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,

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 the Federal Rules of Criminal Procedure, which includes federal and state judges, law professors, attorneys in private practice, and others in the legal community, approved the amendments and rejected criticisms of the proposal. The amendments were then considered and unanimously approved by the Standing Committee on Rules and the Judicial Conference, and adopted by the United States Supreme Court.

It is important to note that the amendments do not change any of the traditional protections and procedures under the Fourth Amendment, such as the requirement that the government establish probable cause. Rather, the amendments would merely ensure that venue exists so that at least one court is available to consider whether a particular warrant application comports with the Fourth Amendment.

Further, the amendments would not authorize the government to undertake any search or seizure or use any remote search technique, whether inside or outside the United States, that is not already permitted under current law. The use of remote searches is not new, and warrants for remote searches are currently issued under Rule 41. In addition, courts already permit the search of multiple computers pursuant to a single warrant, so long as the necessary legal requirements are met with respect to each computer. Nothing in the amendments changes the existing legal requirements.

The amendments apply in two narrow circumstances. First, where a criminal suspect has hidden the location of his computer using technological means, the changes 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 for others to see—but 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 the abuse—illustrates the importance of this change. During the investigation, authorities were able to wrest control of the site from its administrators, and then obtained approval from a federal court 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 on the site (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 true IP address, to help locate and 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 court-authorized remote searches in the Playpen case have led to more than 200 active prosecutions—including the prosecution of at least 48 alleged abusers—and the identification or rescue of at least 49 American children who were subject to sexual abuse. Nonetheless, despite the success of the Playpen investigation, Federal courts have ordered the suppression of evidence 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.

Second, where the crime involves criminals hacking computers located in five or more different judicial districts, the changes to Rule 41 would ensure that federal agents may identify one judge to review an application for a search warrant rather than be required to submit separate warrant applications in each district—up to 94—where a computer is affected. For example, agents may seek a search warrant to assist in the investigation of a ransomware scheme facilitated by a botnet that enables criminals abroad to extort thousands of Americans. 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. This change would not permit indiscriminate surveillance of thousands of victim 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 court to consider the warrant application, 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 crime may have occurred.'' 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.

In cases involving widespread criminal conduct, activities related to the crime may have occurred in multiple districts, and thus there may be multiple districts in which investigators may seek a warrant under the new amendment. For many years, however, existing laws have recognized the need for warrants to be issued in a district connected to criminal activity even when the information sought may not be present in the district. The language of the new Rule 41(6)(6) amendment limiting warrant venue to ''any district where activities related to a crime may have occurred'' was copied verbatim from the existing warrant venue provisions in Rule 41(6)(3) and (b)(5), which authorize judges to issue out-of-district warrants in cases involving terrorism and searches of U.S. territories and overseas diplomatic premises. Thus, the new venue provision of Rule 41(b)(6) for remote searches is consistent with existing practices in these other contexts. Similarly, warrants for email and other stored electronic communications are sought tens of thousands of times a year in a wide range of investigations. Such warrants may be issued in any district by a court that ''has jurisdiction over the offense being investigated.'' 18 U.S.C. §§2703 & 2711(3).

As with law enforcement activities in the physical world, law enforcement actions to prevent or redress online crime can never be completely free of risk. Before we conduct online investigations, 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 complex online operations, we typically work closely with sophisticated computer security researchers both inside and outside the government. As part of operational planning, investigators conduct predeployment 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 cybersecurity experts in the development and use of botnet mitigation techniques. The Department's antibotnet 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.

Law enforcement could obtain identifying information (such as an IP address) from infected computers comprising a botnet in order to make sure owners are warned of the infection (typically, by their Internet 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, we anticipate that the items to be searched or seized from victim computers pursuant to a botnet warrant will be quite limited. For example, we believe that it may be reasonable in a botnet investigation 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, which is not changed by the amendments to Rule 41. Simply put, the amendments do not authorize the government to undertake any search or seizure or use any remote search technique that is not already permitted under the Fourth Amendment. They merely ensure that searches that are appropriate under the Fourth Amendment and necessary to help free victim 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 person whose property was searched or whose information was seized or copied,'' and that ''[s]ervice 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 where appropriate in ongoing investigations). If the search is unsuccessful, then investigators would have to consider other means that may be available, for example through a known email address. In an investigation involving botnet victims, the Department would make reasonable efforts to

notify victims of any search conducted pursuant to warrant. For example, if investigators obtained victims' IP addresses at a particular date and time in order to measure the size of the botnet, investigators could ask the victims' Internet service providers to notify the individuals whose computers were identified as being under the control of criminal bot herders. Under such an approach, it would not even be necessary for investigators to learn the identities of specific victims. The Department will, of course, also consider other appropriate mechanisms to provide notice consistent with the amended Rule 41.

Under the Federal Rules of Evidence, the government must establish the authenticity of any item of electronic evidence it moves to admit in evidence. To do so, it must offer evidence ''sufficient to support a finding that the item is'' what the government claims it to be, and a criminal defendant may object to the admission of evidence on the basis that the government has not established its authenticity. The amendments to Rule 41 do not make any change to the law governing the admissibility of lawfully obtained evidence at trial, whether on the basis of authenticity or any other basis, and to our knowledge authenticity objections have not played a substantial role in prior federal criminal trials at which evidence obtained as a result of remote searches was introduced.

Protecting victims' privacy is one of the Department's top priorities. To the extent that investigators collect any information concerning botnet victims, the Department will take all appropriate steps to safeguard any such information from improper use or disclosure. The Department presently and vigorously protects the private information collected pursuant to search warrants for computers and documents seized from a home or business and the Department will follow the same exacting standards for any warrant executed under the amendments to Rule 41.

We hope that this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

PETER J. KADZIK,
Assistant Attorney General.

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 government's hacking authority.

I ask unanimous consent that the Senate proceed to the immediate consideration of S. 3485, introduced earlier today; that at a time to be determined by the majority leader, in consultation with the Democratic leader, but no later than 4 p.m. today, the Senate proceed to vote in relation to this bill.

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 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 to 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 of Alaska, we always try to strike 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 when we want to change a Federal rule of criminal procedure. We have to get it approved by the Rules Advisory Committee. It is made up of judges, law professors, and practicing lawyers. Then it has to be approved 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, dispels 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 has gotten now.

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—an impartial magistrate—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 facts.

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 there has to be a way for 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 operating from—then this 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 or hasty 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.

Mr. WYDEN. Mr. President, before he leaves the floor, I wish to engage my friend for a moment with respect to his remarks. He is absolutely right that we

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 in response to my colleague.

My colleague said there had been an inclusive process for discussing this. As far as I can tell, the vast amount of discussion basically took place between the judges and the government. My guess is, if you 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 with some judges, and I guess some folks got a chance to submit a brief. Maybe there was a 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 know anything about something like this, and it has real implications for them because our medical facilities—something we all agree on that have been major sources of cyber hackings—they have been major kinds of targets.

Again, this is not the kind of thing where somebody is saying something 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 process, they say: Hey, I guess that 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 worth debating. To me, at a minimum, 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 most people 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 acting, has put a stamp of approval on a major policy change that has not had a single hearing, no oversight, no discussion. In effect, the Senate—this is not even Senate 101. That is what everybody thinks Senators are supposed to be about. When we are talking about search and seizure, that is an issue for Congress to debate, and the Justice Department shouldn't have the ability to, at a minimum, as I indicated in my conversation with my colleague from Texas, come up with a very novel approach to the Fourth Amendment without elected officials being able to weigh in.

Now I will close by way of saying that when Americans find out that the Congress is allowing the Justice Department to just wave its arms in the air and grant itself new powers under the Fourth Amendment without the Senate even being a part of a single hearing, I think law abiding Americans are going to ask: So what were you people in the Senate thinking about? What are you thinking about when the FBI starts hacking the victims of a botnet attack or when a mass attack breaks their device or an entire hospital system, in effect, has great damage done, faces great damage, and possibly puts lives at risk?

My hope is that Congress would add protections for Americans surrounding the whole issue of government hacking. I have said again and again and again that the smart technology policy, the smart surveillance policy from the getgo is built around the idea that security and liberty are not mutually exclusive, that a smart policy will do both, but increasingly, policies coming out of here aren't doing a whole lot of either. In this case, I think the Senate is abdicating its obligations. Certainly, in the digital era, Americans do not throw their Fourth Amendment rights out the window because they use a device that connects to the Internet.

So I am going to close by way of saying that I think this debate about government hacking is far from over. My guess is that Senators are going to hear from their constituents about this policy sooner rather than later, and we will be back on the floor then, looking to do what should have been done prior to midnight tonight, which is to have hearings, to involve the public—not just Justices and maybe a few people who can figure out how to find that section of the Federal Register so they can weigh in.

Americans are going to continue to demand from all of us in the Senate policies that protect their security and their liberty. They are right to do so. That cause will be harmed if the Senate doesn't take steps between now and midnight.

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

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

21ST CENTURY CURES BILL

Ms. WARREN. Mr. President, I am glad to be here with my colleagues today to have a chance to talk about the 21st Century Cures bill. On Monday I came to the Senate floor to speak against a deal that was emerging in the House of Representatives around this bill.

When Congress first started working on this proposal 2 years ago, the idea was for Democrats and Republicans to work together to improve medical innovation and access to lifesaving cures. For over 2 years a lot of people worked really hard on that effort. We had a chance to bring down the cost of skyrocketing drugs. We had a chance to support medical research so we could start to cure diseases such as Alzheimer's and diabetes. We had a chance to help coal miners whose health care is on the ropes and who are running out of time. Unfortunately, the Cures bill introduced in the House last week didn't do any of those things. Instead, it was a typical Washington deal—a deal that ignored what voters want, and held a bunch of commonsense, bipartisan health proposals hostage unless Congress also agreed to pass a giant giveaway to drug companies.

So how did this happen? Lobbyists. Kaiser Health News estimated that the new Cures bill has generated more lobbying than almost all of the 11,000 bills that have been proposed during this Congress. At one point, there were about three lobbyists for every single Member of Congress. Every one of those lobbyists wanted favors. Wow. Did they get some doozies here: a provision to make it easier for drug companies to commit off-label marketing fraud—taking pills that are approved for one use and using them for a whole lot of other purposes—without any evidence that it is either safe or effective, a provision making it easier for drug companies to hide gifts they give to doctors who prescribe certain drugs, a giveaway to a major super PAC donor who stands to benefit financially through pushing regenerative therapies through FDA, even if they don't meet the FDA's gold standard for safety and effectiveness.

This bill is not about doing what the American people want. This bill is about doing what drug companies and donors want. On Monday, I made it clear that I oppose this. Since then, two things have happened. First, since Monday, the public has gotten wind of this deal and they don't like it. In the last 24 hours, more than 100,000 people