE ON THE PREVIOUS QUESTION: WHAT IT REALLY MEANS

This vote, the vote on whether to order the previous question on a special rule, is not merely a procedural vote. A vote against ordering the previous question is a vote against the Republican majority agenda and a vote to allow the Democratic minority to offer an alternative plan. It is a vote about what the House should be debating.

Mr. Clarence Cannon's Precedents of the House of Representatives (VI, 308–311), describes the vote on the previous question on the rule as ''a motion to direct or control the consideration of the subject before the House being made by the Member in charge.'' To defeat the previous question is to give the opposition a chance to decide the subject before the House. Cannon cites the Speaker's ruling of January 13, 1920, to the effect that ''the refusal of the House to sustain the demand for the previous question passes the control of the resolution to the opposition'' in order to offer an amendment. On March 15, 1909, a member of the majority party offered a rule resolution. The House defeated the previous question and a member of the opposition rose to a parliamentary inquiry, asking who was entitled to recognition. Speaker Joseph G. Cannon (R-Illinois) said: ''The previous question having been refused, the gentleman from New York, Mr. Fitzgerald, who had asked the gentleman to yield to him for an amendment, is entitled to the first recognition.''

The Republican majority may say ''the vote on the previous question is simply a vote on whether to proceed to an immediate vote on adopting the resolution . . . [and] has no substantive legislative or policy implications whatsoever.'' But that is not what they have always said. Listen to the Republican Leadership Manual on the Legislative Process in the United States House of Representatives, (6th edition, page 135). Here's how the Republicans describe the previous question vote in their own manual: ''Although it is generally not possible to amend the rule because the majority Member controlling the time will not yield for the purpose of offering an amendment, the same result may be achieved by voting down the previous question on the rule. . . . When the motion for the previous question is defeated, control of the time passes to the Member who led the opposition to ordering the previous question. That Member, because he then controls the time, may offer an amendment to the rule, or yield for the purpose of amendment.''

In Deschler's Procedure in the U.S. House of Representatives, the subchapter titled ''Amending Special Rules'' states: ''a refusal to order the previous question on such a rule [a special rule reported from the Committee on Rules] opens the resolution to amendment and further debate.'' (Chapter 21, section 21.2) Section 21.3 continues: ''Upon rejection of the motion for the previous question on a resolution reported from the Committee on Rules, control shifts to the Member leading the opposition to the previous question, who may offer a proper amendment or motion and who controls the time for debate thereon.''

Clearly, the vote on the previous question on a rule does have substantive policy implications. It is one of the only available tools for those who oppose the Republican majority's agenda and allows those with alternative views the opportunity to offer an alternative plan.

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

The SPEAKER pro tempore (Mr. MARCHANT). The question is on ordering the previous question.

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

Mr. POLIS. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 9 of rule XX, the Chair will reduce to 5 minutes the minimum time for any electronic vote on the question of adoption of the resolution.

The vote was taken by electronic device, and there were—yeas 237, nays 179, not voting 15, as follows:

[Roll No. 163]

YEAS—237

Abraham	Brat	Collins (NY)
Aderholt	Bridenstine	Comstock
Allen	Brooks (AL)	Conaway
Amash	Brooks (IN)	Cook
Amodei	Buchanan	Costello (PA)
Babin	Buck	Cramer
Barletta	Bucshon	Crawford
Barr	Burgess	Crenshaw
Barton	Byrne	Culberson
Benishek	Calvert	Davis, Rodney
Bilirakis	Carter (GA)	Denham
Bishop (MI)	Carter (TX)	Dent
Bishop (UT)	Chabot	DeSantis
Black	Chaffetz	Diaz-Balart
Blackburn	Clawson (FL)	Dold
Blum	Coffman	Duffy
Bost	Cole	Duncan (SC)
Boustany	Collins (GA)	Duncan (TN)

Ellmers (NC)
Emmer (MN)
Farenthold
Fincher
Fitzpatrick
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Franks (AZ)
Frelinghuysen
Garrett
Gibbs
Gibson
Gohmert
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (LA)
Griffith
Grothman
Guinta
Guthrie
Hanna
Hardy
Harper
Harris
Hartzler
Heck (NV)
Hensarling
Herrera Beutler
Hice, Jody B.
Hill
Holding
Hudson
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurd (TX)
Hurt (VA)
Issa
Jenkins (KS)
Jenkins (WV)
Johnson (OH)
Johnson, Sam
Jolly
Jones
Jordan
Joyce
Katko
Kelly (PA)
King (IA)
King (NY)
Kinzinger (IL)
Kline
Knight
Labrador
LaMalfa
Lamborn
Lance
Latta
LoBiondo
Long
Loudermilk
Love
Lucas
Luetkemeyer
Lummis
MacArthur
Marchant
Marino
Massie
McCarthy
McCaul
McClintock
McHenry
McKinley
McMorris Rodgers
McSally
Meadows
Meehan
Messer
Mica
Miller (FL)
Miller (MI)
Moolenaar
Mooney (WV)
Mullin
Mulvaney
Murphy (PA)
Neugebauer
Newhouse
Noem
Nugent
Nunes
Palazzo
Palmer
Paulsen
Pearce
Perry
Pittenger
Pitts
Poliquin
Pompeo
Posey
Price, Tom
Ratcliffe
Reed
Reichert
Renacci
Ribble
Rice (SC)
Rigell
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rohrabacher
Rokita
Rooney (FL)
Ros-Lehtinen
Roskam
Ross
Rothfus
Rouzer
Royce
Russell
Ryan (WI)
Salmon
Sanford
Scalise
Schweikert
Scott, Austin
Sensenbrenner
Sessions
Shimkus
Shuster
Simpson
Smith (MO)
Smith (NE)
Smith (NJ)
Smith (TX)
Stefanik
Stewart
Stivers
Stutzman
Thompson (PA)
Thornberry
Tiberi
Tipton
Trott
Turner
Upton
Valadao
Wagner
Walberg
Walden
Walker
Walorski
Walters, Mimi
Weber (TX)
Webster (FL)
Wenstrup
Westerman
Westmoreland
Whitfield
Williams
Wilson (SC)
Wittman
Womack
Woodall
Yoder
Yoho
Young (AK)
Young (IA)
Young (IN)
Zeldin
Zinke

NAYS—179

Adams
Aguilar
Ashford
Bass
Beatty
Becerra
Bera
Beyer
Bishop (GA)
Blumenauer
Bonamici
Boyle, Brendan F.
Brady (PA)
Brown (FL)
Brownley (CA)
Bustos
Butterfield
Capps
Capuano
Cárdenas
Carney
Carson (IN)
Cartwright
Castor (FL)
Castro (TX)
Chu, Judy
Cicilline
Clark (MA)
Clarke (NY)
Clay
Cleaver
Clyburn
Cohen
Connolly
Conyers
Cooper
Courtney
Crowley
Cuellar
Cummings
Davis (CA)
Davis, Danny
DeFazio
DeGette
Delaney
DeLauro
DelBene
DeSaulnier
Dingell
Doggett
Doyle, Michael F.
Duckworth
Edwards
Ellison
Engel
Eshoo
Esty
Farr
Fattah
Foster
Frankel (FL)
Fudge
Gabbard
Gallego
Garamendi
Graham
Grayson
Green, Al
Green, Gene
Grijalva
Gutiérrez
Hahn
Heck (WA)
Higgins
Himes
Hinojosa
Honda
Hoyer
Huffman
Israel
Jackson Lee
Jeffries
Johnson (GA)
Johnson, E. B.
Kaptur
Keating
Kelly (IL)
Kennedy
Kildee
Kilmer
Kind
Kirkpatrick
Kuster
Langevin
Larsen (WA)
Larson (CT)
Lawrence
Lee
Levin
Lewis
Lieu, Ted
Lipinski
Loebsack
Lofgren
Lowenthal
Lowey
Lujan Grisham (NM)
Luján, Ben Ray (NM)
Lynch
Maloney, Carolyn
Maloney, Sean
Matsui
McCollum
McDermott
McGovern
McNerney
Meeks
Meng
Moore
Moulton
Nadler
Napolitano
Nolan
Norcross
O'Rourke
Pallone
Pascrell
Pelosi
Perlmutter
Peters
Peterson
Pingree
Pocan
Polis
Price (NC)
Quigley
Rangel
Rice (NY)
Richmond
Roybal-Allard
Ruiz
Ruppersberger
Rush
Ryan (OH)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Schakowsky
Schiff
Scott (VA)
Scott, David
Serrano
Sewell (AL)
Sherman
Sinema
Sires
Slaughter
Speier
Swalwell (CA)
Takai
Takano
Thompson (CA)
Thompson (MS)
Titus
Tonko
Torres
Tsongas
Van Hollen
Vargas
Veasey
Vela
Velázquez
Visclosky
Walz
Waters, Maxine
Watson Coleman
Welch
Wilson (FL)
Yarmuth

NOT VOTING—15

Brady (TX)
Costa
Curbelo (FL)
DesJarlais
Deutch
Graves (MO)
Hastings
Murphy (FL)
Neal
Olson
Payne
Poe (TX)
Schrader
Smith (WA)
Wasserman Schultz

□ 1349

Messrs. CLEAVER and GENE GREEN of Texas changed their vote from ''yea'' to ''nay.''

Messrs. NEUGEBAUER, HUDSON, and STIVERS changed their vote from ''nay'' to ''yea.''

So the previous question was ordered.

The result of the vote was announced as above recorded.

Stated against:

Mr. DEUTCH. Mr. Speaker, on rollcall No. 163, had I been present, I would have voted ''no.''

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

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

RECORDED VOTE

Mr. POLIS. Mr. Speaker, I demand a recorded vote.

A recorded vote was ordered.

The vote was taken by electronic device, and there were—ayes 238, noes 182, not voting 11, as follows:

[Roll No. 164]

AYES—238

Abraham
Aderholt
Allen
Amodei
Ashford
Babin
Barletta
Barr
Barton
Benishek
Bilirakis
Bishop (MI)
Bishop (UT)
Black
Blackburn
Blum
Bost
Boustany
Brat
Bridenstine
Brooks (AL)
Brooks (IN)
Buchanan
Buck
Bucshon
Burgess
Byrne
Calvert
Carter (GA)
Carter (TX)
Chabot
Chaffetz
Clawson (FL)
Coffman
Cole
Collins (GA)
Collins (NY)
Comstock
Conaway
Cook
Costa
Costello (PA)
Cramer
Crawford
Crenshaw
Culberson
Davis, Rodney
Denham
Dent
DeSantis
Diaz-Balart
Dold
Duckworth
Duffy
Duncan (SC)
Duncan (TN)
Ellmers (NC)
Emmer (MN)
Farenthold
Fincher
Fitzpatrick
Fleischmann
Fleming
Flores
Forbes
Fortenberry
Foxx
Franks (AZ)
Frelinghuysen
Garrett
Gibbs
Gibson
Gohmert
Goodlatte
Gosar
Gowdy
Granger
Graves (GA)
Graves (LA)
Griffith
Grothman
Guinta
Guthrie
Hanna
Hardy
Harper
Harris
Hartzler
Heck (NV)
Hensarling
Herrera Beutler
Hice, Jody B.
Hill
Holding
Hudson
Huizenga (MI)
Hultgren
Hunter
Hurd (TX)
Hurt (VA)
Issa
Jenkins (KS)
Jenkins (WV)
Johnson (OH)
Johnson, Sam
Jolly
Jordan
Joyce
Katko
Kelly (PA)
King (IA)
King (NY)
Kinzinger (IL)
Kline
Knight
Labrador
LaMalfa
Lamborn
Lance
Latta
LoBiondo
Long
Loudermilk
Love
Lucas
Luetkemeyer
Lummis
MacArthur
Marchant
Marino
McCarthy
McCaul
McClintock
McHenry
McKinley
McMorris Rodgers
McSally
Meadows
Meehan
Messer
Mica
Miller (FL)
Miller (MI)
Moolenaar
Mooney (WV)
Mullin
Mulvaney
Murphy (PA)
Neugebauer
Newhouse
Noem
Nugent
Nunes
Palazzo
Palmer
Paulsen
Pearce
Perry
Pittenger
Pitts
Poe (TX)
Poliquin
Pompeo
Posey
Price, Tom
Ratcliffe
Reed
Reichert
Renacci
Ribble
Rice (SC)
Rigell
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rohrabacher
Rokita
Rooney (FL)
Ros-Lehtinen
Roskam
Ross
Rothfus
Rouzer
Royce
Russell
Ryan (WI)
Salmon
Sanford
Scalise
Schweikert
Scott, Austin
Sensenbrenner
Sessions
Shimkus
Shuster
Simpson
Sinema
Smith (MO)
Smith (NE)
Smith (NJ)
Smith (TX)
Stefanik
Stewart
Stivers
Stutzman
Thompson (PA)
Thornberry
Tiberi
Tipton
Trott
Turner
Upton
Valadao
Wagner
Walberg
Walden
Walker
Walorski
Walters, Mimi
Weber (TX)
Webster (FL)
Wenstrup
Westerman
Westmoreland
Whitfield
Williams
Wilson (SC)
Wittman
Womack
Woodall
Yoder
Yoho
Young (AK)
Young (IA)
Young (IN)
Zeldin
Zinke

NOES—182

Adams
Aguilar
Amash
Bass
Beatty
Becerra
Bera
Beyer
Bishop (GA)
Blumenauer
Bonamici
Boyle, Brendan F.
Brady (PA)
Brown (FL)
Brownley (CA)
Bustos
Butterfield
Capps
Capuano
Cárdenas
Carney
Carson (IN)
Cartwright
Castor (FL)
Castro (TX)
Chu, Judy
Cicilline
Clark (MA)
Clarke (NY)
Clay
Cleaver
Clyburn
Cohen
Connolly
Conyers
Cooper
Courtney
Crowley
Cuellar
Cummings
Davis (CA)
Davis, Danny
DeFazio
DeGette
Delaney
DeLauro
DelBene
DeSaulnier
Deutch
Dingell
Doggett
Doyle, Michael F.
Edwards
Ellison
Engel
Eshoo
Esty
Farr
Fattah
Foster
Frankel (FL)
Fudge
Gabbard
Gallego
Garamendi
Graham
Grayson
Green, Al
Green, Gene
Grijalva
Gutiérrez
Hahn
Heck (WA)
Higgins
Himes
Hinojosa
Honda
Hoyer
Huelskamp
Huffman
Israel
Jackson Lee
Jeffries
Johnson (GA)
Johnson, E. B.
Jones
Kaptur
Keating
Kelly (IL)
Kennedy
Kildee
Kilmer
Kind
Kirkpatrick
Kuster
Langevin
Larsen (WA)
Larson (CT)
Lawrence
Lee
Levin
Lewis
Lieu, Ted
Lipinski
Loebsack
Lofgren
Lowenthal
Lowey
Lujan Grisham (NM)
Luján, Ben Ray (NM)
Lynch
Maloney, Carolyn
Maloney, Sean
Massie
Matsui
McCollum
McDermott
McGovern
McNerney
Meeks
Meng
Moore
Moulton
Nadler

Napolitano
Nolan
Norcross
O'Rourke
Pallone
Pascrell
Pelosi
Perlmutter
Peters
Peterson
Pingree
Pocan
Polis
Price (NC)
Quigley
Rangel
Rice (NY)
Richmond
Roybal-Allard
Ruiz
Ruppersberger
Rush
Ryan (OH)
Sánchez, Linda T.
Sanchez, Loretta
Sarbanes
Schakowsky
Schiff
Schrader
Scott (VA)
Scott, David
Serrano
Sewell (AL)
Sherman
Sires
Slaughter
Speier
Swalwell (CA)
Takai
Takano
Thompson (CA)
Thompson (MS)
Titus
Tonko
Torres
Tsongas
Van Hollen
Vargas
Veasey
Vela
Velázquez
Visclosky
Walz
Waters, Maxine
Watson Coleman
Welch
Wilson (FL)
Yarmuth

NOT VOTING—11

Brady (TX)
Curbelo (FL)
DesJarlais
Graves (MO)
Hastings
Murphy (FL)
Neal
Olson
Payne
Smith (WA)
Wasserman Schultz

□ 1356

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.

MESSAGE FROM THE SENATE

A message from the Senate by Ms. Curtis, one of its clerks, announced that the Senate has passed bills of the following titles in which the concurrence of the House is requested:

S. 971. An act to amend title XVIII of the Social Security Act to provide for an increase in the limit on the length of an agreement under the Medicare independence at home medical practice demonstration program.

S. 984. An act to amend title XVIII of the Social Security Act to provide Medicare beneficiary access to eye tracking accessories for speech generating devices and to remove the rental cap for durable medical equipment under the Medicare Program with respect to speech generating devices.

BUREAU OF CONSUMER FINANCIAL PROTECTION ADVISORY BOARDS ACT

The SPEAKER pro tempore (Mr. DENHAM). Pursuant to House Resolution 200 and rule XVIII, the Chair declares the House in the Committee of the Whole House on the state of the Union for the further consideration of the bill, H.R. 1195.

Will the gentleman from Kansas (Mr. YODER) kindly take the chair.

□ 1358

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 further consideration of the bill (H.R. 1195) to amend the Consumer Financial Protection Act of 2010 to establish advisory boards, and for other purposes, with Mr. YODER (Acting Chair) in the chair.

The Clerk read the title of the bill.

The Acting CHAIR. When the Committee of the Whole rose on Tuesday, April 21, 2015, amendment No. 2 printed in part D of House Report 114–74 offered by the gentlewoman from New Hampshire (Ms. KUSTER) had been disposed of.

AMENDMENT NO. 1 OFFERED BY MS. KUSTER

The Acting CHAIR. Pursuant to clause 6 of rule XVIII, the unfinished business is the demand for a recorded vote on amendment No. 1 printed in part D of House Report 114–74 offered by the gentlewoman from New Hampshire (Ms. KUSTER) on which further proceedings were postponed and on which the noes prevailed by voice vote.

The Clerk will redesignate the amendment.

The Clerk redesignated the amendment.

RECORDED VOTE

The Acting CHAIR. A recorded vote has been demanded.

A recorded vote was ordered.

The Acting CHAIR. This will be a 2-minute vote.

The vote was taken by electronic device, and there were—ayes 244, noes 173, not voting 14, as follows:

[Roll No. 165]

AYES—244

Adams
Aguilar
Ashford
Barletta
Barton
Bass
Beatty
Becerra
Benishek
Bera
Beyer
Bilirakis
Bishop (GA)
Blumenauer
Bonamici
Boyle, Brendan F.
Brady (PA)
Brooks (IN)
Brown (FL)
Brownley (CA)
Buchanan
Bustos
Butterfield
Calvert
Capps
Capuano
Cárdenas
Carney
Carson (IN)
Cartwright
Castor (FL)
Castro (TX)
Chu, Judy
Cicilline
Clark (MA)
Clarke (NY)
Clay
Cleaver
Clyburn
Cohen
Collins (NY)
Comstock
Connolly
Conyers
Cooper
Costa
Costello (PA)
Courtney
Crowley
Cuellar
Cummings
Davis (CA)
Davis, Danny
Davis, Rodney
DeFazio
DeGette
Delaney
DeLauro
DelBene
Dent
DeSaulnier
Deutch
Diaz-Balart
Dingell
Doggett
Dold
Doyle, Michael F.
Duckworth
Duncan (TN)
Edwards
Ellison
Engel
Eshoo
Esty
Farenthold
Farr
Fattah
Fitzpatrick
Fleming
Flores
Foster
Frankel (FL)
Fudge
Gabbard
Gallego
Garamendi
Gibson
Graham
Graves (GA)
Graves (LA)
Grayson
Green, Al
Green, Gene
Grijalva
Gutiérrez
Hahn
Hanna
Heck (WA)
Herrera Beutler
Higgins
Himes
Hinojosa
Honda
Hoyer
Huffman
Hurd (TX)
Israel
Issa
Jackson Lee
Jeffries
Johnson (GA)
Johnson, E. B.
Jolly
Jones
Joyce
Kaptur
Katko
Keating
Kelly (IL)
Kelly (PA)
Kennedy
Kildee
Kilmer
Kind
Kirkpatrick
Kuster
Lance
Langevin
Larsen (WA)
Larson (CT)
Latta
Lawrence
Lee
Levin
Lewis
Lieu, Ted
Lipinski
LoBiondo
Loebsack
Lofgren
Lowenthal
Lowey
Lujan Grisham (NM)
Luján, Ben Ray (NM)
Lynch
MacArthur
Maloney, Carolyn
Maloney, Sean
Marino
Matsui
McCollum
McDermott
McNerney
McSally
Meehan
Meeks
Meng
Messer
Moolenaar
Moore
Moulton
Nadler
Napolitano
Nolan
Norcross
Nugent
O'Rourke
Pallone
Pascrell
Paulsen
Pearce
Pelosi
Perlmutter
Peters
Pingree
Pocan
Polis
Posey
Price (NC)
Quigley
Rangel
Reed
Renacci
Ribble
Rice (NY)
Richmond
Rigell
Rohrabacher
Ros-Lehtinen
Roybal-Allard
Royce
Ruiz
Ruppersberger
Rush
Ryan (OH)
Sánchez, Linda T.
Sanchez, Loretta
Sanford
Sarbanes
Schakowsky
Schiff
Schrader
Scott (VA)
Scott, David
Sensenbrenner
Serrano
Sewell (AL)
Sherman
Simpson
Sinema
Sires
Slaughter
Smith (NJ)
Speier
Stefanik
Stivers
Swalwell (CA)
Takai
Takano
Thompson (CA)
Thompson (MS)
Thompson (PA)
Tiberi
Titus
Tonko
Torres
Tsongas
Upton
Van Hollen
Vargas
Veasey
Vela
Velázquez
Visclosky
Walden
Walters, Mimi
Walz
Waters, Maxine
Watson Coleman
Webster (FL)
Welch
Wilson (FL)
Yarmuth
Yoder

NOES—173

Abraham
Allen
Amash
Amodei
Babin
Barr
Bishop (MI)
Bishop (UT)
Black
Blackburn
Blum
Bost
Boustany
Brat
Bridenstine
Brooks (AL)
Buck
Bucshon
Burgess
Byrne
Carter (GA)
Carter (TX)
Chabot
Chaffetz
Clawson (FL)
Coffman
Cole
Collins (GA)
Conaway
Cook
Cramer
Crawford
Crenshaw
Culberson
Denham
DeSantis
Duffy
Duncan (SC)
Ellmers (NC)
Emmer (MN)
Fincher
Fleischmann
Forbes
Fortenberry
Foxx
Franks (AZ)
Frelinghuysen
Garrett
Gibbs
Gohmert
Goodlatte
Gosar
Gowdy
Granger
Griffith
Grothman
Guinta
Guthrie
Hardy
Harper
Harris
Hartzler
Heck (NV)
Hensarling
Hice, Jody B.
Hill
Holding
Hudson
Huelskamp
Huizenga (MI)
Hultgren
Hunter
Hurt (VA)
Jenkins (KS)
Jenkins (WV)
Johnson (OH)
Johnson, Sam
Jordan
King (IA)
King (NY)
Kinzinger (IL)
Kline
Knight
Labrador
LaMalfa
Lamborn
Long
Loudermilk
Love
Lucas
Luetkemeyer
Lummis
Marchant
Massie
McCarthy
McCaul
McClintock
McHenry
McKinley
McMorris Rodgers
Meadows
Mica
Miller (FL)
Miller (MI)
Mooney (WV)
Mullin
Mulvaney
Murphy (PA)
Neugebauer
Newhouse
Noem
Nunes
Palazzo
Palmer
Perry
Peterson
Pittenger
Pitts
Poe (TX)
Poliquin
Pompeo
Price, Tom
Ratcliffe
Reichert
Rice (SC)
Roby
Roe (TN)
Rogers (AL)
Rogers (KY)
Rokita
Rooney (FL)
Roskam
Ross
Rouzer
Russell
Ryan (WI)
Salmon
Scalise
Schweikert
Scott, Austin
Sessions
Shimkus
Shuster
Smith (MO)
Smith (NE)
Smith (TX)
Stewart
Stutzman
Thornberry
Tipton
Trott
Turner
Valadao
Wagner
Walberg
Walker
Walorski
Weber (TX)
Wenstrup
Westerman
Westmoreland
Whitfield
Williams
Wilson (SC)
Wittman
Womack
Woodall
Yoho
Young (AK)
Young (IA)
Young (IN)
Zeldin
Zinke

NOT VOTING—14

Aderholt
Brady (TX)
Curbelo (FL)
DesJarlais
Graves (MO)
Hastings
McGovern
Murphy (FL)
Neal
Olson
Payne
Rothfus
Smith (WA)
Wasserman Schultz

□ 1405

Mr. LATTA changed his vote from ''no'' to ''aye.''

So the amendment was agreed to.

The result of the vote was announced as above recorded.

Stated against: