Americans deserve a real debate about the best way to update our laws to address online threats.

Mr. WYDEN. In the op-ed, we point out that legislators and the public know next to nothing about how the government conducts the searches and that the government itself is planning to use software that has not been properly vetted by outside security experts. A bungled government hack could damage systems at hospitals, the power grid, transportation, or other critical infrastructure, and Congress has not had a single hearing on this issue—not one.

In addition, the Rules Enabling Act gives Congress the opportunity to weigh in, which is exactly what my colleagues hope to be doing now on this important issue.

Because of these serious damages, I introduced a bill called the Stop Mass Hacking Act with a number of my colleagues, including Senators DAINES and PAUL. This bill would stop these changes from taking effect, and I am here this morning to ask unanimous consent that the bill be taken up and passed.

Mr. President, I ask unanimous consent that the Judiciary Committee be discharged from further consideration of S. 2952 and the Senate proceed to its immediate consideration, that the bill be read a third time and passed, and the motion to reconsider be considered made and laid upon the table with no intervening action or debate.

The PRESIDING OFFICER. Is there objection?

The majority whip.

Mr. CORNYN. Mr. President, reserving the right to object, I respect our colleague's right to come to the floor and ask unanimous consent. I understand that there are three unanimous consent requests, and I will be objecting to all three of them. I will reserve my statement as to why I am objecting after the third request.

At this point, I object to the unanimous consent request.

The PRESIDING OFFICER. Objection is heard.

Mr. WYDEN. Mr. President, I wish to recognize my colleague from Montana, and after my colleague from Montana speaks, my friend from Delaware will address the Senate.

The PRESIDING OFFICER. The Senator from Montana.

Mr. DAINES. Mr. President, I thank my colleague from Oregon, Senator WYDEN, for talking about this important issue on the floor today.

We shop online with our credit cards, order medicine with our electronic health care records, talk to friends, share personal information, Skype, post beliefs and photos on social media, or Snapchat fun moments, all the while believing everything is safe and secure. It is more important now than ever to ensure that the information we store on our devices is kept safe and that our right to privacy is protected, and that is what we are really talking about here today. How can we ensure that our information is both safe and secure from hacking and government surveillance?

Certainly technology has made our lives easier, but it has also made it easier for criminals to commit crimes and evade law enforcement. In short, our laws aren't keeping up with 21st-century technology advances. But the government's solution to this problem we are talking about today, the change to rule 41 of the Federal Rules of Criminal Procedure, represents a major policy shift in the way the government investigates cyber crime. This proposed solution essentially gives the government a blank check to infringe upon our civil liberties. The change greatly expands the hacking power of the Federal Government, allowing the search of potentially millions of Americans' devices with a single warrant. What this means is that the victims of hacks could be hacked again by their very own government.

You would think such a drastic policy change that directly impacts our Fourth Amendment right would need to come before Congress. It would need to have a hearing and be heard before the American people with full transparency. But, in fact, we have had no hearings. There has been no real debate on this issue.

My colleagues and I have introduced bipartisan, bicameral legislation to stop the rule change and ensure that the American people have a voice. The American people deserve transparency, and Congress needs time to review this policy to ensure that the privacy rights of Americans are protected.

The fact that the Department of Justice is insisting this rule change take effect on December 1—that is tonight at midnight—frankly, should send a shiver down the spines of all Americans.

My colleagues and I are here today to not only wake up Americans to this great expansion of powers by our government but also to urge our colleagues to join this bipartisan effort to stop rule 41 changes without duly considering the impact to our civil liberties. Our civil liberties and our Fourth Amendment can be chipped away little by little until we barely recognize them anymore. We simply can't give unlimited power for unlimited hacking which puts Americans' civil liberties at risk.

Again, I thank my colleagues from Delaware and Oregon for joining me here today, and I yield to my friend and colleague from Delaware, Senator COONS.

The PRESIDING OFFICER. The Senator from Delaware.

UNANIMOUS CONSENT REQUEST—S. 3475

Mr. COONS. Mr. President, I thank my colleagues, Senator WYDEN and Senator DAINES. They have worked tirelessly to address this pressing issue of the pending change to privacy protections contained in a proposed change to the Federal Rules of Criminal Procedure.

As you have heard, if Congress fails to act today and thoroughly consider and debate these rule changes, they will go into effect at midnight tonight. They will take effect tomorrow, December 1. I believe it is essential that these rules strike a careful balance, giving law enforcement the tools they need to investigate cyber attacks and cyber crimes to keep us safe while also protecting Americans' constitutional rights to freedom from unreasonable searchs, our right to privacy.

Neither the Senate nor House has held a single hearing or markup to evaluate these changes to the Federal Rules of Criminal Procedure. The body of government closest to the people has utterly failed to weigh in on an issue that can immediately and directly impact our constituents—our citizens. While the proposed changes are not necessarily bad or good, they are serious and present significant privacy concerns that warrant careful consideration and debate.

All Americans should want criminal investigations to proceed quickly and thoroughly, but, as I have said, I am concerned that these changes would remove important judicial safeguards by having one judge decide on a search that would give our government the ability to search and possibly alter thousands of computers owned by innocent and unknowing American citizens all over our country.

Members of Congress should have an opportunity to consider this information seriously. We should carefully evaluate the merits of these proposed changes and their ramifications. I think it is our duty to have a frank and open discussion so we can think about the unintended consequences and protect our constituents' rights. Two weeks ago, I introduced legislation that would give Congress the time to have that conversation. The Review the Rule Act, or S. 3475, would delay the changes to rule 41 until July 1, 2017. That bill is cosponsored by Senators WYDEN, LEAHY, BALDWIN, and FRANKEN, as well as Republican Senators DAINES, LEE, and PAUL. That list of Senators from every part of our ideological spectrum is just a reminder that this is not a partisan issue. This is a bipartisan group of Senators raising questions and challenges to a proposal by the Obama administration's Justice Department.

I think it is important to remind anyone watching or listening that we want to ensure that the American people are kept safe from hackers and online criminal activity. We want law enforcement to have the tools to investigate and address potential threats, but we shouldn't have to sacrifice our rights to privacy and protection from unreasonable searches and seizures just to achieve that protection.

I encourage my colleagues to join me in supporting this legislation and

working together to evaluate these changes to the Federal Rules of Criminal Procedure.

Mr. President, I ask unanimous consent that the Judiciary Committee be discharged from further consideration of S. 3475 and that the Senate proceed to its immediate consideration. I further ask that the bill be read a third time and passed and the motion to reconsider be considered made and laid upon the table.

The PRESIDING OFFICER. Is there objection?

The majority whip.

Mr. CORNYN. Mr. President, I object.

The PRESIDING OFFICER. Objection is heard.

Mr. CORNYN. Mr. President, I understand that the Senator from Montana will not be offering a unanimous consent request, so if it is all right with my colleagues, I wish to explain why I have objected.

Excuse me. I will yield back to the Senator from Oregon.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Mr. President, I will still be offering a third proposal, so I ask my colleague if he wishes to speak now or after the third request.

Mr. CORNYN. Mr. President, I appreciate the courtesy of my friend and colleague from Washington—excuse me, Oregon, but I will reserve my remarks until after he makes the next UC request.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Mr. President, when the Oregon Ducks go to the NCAA title game in basketball, I will invite my friend to sit with me and he will see Oregon in action.

UNANIMOUS CONSENT REQUEST—S. 3485

Mr. WYDEN. Senator CORNYN has now objected to passage of the two bills relating to rule 41, and he is certainly within his right to do so. I wish to offer the theory—not exactly a radical one, in my view—that if we can't pass bills with respect to mass surveillance or have hearings, we at least ought to have a vote so that the American people can actually determine if their Senators support authorizing unprecedented, sweeping government hacking without a single hearing. There is a lot more debate in this body over the tax treatment of race horses than massive expansion of surveillance authority.

In a moment, I will ask unanimous consent that the body move to an immediate rollcall vote on the Stalling Mass Damaging Hacking Act which would delay rule 41 changes until March 31. I don't condone Congress kicking cans down the road. This is one example of where, with a short delay, it would be possible to have at least one hearing in both bodies so that Congress would have a chance to debate a very significant change in our hacking policy.

Congress has not weighed, considered, amended, or acted like anything resembling an elected legislature on this issue. There have been some who have looked into the issue, but—I call it Senate 101—we should at least have a hearing on a topic with enormous potential consequences for millions of Americans. That had not been done, despite a bipartisan bill being introduced in the House and the Senate, days after the changes were approved. Lawmakers and the public ought to know more about a novel, complicated, and controversial topic, and they would be in a position to have that information if there was a hearing and Members of both sides of the aisle could ask important questions.

Since the Senate has not had a hearing on this issue, lawmakers have still been trying to get answers to important questions. Twenty-three elected representatives from the House and Senate, Democrats and Republicans spanning the philosophical spectrum, have asked substantive questions that the Department of Justice has failed to answer, and they barely went through the motions. They spectacularly failed to respond to both concerns of Democrats and Republicans in both the Senate and in the House.

I ask unanimous consent that the letter that was sent to the DOJ, signed by myself and 22 bipartisan colleagues from the House and Senate, be printed in the RECORD.

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

CONGRESS OF THE UNITED STATES,
Washington, DC, October 27, 2016.

Hon. LORETTA LYNCH,
U.S. Attorney General,
Department of Justice, Washington, DC.

DEAR ATTORNEY GENERAL LYNCH: We write to request information regarding the Department of Justice's proposed amendments to Rule 41 of the Federal Rules of Criminal Procedure. These amendments were approved by the Supreme Court and transmitted to Congress pursuant to the Rules Enabling Act on April 30, 2016. Absent congressional action the amendments will take effect on December 1, 2016.

The proposed amendments to Rule 41 have the potential to significantly expand the Department's ability to obtain a warrant to engage in ''remote access,'' or hacking of computers and other electronic devices. We are concerned about the full scope of the new authority that would be provided to the Department of Justice. We believe that Congress—and the American public—must better understand the Department's need for the proposed amendments, how the Department intends to use its proposed new powers, and the potential consequences to our digital security before these rules go into effect. In light of the limited time for congressional consideration of the proposed amendments, we request that you provide us with the following information two weeks after your receipt of this letter.

1. How would the government prevent ''forum shopping'' under the proposed amendments? The proposed amendments would allow prosecutors to seek a warrant in any district ''where activities related to a crime may have occurred.'' Will the Department issue guidance to prosecutors on how this should be interpreted?

2. We are concerned that the deployment of software to search for and possibly disable a botnet may have unintended consequences on internet-connected devices, from smartphones to medical devices. Please describe the testing that is conducted on the viability of 'network investigative techniques' (''NITs'') to safely search devices such as phones, tablets, hospital information systems, and internet-connected video monitoring systems.

3. Will law enforcement use authority under the proposed amendments to disable or otherwise render inoperable software that is damaging or has damaged a protected device? In other words, will network investigative techniques be used to ''clean'' infected devices, including devices that belong to innocent Americans? Has the Department ever attempted to ''clean'' infected computers in the past? If so, under what legal authority?

4. What methods will the Department use to notify users and owners of devices that have been searched, particularly in potential cases where tens of thousands of devices are searched?

5. How will the Department maintain proper chain of custody when analyzing or removing evidence from a suspect's device? Please describe how the Department intends to address technical issues such as fluctuations of internet speed and limitations on the ability to securely transfer data.

6. Please describe any differences in legal requirements between obtaining a warrant for a physical search versus obtaining a warrant for a remote electronic search. In particular, and if applicable, please describe how the principle of probable cause may be used to justify the remote search of tens of thousands of devices. Is it sufficient probable cause for a search that a device merely be ''damaged'' and connected to a crime?

7. If the Department were to search devices belonging to innocent Americans to combat a complicated computer crime, please describe what procedures the Department would use to protect the private information of victims and prevent further damage to accessed devices.

Sincerely,

Ron Wyden; Patrick Leahy; Tammy Baldwin; Christopher A. Coons; Ted Poe; John Conyers, Jr.; Justin Amash; Jason Chaffetz; Steve Daines; Al Franken; Mazie K. Hirono; Mike Lee; Jon Tester; Elizabeth Warren; Martin Heinrich; Judy Chu; Steve Cohen; Suzan DelBene; Louie Gohmert; Henry C. ''Hank'' Johnson; Ted W. Lieu; Zoe Lofgren; Jerrold Nadler.

Mr. WYDEN. I also ask unanimous consent that the response from the Department of Justice, which I have characterized as extraordinarily unresponsive to what legislators have said, be printed in the RECORD as well.

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

U.S. DEPARTMENT OF JUSTICE,
OFFICE OF LEGISLATIVE AFFAIRS,
Washington, DC, November 18, 2016.

Hon. RON WYDEN,
U.S. Senate,
Washington, DC.

DEAR SENATOR WYDEN: This responds to your letter to the Attorney General, dated October 27, 2016, regarding proposed amendments to Rule 41 of the Federal Rules of Criminal Procedure, recently approved by the Supreme Court. We are sending identical responses to the Senators and Members who joined in your letter.

The amendments to Rule 41, which are scheduled to take effect on December 1, 2016,