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 would not 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—who now comprise the bipartisan task force on expanding 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 the bipartisan questions from 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:

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 having 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 rolloca vote on the Stopping 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 able 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.
mark the end of a three-year deliberation process, which included extensive written comments and public testimony. After hearing the public’s views, the federal judiciary’s Advisory Committee on Criminal Procedure, which includes federal and state judges, law professors, attorneys in private practice, and others in the legal community, has recommended the amendments to Rule 41.

Rule 41 involves criminal hacking computers located in five or more different judicial districts, the changes to Rule 41 would allow federal agents to compel one judge to review an application for a search warrant rather than be required to submit separate warrant applications in each district where a computer is affected. For example, agents may seek a search warrant to assist in the investigation of a ransomware scheme facilitated by computers infected with such malware. The change would not permit indiscriminate surveillance of computers that is not permissible now and will continue to be prohibited when the amendment goes into effect. This is because other than identifying a computer infected with such malware, the amendment makes no change to the substantive law governing when a warrant application should be granted or denied. The amended rule limits forum shopping by restricting the venue in which a magistrate judge may issue a warrant for a remote search to “any district where activities related to a cybercrime may be occurring.” Often, this language will leave only a single district in which investigators can seek a warrant. For example, where a victim has received death threats, extortion demands, or ransomware demands from a criminal hiding behind Internet anonymizing technologies, the victim’s district would likely be the only district in which a warrant could be issued for a remote search to identify the perpetrator.

Such botnets, which range in size from hundreds to millions of infected computers and may be used for a variety of criminal purposes, represent one of the fastest-growing species of computer crime and are among the key cybersecurity threats facing American citizens and businesses. Absent the amendments to Rule 41, however, the requirement to obtain up to 94 simultaneous search warrants may prevent cyber investigators from taking needed action to liberate computers infected with such malware. The change would not permit indiscriminate surveillance of computers that is not permissible now and will continue to be prohibited when the amendment goes into effect. This is because other than identifying a computer infected with such malware, the amendment makes no change to the substantive law governing when a warrant application should be granted or denied. The amended rule limits forum shopping by restricting the venue in which a magistrate judge may issue a warrant for a remote search to “any district where activities related to a cybercrime may be occurring.” Often, this language will leave only a single district in which investigators can seek a warrant. For example, where a victim has received death threats, extortion demands, or ransomware demands from a criminal hiding behind Internet anonymizing technologies, the victim’s district would likely be the only district in which a warrant could be issued for a remote search to identify the perpetrator.

The amendments apply in two narrow circumstances. First, where a criminal suspect has hidden the location of his computer using anonymity technologies, the amendments to Rule 41 would ensure that federal agents know which magistrate judge to go to in order to apply for a warrant. For example, if agents are investigating criminals who are sexually exploiting children and uploading videos of that exploitation to others to see—concealing their locations through anonymizing technology—agents will be able to apply for a search warrant to discover where they are located.

An investigation of the Playpen website—a Tor site used by more than 100,000 pedophiles to encourage sexual abuse and exploitation of children and to trade sexually explicit images of abused children—illustrates the importance of this change. During the investigation, authorities were able to wrest control of the site from its administrators, and then obtained from a federal judge to use a remote search tool to undo the anonymity promised by Tor. The search would occur only if a Playpen user accessed child pornography (a federal crime), in which case the tool would cause the user’s computer to transmit to investigators a limited amount of information, including the user’s name, address, and IP address, to help investigators identify the user and his computer. Based on that information, investigators could then conduct a traditional, real-world investigation, such as by running a criminal records check, interviewing neighbors, or applying for an additional warrant to search a suspect’s house for incriminating evidence. Those pursuing online investigations of the Playpen case have led to more than 200 active proceedings—including the prosecution of at least 48 alleged abusers—and the identification of at least 250 American children who were subject to sexual abuse. Nonetheless, despite the success of the Playpen investigation, Federal courts have had to rely on cumbersome procedures in some of the resulting prosecutions because of the lack of clear venue in the current version of Rule 41. In other cases, courts have declined to suppress evidence because the law was not clear, but have suggested that they would do so in future cases. Recently, the Department of Justice (the Department) carefully considers both the need to prevent harm to the public caused by criminals and the potential risks of taking action. In particular, when conducting computer searches, agents typically work closely with sophisticated computer security researchers both inside and outside the government. As part of the process, agents typically deploy verification and validation of computer tools. Such testing is designed to ensure that tools work as intended and do not create unintended consequences. That kind of careful consideration of any future technical measures will continue, and we welcome continued collaboration with the private sector and law enforcement in the development and use of botnet mitigation techniques. The Department’s botnet successes have demonstrated that the Department can disrupt and dismantle botnets while avoiding collateral damage to victims. And of course, choosing to do nothing has its own cost: leaving victims’ computers under the control of criminals who will continue to invade their privacy, extort money from them through ransomware, or steal their financial information.

Second, the amendments to Rule 41 permit identifying information (such as an IP address) from infected computers comprising a botnet in order to make sure owners of the infected computers are found (typically, a service provider). Or law enforcement might engage in an online operation that is designed to disrupt the botnet and restore full control over computers to their legal owners. Both of these techniques, however, could involve conduct that some courts might hold constitutes a search or seizure under the Fourth Amendment. In general, it is not the case that the items to be searched or seized from victim computers pursuant to a botnet warrant will be quite limited. For example, we believe it may be necessary to take steps to measure the size of the botnet by having each victim computer report a unique identifier; but it would not be lawful in such circumstances to search the victims’ unrelated private files. Whether or not a warrant authorizing a remote search is proper is a question of Fourth Amendment law, determined by the amendments to Rule 41. Simply put, the amendments do not authorize the government to undertake any search or seizure of computers from their legal owners. Both computers from criminal control are not, as a practical matter, blocked by outmoded venue rules.

The amendment’s notice requirement mandates that when executing a warrant for a remote search, “the officer must make reasonable efforts to serve a copy of the warrant on the owner of the computer whose information was seized or copied,” and that “[t]his service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.” What means are reasonably available to notify an individual who has concealed his location and identity will of course vary from case to case. If the remote search is successful in identifying the suspect, then notice can be provided in the traditional manner (following existing rules for delaying notice of appropriate law enforcement investigations). If the search is unsuccessful, then investigators would have to consider other means that may be available, for example through through ex parte presentation of an investigation involving botnet victims, the Department would make reasonable efforts to
Mr. WYDEN. Colleagues are going to see that substantive, clear questions, posed by Democrats and Republicans in writing, were not responded to.

Because of the lack of genuine answers from the Justice Department to this letter, signed by 23 Members of Congress, and the substantial nature of these unprecedented changes in surveillance policy, I ask now for unanimous consent for a vote on the SMDH Act to give Congress time to debate these sweeping changes to surveillance policy, I ask now for unanimous consent for a vote on the SMDH Act to give Congress time to debate these sweeping changes to surveillance policy.

The PRESIDING OFFICER. Is there objection?

The majori whip.

Mr. CORYN. Mr. President, I object. The PRESIDING OFFICER. Objection is heard.

Mr. CORYN. Mr. President, I know sometimes that when people hear us engage in these debates, they think we don’t like each other and we can’t work together; that we are so polarized, we are dysfunctional. Actually, these Senators are my friends in addition being colleagues. Let me just explain how I think their concerns are misplaced.

First of all, we all care about, on the spectrum of privacy to security, how that is dialed in. As the Presiding Officer knows, as the former attorney general—thereby for the right balance between individual privacy and safety and security and law enforcement, and sometimes we have differences of opinion as to where exactly on that spectrum that ought to be struck, but the fundamental problem with the requests that have been made today is, Federal Rule Of Criminal Procedure 41 has already been the subject of a lengthy 3-year process with a lot of thoughtful input, public hearings, and deliberation.

As the Presiding Officer knows, the courts have the inherent power to write their own rules of procedure, and that is what this is, part of the Federal Rules of Criminal Procedure. What happens is a pretty challenging process where you have to have unanimous consent by the judicial conference. Then, as in this case, they have to be endorsed by the U.S. Supreme Court, which is Federal Rule of Criminal Procedure 41, which happened on May 1, 2016.

If there was any basis for the claim that this is somehow a hacking of personal information without due process of law or without adequate consideration, I just—I think the process by which the Supreme Court has set up, through the Rules Advisory Committee and through the Judicial Conference, for example, any concerns that the objections that were raised were not adequately considered.

I am also told, Senator Graham from South Carolina chaired a subcommittee hearing of the Senate Judiciary Committee—I believe it was last spring—on this very issue. So there has been some effort in the Congress to do oversight and to look into this, although perhaps it didn’t get the sort of attention that it deserved.

The biggest, most important point to me is that for everybody who cares about civil liberties and for everybody who cares about the personal right of privacy we all have in our homes and the expectation of privacy we have against intrusion by the government without due process, this still requires the government to come forward and do what it always has to do when it seeks a search warrant under the Fourth Amendment. You still have to go before a judge and show probable cause—you still have to show probable cause that a crime has been committed, and the defendant can still challenge the lawfulness of the search. The defendant always reserves that right to challenge the lawfulness of the search. I believe all of these constitutional protections, all of these procedural protections, all the concerns about lack of adequate deliberation can be dispelled by the simple steps I have described.

There is a challenge when cyber criminals use the Internet and social media to prey on innocent children, to traffic in human beings, to buy and sell drugs, and they have to be dealt with by law enforcement—for the Federal Government—to get a search warrant approved by a judge based on the showing of probable cause to be able to get that evidence so the law can be enforced and these cyber criminals can be prosecuted. That is what we are talking about. All this rule 41 does is creates a circumstance where if the criminal is using an anonymizer, or some way to scramble the IP address—the Internet Protocol address of the computer they are using—from the rule of procedure allows the U.S. attorney, the Justice Department, to go to any court that will then require probable cause, that will then allow the defendant to challenge that search warrant—but to provide a means by which you can go to court and get a search warrant and investigate the facts and, if a crime has been committed, to make sure that person is prosecuted under the letter of the law. I appreciate the concerns my colleagues have expressed, that somehow we have gotten the balance between security and privacy wrong, but I believe that as a result of the process by which the Rules Advisory Committee, the Judicial Conference, and the Supreme Court have approved this rule after 3 years of deliberation, including public hearings, scholarly input by academicians, practicing lawyers, law professors and the like, I think that ought to allay their concerns that somehow this is an unthought through rule that is going to have unintended consequences. I think the fundamental protection we all have under the Fourth Amendment of the Constitution against unreasonable searches and seizures and the requirement that the government come to court in front of a judge and show probable cause that a crime has been committed, and that even once the search warrant is issued, that the defendant can challenge the lawfulness of the search—all of that ought to allay the concerns of my colleagues that somehow we have gotten that balance between privacy and security right because I think this does strike an appropriate balance.

Those are the reasons I felt compelled to object to the unanimous consent requests, and I appreciate the courtesy of each of my colleagues. The PRESIDING OFFICER. The Senator from Oregon.
have been friends since we arrived here, and we are working together on a whole host of projects right now. So this is debate about differences of opinion with respect to some of the key issues. I wish to make a couple of quick points. First, my colleague Mr. Paul introduced a major policy change that has not had a single hearing, no oversight, no discussion. In effect, the Senate—by not voting on this bill today with the hack. So my colleague and I walked into a coffee shop in Houston or Dallas, or in my home State, in Coos Bay or Eugene, people wouldn’t have any idea what was going to happen tonight at midnight. Tonight at midnight is going to be a significant moment in this discussion.

My colleague made the point with respect to security and privacy. I definitely feel those two are not mutually exclusive; we can have both, but it is going to take smart policies. My colleague has done a lot of important work on the Freedom of Information Act issues. These are complicated, important issues, and nobody up here has had a chance to weigh in. There has been a process among some judges, and our colleagues have had a chance to submit a brief. Maybe there was notice in the Federal Register; that is the way it usually works, but nobody at home knows anything about that. My guess is, none of our hospitals knows anything about this. My colleagues are asking: If there was a motion to perhaps derogatory about somebody personally; we just have a difference of opinion with respect to the process. To me, at home, when people hear about a government hacking, that is what means I get a chance to weigh in. That is why I have townhall meetings in every county every year because that is what the people think the process is, not judges talking among themselves.

The second point my friend touched on was essentially the warrant policies and that he supports the Fourth Amendment and this is about the Fourth Amendment. I think that is worthy, and I agree, as my colleague, this is an awful novel approach to the Fourth Amendment. One judge, one warrant for thousands and potentially millions of computers which could result in more damage to the citizen after the citizen has already been hit once with the hack. So my colleague said this is what the Fourth Amendment is about. I think that is a fair point for debate. I would argue this is an awful novel approach to the Fourth Amendment. This is not what I think the Fourth Amendment is. Hey, this is about me and somebody is going to have to get a warrant about me. It is about individuals.

To me, the Senate has now—and we still have officially 12 hours to do something about it—but as of now, the Senate has given consent to an expansion of government hacking and surveillance. In effect, the Senate, by not voting on this bill, has essentially the warrant policies that protect their security and their liberty. They are right to do so. That cause will be harmed if the Senate—by not voting on this bill today—does not take steps between now and midnight.

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