The PRESIDING OFFICER. The question is on agreeing to the motion.

The motion was agreed to.

PROVIDING FOR CONGRESSIONAL DISAPPROVAL OF A RULE SUBMITTED BY THE FEDERAL COMMUNICATIONS COMMISSION—MOTION TO PROCEED

Mr. MCCONNELL. Mr. President, I move to proceed to S.J. Res. 34.

The PRESIDING OFFICER. The clerk will report the motion.

The senior assistant legislative clerk read as follows:

Motion to proceed to Calendar No. 16, S.J. Res. 34, a joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to ''Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.''

The PRESIDING OFFICER. The question is on agreeing to the motion.

The motion was agreed to.

PROVIDING FOR CONGRESSIONAL DISAPPROVAL OF A RULE SUBMITTED BY THE FEDERAL COMMUNICATIONS COMMISSION

The PRESIDING OFFICER. The clerk will report the joint resolution.

The senior assistant legislative clerk read as follows:

A joint resolution (S.J. Res. 34) providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to ''Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.''

The PRESIDING OFFICER. The Senator from Arizona.

Mr. FLAKE. Mr. President, I rise in support of my resolution of disapproval under the Congressional Review Act of the FCC's broadband privacy restrictions. As chairman of the Senate Judiciary Committee's Privacy Subcommittee, I have spent more than a year closely examining this issue.

In February of 2015 the FCC, under then-Chairman Tom Wheeler, took the unprecedented step of reclassifying broadband providers as ''common carriers'' under title II of the Communications Act. In other words, on a 3-to-2 party-line vote, the FCC decided that internet service providers should be treated like telephone companies for regulatory purposes. The decision encroached on the Federal Trade Commission's jurisdiction to regulate ISP privacy policies, stripping these companies of their traditional privacy regulator.

Recognizing that his actions to impose net neutrality on ISPs created regulatory uncertainty, last spring Chairman Wheeler began to float the idea of implementing new FCC privacy rules. The FCC decided, again on a 3-to-2 party-line vote, to move forward with the rule change just before election day. The whole process was unsettling, to say the least.

The FCC ultimately decided to commandeer an area of regulatory authority for itself, without any meaningful check on this unilateral action. Once it initiated the bureaucratic power grab, it proceeded to establish new rules restricting the free speech of its regulatory target.

I submitted comments to the agency expressing my constitutional concerns about its proposed rule. I wasn't alone in doing so. Noted Harvard law professor Larry Tribe, hardly one to be confused for a conservative, did the same. But the rules were finalized nonetheless.

While the FCC recently took a step in the right direction by staying the application of the privacy rules, these midnight regulations are still hanging out there. Congress needs to repeal these privacy restrictions in order to restore balance to the internet ecosystem and provide certainty to consumers.

These regulations have altered the basic nature of privacy protection in the United States. For decades, the FTC policed privacy based on consumer expectations for their data, not bureaucratic preferences. These consumer expectations were just common sense: Sensitive data deserves more protection than nonsensitive data.

Unfortunately, the FCC rules dispensed with this commonsense regulatory approach. Under the new rules, what matters isn't what the data is but, rather, who uses it. This creates a dual-track regulatory environment where some consumer data is regulated one way if a company is using it under the FCC's jurisdiction and an entirely different way if its use falls under the FTC, or the Federal Trade Commission.

This is all confusing enough, but it gets worse. In the consumer technology sector, innovation is the name of the game. Companies are constantly rolling out new products and competing to win over consumers. By the same token, consumers are always on the lookout for the newest gadget or app. But the FCC's privacy order makes it increasingly difficult for consumers to learn about the latest product offerings from broadband providers. Instead of being notified about faster and more affordable alternatives for their family's home internet needs, under the FCC's privacy order, Arizonans might get left in the dark.

The FCC's heavyhanded data requirements restrict the ability of broadband providers to offer services tailored to their customers' needs and interests, and they lead to inconsistent treatment of otherwise identical data online. When a regulation diminishes innovation, harms consumer choice, and is just all-around confusing, it is a bad regulation. The FCC's privacy rule for ISPs is a bad regulation.

When it chose to impose needlessly onerous privacy regulations on broadband providers while leaving the rest of the internet under the successful FTC regime, the FCC unfairly picked one politically favored industry—the edge providers—to prevail over a different industry—broadband.

Repealing the FCC's privacy action is a crucial step toward restoring a single, uniform set of privacy rules for the internet. The FTC's privacy rules are the result of an ongoing, data-driven effort to understand and protect consumer expectations. That is the FTC. The FCC's rules, on the other hand, are the hasty byproduct of political interest groups and reflect the narrow preferences of well-connected insiders.

To sum all of this up, the FCC's midnight privacy rules are confusing and counterproductive. This CRA will get rid of it, pure and simple. But let me say what it won't do. Despite claims to the contrary, using this CRA will not leave consumers unprotected. That is because the FCC is already obligated to police the privacy practices of broadband providers under section 222 of the Communications Act, as well as various other Federal and State laws.

Both Chairman Wheeler and Chairman Pai agree on that point. Just last week, Chairman Pai wrote to my friends on the other side of the aisle confirming this legal fact.

This resolution will not disrupt the FCC's power, nor will it infringe on the FTC's jurisdiction elsewhere. Neither will it affect how broadband providers currently handle consumer data. Broadband providers are currently regulated under section 222, and they will continue to be after these midnight regulations are rescinded.

Passing this CRA will send a powerful message that Federal agencies can't unilaterally restrict constitutional rights and expect to get away with it. I urge my colleagues to support this resolution of disapproval.

I yield back the remainder of my time.

The PRESIDING OFFICER. The Senator from Florida.

Mr. NELSON. Mr. President, we are talking about taking privacy rights away from individuals if we suddenly eliminate this rule. Do you want a large company that is an internet provider, that has all the personal, sensitive information because of what you have been doing on the internet—do you want that company to be able to use that for commercial purposes without your consent? That is the issue.

If you want to protect people's privacy, I would think you would want to require that an individual who has paid money for the internet provider to provide them with the internet—you go on the internet, and you go to whatever site you want. You do business. You do personal business. You do banking. You go on the internet and you buy things. You talk about your children's school, about when you are going to pick up your children, maybe what your children want to wear to school. You want to talk on the internet about anything that is personal. Do you want that internet provider to have access to

that information to be used for commercial purposes without your consent? If you ask that question to the American people, they are going to give you a big, resounding no.

Should the internet provider use that information if you give your consent? Then that is fair game. If you give your consent so that they can alert you before a certain day—you might want to give a certain gift to your wife on her birthday, and they might have all that information, but maybe you don't want them to have the information about where your children go to school.

Personal, sensitive information is what we are talking about; therefore, the whole issue here is, do you want the internet provider to be able to use that information without the person's consent, or do you want the person to have to actually effectively opt-in in order to give the internet provider that consent? To me, this is a clear-cut case of privacy.

You can fancy it up, talking about FCC rules and so forth—and we have the author of the Telecom Act, Senator MARKEY, here, and he is going to talk about this and protections that were put in for telephones. But back then, remember, it was just you call from this number to this number on such and such a day for such and such a period of time. Even that was protected. But now—just think about this—we are talking about all the personal transactions that you do every day through the internet.

So I rise today in opposition to this resolution brought under the Congressional Review Act to disapprove the Federal Communications Commission's broadband consumer privacy rules. I would think that the distinguished Senator sitting in the Chair, who values privacy as he does—that this is going to be something he would be concerned about, as well as every other Senator in this Chamber, because you know that if you ask your constituents ''Do you want your privacy invaded without your consent?'' you know what the answer is going to be.

Americans care about their online privacy. They want to have control over how their personal information is exploited by third parties. In fact, a recent survey by the Pew Research Center found that 91 percent of adults feel they have lost control of how their personal information is collected and then used. That same study found that 74 percent of Americans believe it is very important that they be in control of who can get information about them, and a majority believe that their travels around the internet—the sites they visit and how long they spend in that location—are sensitive information that should be protected. I hope the Senators are going to pay attention to this because we are talking about sensitive, personal information.

Do you know that your geolocation is something that you are transmitting over the internet? Do you want your location and where you have been to be in the hands of somebody who could use that for commercial purposes? I don't think so. That is why this past October the FCC provided broadband subscribers with tools to allow them to have greater control over how their personal online information is used, shared, and then sold.

The FCC has been protecting telephone customers' privacy for decades, and it updated its longstanding privacy protections to protect the privacy of broadband customers. In fact, it is safe to say that what the FCC did last October was the most comprehensive update to its consumer privacy and data protection rules in decades.

The FCC put in place clear rules that require broadband providers to seek their subscribers' specific and informed consent before using or sharing sensitive personal information and give broadband customers the right to opt out of having their nonsensitive information used and shared if they chose to do so. The FCC also gave broadband subscribers additional confidence in the protection and security of their data by putting in place reasonable data security and breach notification requirements for broadband providers.

Simply put, the FCC decided to put American consumers—each one of us who pays these monthly fees for our broadband service—in the driver's seat of how their personal online data is used and shared by the broadband provider to which they have been paying a monthly fee to use their service. Is that too much to ask? I don't think so.

Please understand that broadband providers know a lot about every one of us. In fact, it may be startling, the picture that your broadband provider can develop about your daily habits and then sell to the highest bidder.

Your home broadband provider can know when you wake up every day either by knowing the time each morning that you log on to the internet to check the weather and news of the morning or through a connected device in your home.

That provider may know immediately that you are not feeling well, that you kind of feel sick, assuming you peruse the internet, like most of us do, to get a quick check on your symptoms. In fact, your broadband provider may know more about your health and your reaction to illness than you are willing to share with your doctor. Think about that.

Personal privacy? If you let this go to the highest bidder, personal privacy of sensitive information is going to be out the window.

Your home broadband provider can build a profile about your listening and viewing habits given that today most of us access music, news, and video programming over broadband.

Your broadband provider may have a better financial picture of you than even your bank or your brokerage firm or your financial adviser because they see every website you visit across every device in your home and can build a thorough profile about you through these habits.

If you live in a connected home, the home of the future—and the future is now, by the way—they may know even more details about how you go about your day-to-day activities. Your mobile broadband provider knows how you move about through the day, your geolocation. They know through information about that geolocation and the internet activity. All of that is through—guess what—this mobile device. Don't you think this is connected to the internet? And that is not to mention the sort of profile a broadband provider can start to build about our children from their birth. It is a gold mine of data, the holy grail, so to speak.

It is no wonder that broadband providers want to be able to sell this information to the highest bidder without the consumer's knowledge or consent. And they want to collect and use this information without providing transparency or being held accountable. Is this what you want to inflict upon your constituents in your State by changing this rule about their personal, sensitive privacy? I don't think so. You better know what you are doing when you vote tomorrow. This vote is coming about noon tomorrow. You better know.

As a country, we have not stood for this in the past, this kind of free utilization of information by entities that may want to have a unique look at who we are. We place stringent limits on the use of information by our doctors. We place stringent limits on our banks. When it comes to our children, I mean, that ought to be off-limits.

Broadband providers can build similar profiles about us and in fact may be able to provide more detail about someone than any one of those entities can. Passing this Senate resolution will take consumers out of the driver's seat and place the collection and use of their information behind a veil of secrecy, despite the rhetoric surrounding our debate today suggesting that eliminating these commonsense rules will better protect consumers' privacy online or will eliminate consumer confusion.

Don't fall for that argument, Senators. In fact, the resolution will wipe out thoughtful rules that were the product of months of hard work by the experts at the agency on regulating communications networks of all kinds. Those rules were crafted based upon a thorough record developed through an extensive multimonth rulemaking proceeding. The FCC received more than one-quarter of a million filings during this proceeding. They listened to the American people.

The agency received extensive input from stakeholders in all quarters of the debate, from the broadband providers and telephone companies to the public interest groups and from academics to individual consumers. We are going to wipe all of this away at noon tomorrow

with a vote that you can do it by 50 votes in this Chamber? I don't think this is what the people want.

On top of this, the rules are based on longstanding privacy protections maintained by the FCC for telephone companies, as well as the work of and the principles advocated by the Federal Trade Commission and advocated by State attorneys general and others in protecting consumer privacy. The FCC rules put in place basic safeguards for consumers' privacy based on three concepts that are widely accepted as the basis for privacy regulation in the United States and around the world: notice, choice—individual choice, consumer choice—and security, those three. They are not the radical proposals that some would have you believe they are.

First, the rules require broadband providers to notify their customers about what types of information it collects about the individual customers, when they disclose or permit access to that information, and how customers can provide consent to that collection and disclosure.

Second, the rules give consumers choice by requiring broadband providers to obtain a customer's affirmative opt in; in other words, I give you my consent before you can use or share my sensitive personal information.

As I mentioned earlier, sensitive information includes a customer's precise geographic location—I don't think you want some people to know exactly where you are—your personal information, health, financial, information about your children, your Social Security number—how many laws do we have protecting Social Security numbers—the content you have accumulated on the web, web browsing, and application usage information.

For information considered nonsensitive, broadband providers must allow customers to opt out of use and sharing of such information. Broadband providers must provide a simple, persistently available means for customers to exercise their privacy choices.

Third, broadband providers are required to take reasonable measures to protect customers' information from unauthorized use, disclosure, or access. They must also comply with specific breach notifications. In other words, if somebody has busted the internet and stolen all of this information from the site, don't you think you ought to be notified that your personal information was hacked? Well, that is one of the requirements.

So then I ask my colleagues: What in the world is wrong with requiring broadband providers to give their paying customers clear, understandable, and accurate information about what confidential and potentially highly personal information those companies collect? What is wrong with getting their consent to collect that information from their subscribers?

What is wrong with telling customers how their information is collected when they use their broadband service? What is wrong with telling customers with whom they share this sensitive information? What is wrong with letting customers have a say in how their information is used? What is wrong with recognizing that information about a consumer's browsing history and ap usage, sensitive and personal information, should be held to a higher standard before it is shared with others? What is wrong with all of that?

What is wrong with seeking a parent's consent before information about their children's activities or location is sold to the highest bidder? Do we as parents not go out of our way to protect our children's well-being and their privacy? Trying to overturn this rule is what is wrong.

What is wrong with protecting consumers from being forced to sign away their privacy rights in order to subscribe to a broadband service? I want your internet service. Do I have to sign away the rights to my private information—private, sensitive information? What is wrong with making companies take reasonable efforts to safeguard the security of consumers' data?

What is wrong with making companies notify their subscribers when they have had a breach? Again, I ask my colleagues: What in the world is wrong with giving consumers increased choice, transparency, and security online?

Supporters of the joint resolution fail to acknowledge the negative impact this resolution is going to have on the American people. This regulation is going to wipe away a set of reasonable, commonsense protections. I want to emphasize that. Is it common sense to protect our personal, sensitive, private information? Of course it is. But we are just about—in a vote at noon tomorrow, with a majority vote, not a 60-vote threshold, a majority vote here—we are just about to wipe all of that out. It will open our internet browsing histories and application usage patterns up to exploitation for commercial purposes by broadband providers and third parties who will line up to buy your information.

It will create a privacy-free zone for broadband companies, with no Federal regulator having effective tools to set rules of the road for collection, use, and sale of that uniquely personal information of yours. It will tie the hands of the FCC because they cannot go back. Once this rule is overturned, they cannot go back and redo this rule. It will tie the hands of the Federal Communications Commission and eliminate the future ability to adopt clear, effective privacy and data security protections for you as a subscriber, in some cases even for telephone subscribers.

To be sure, there are those who disagree with the FCC's broadband consumer privacy rules. There is an avenue for those complaints. These same companies that are pushing the joint resolution have filed for reconsideration of the rule at the FCC, and there is a judicial system. That is the appropriate way. Go back and get the FCC to amend—if you all are so concerned—or let the judicial system work its will, but do not do it in one fell swoop in a majority rule in this body tomorrow at noon.

In fact, the critics of the FCC's rules have an open proceeding at the FCC in which they can argue on the record with an opportunity for full public participation to change and alter these rules.

If the FCC did it—you have a new FCC, a new Chairman, a new majority on the FCC—let them be the ones to amend the rules after all the safeguards of the open hearings, of the comment period, all of that. By contrast, what we are using here to invade our privacy is a blunt congressional instrument called the Congressional Review Act. It means that all aspects of the rules adopted by the FCC must be overturned at once, including changes to the FCC's telephone privacy rules.

It would deny the agency the power to protect consumers' privacy online, and it would prevent the FCC—get this—prevent them, the FCC, the regulatory body that now has a new chairman and a new majority—it would prevent the FCC from ever adopting even similar rules. I don't think that is what we want to do because it does not make sense. That is exactly what we are about to do.

I also want to address the argument that the FCC rules are unfair to broadband providers because the same rules do not apply to other companies in the internet ecosystem. Supporters of this resolution will argue that the other entities in the internet ecosystem have access to the same personal information that the broadband providers do.

They argue that everyone in the data collection business should be on a level playing field. Well, I ask my colleagues whether they have asked their constituents that question directly. Do Americans really believe that all persons who hold data about them should be treated the same? I venture to guess that most Americans would agree with the FCC that companies that are able to build detailed particulars about you and build those particular pictures about your lives through unique insights because of what you do every day in their internet usage—shouldn't those companies be held to a higher standard?

In addition, the FCC's rules still allow broadband providers to collect and use their subscribers' information. The providers merely need to obtain consent from those activities when it comes to their subscribers' highly sensitive information.

The FCC also found that broadband providers, unlike any other companies in the internet ecosystem, are uniquely able to see every packet of information that a subscriber sends and receives—every packet of information that you

send or receive over the internet while on their networks. So if you have a provider, they are on your iPhone, and you are using them, they are seeing everything. That is not the case if you go to Google because Google sees only what you do while you are on Google. But the internet provider, the pipe that is carrying your information—they see everything that you do.

Supporters of the joint resolution also hold out the superiority of the Federal Trade Commission's efforts on protecting privacy. They argue that there should be only one privacy cop on the beat. But, folks, that ignores reality. The FTC doesn't do everything. There are a number of privacy cops on the beat. Congress has given the FCC, the FTC, the FDA, and NHTSA regulatory authority to protect consumers' privacy.

You had better get this clear because the FCC is the only agency to which Congress has given statutory authority to adopt rules to protect broadband customers' privacy. The FTC, the Federal Trade Commission, does not have the rulemaking authority in data security, even though commissioners at the FTC have asked Congress for such authority in the past. Given recent court cases, the FTC now faces even more insurmountable legal obstacles to taking action, protecting broadband consumers' privacy.

So don't be fooled by this argument that folks are telling you over here that it ought to be the FTC, the Federal Trade Commission. As many have pointed out, elimination of the FCC's rules will result in a very wide chasm, where broadband and cable companies have no discernible regulation while internet ''edge'' companies abide by the FTC enforcement efforts.

Without clear rules of the road, broadband subscribers will have no certainty of choice about how their private information can be used and no protection against its abuse—no protection, my fellow Americans, of your personal, sensitive, private data. That is why this Senator supports the FCC's broadband consumer privacy rules.

I want to encourage my fellow Senators: You had better examine what you are about to do to people's personal privacy before you vote to overturn this rule tomorrow.

I urge my colleagues to vote against the joint resolution.

Mr. President, I yield the floor.

The PRESIDING OFFICER (Mr. TILLIS). The Senator from South Dakota.

ORDERS FOR THURSDAY, MARCH 23, 2017

Mr. THUNE. Mr. President, I ask unanimous consent that when the Senate completes its business today, it adjourn until 9:30 a.m., Thursday, March 23; further, that following the prayer and pledge, the morning hour be deemed expired, the Journal of proceedings be approved to date, the time for the two leaders be reserved for their use later in the day, and morning business be closed; finally, that the Senate resume consideration of S.J. Res. 34.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

Mr. THUNE. Mr. President, the internet has grown at an unbounded rate in the years since its inception, a phenomenon no one can argue with. Much of that growth can be attributed to the light-touch regulatory approach that the government adopted in the early days of the web.

As chairman of the Commerce Committee, which has jurisdiction over the internet, I have worked hard to promote policies that encourage the private sector to invest in and grow the internet ecosystem as a whole. All of that is jeopardized, however, if government bureaucrats have the ability to overregulate the digital world. When it comes to overregulating the internet, one need look no further than the Democratic-controlled Federal Communications Commission under President Obama.

In a world that was turning away—it was literally turning away from the legacy telecommunication services and, instead, toward dynamic internet applications, the FCC found its role gradually diminishing. This is an inevitable and good byproduct, I might add, of a more competitive environment brought about by technological innovation and successful light-touch policies.

Yet the Obama FCC fought hard against this technological progress and, instead, pursued an aggressively activist and partisan agenda that put government edicts ahead of real consumer desires. Over the last 2 years, the FCC has made a stunning bureaucratic power grab. First, the FCC stripped away the Federal Trade Commission's authority to police internet providers and seized that for itself by recharacterizing such services as monopoly-era telecommunications.

Then in 2016, the FCC, which has little experience regulating internet privacy, decided to turn our country's privacy laws on their head by abandoning the time-tested enforcement approach of the FTC, the Federal Trade Commission. These actions by the FCC ignored both common sense and real world data and, instead, focused on hypothetical harms of the future.

Ignoring years of internet ecosystem precedent, where everyone was treated the same, the FCC's 2016 broadband privacy regulations would apply only to certain parts of the internet. This is a source of significant concern because at any particular time, consumers will not have reasonable certainty of what the rules are and how their privacy decisions will be applied.

Are you at home on Wi-Fi? At home on a smartphone? Using your smartphone on a friend's Wi-Fi? Using the Internet at a library? Each of these could have very different privacy implications for a consumer because of the FCC's piecemeal approach to privacy, leading to more confusion and uncertainty, not increased privacy protections, as promised.

In enacting these lopsided rules, the FCC seems to have gone out of its way to disregard established FTC practice by creating new regulations that differ significantly from the FTC's tried-and-true framework. The FTC's privacy regime is clear, easy to understand, and applies evenly throughout the marketplace. By contrast, the FCC's rules are complex, confusing, and often lead to the same data being treated inconsistently online.

The FCC's action would harm consumers in other ways as well. Even though no consumer wants to be in the dark about newer and cheaper services, the FCC's rules actually make it more difficult for customers to hear about new, innovative offerings from their broadband providers. And because the FCC imposed heavy-handed data requirements on these internet companies, they will have less ability to offer services that are tailored to their customers' needs and interests. Furthermore, the FCC unfairly distorted the marketplace when it imposed unnecessarily onerous privacy restrictions on broadband providers while leaving the rest of the internet under the strong and successful regime at the FTC.

When speaking about the economic opportunities the internet now affords us, President Obama's last FCC chairman declared that ''government is where we will work this out.''

''Government is where we will work this out.''

Well, I couldn't disagree more. I believe the marketplace should be the center of the debate over how our digital networks would function, not the FCC. I believe consumers and job creators should be the ones deciding about new technologies, not the government.

The resolution before us today is the first step toward restoring regulatory balance to the internet ecosystem. The best way for that balance to be achieved is for there to be a single, uniform set of privacy rules for the internet—the entire internet—rules that appropriately weigh the need to protect consumers with the need to foster economic growth and continued online innovation.

The FCC is simply the wrong venue for that effort. Its statutory scope is too narrow, and it lacks institutional expertise on privacy. The current chairmen of the FCC and the FTC both recognize this, having jointly called for returning jurisdiction over broadband providers' privacy and data security practices to the FTC ''so that all entities in the online space can be subject to the same rules.''

For those reasons, I support the resolution before us that would provide congressional disapproval of the Obama administration's misguided and unfair attempts to regulate the internet, and I encourage my colleagues to support the resolution as well.

To those people who have heard that this resolution somehow results in the elimination of all online protections for consumers, I can assure you those

claims are simply unfounded scaremongering. If this resolution is enacted, it will repeal only a specific rulemaking at the FCC that has yet to be implemented. What we are talking about here hasn't even been implemented yet. It will not touch the FCC's underlying statutory authority. Indeed, the FCC will still be obligated to police the privacy practices of broadband providers, as provided for in the Communications Act. The new chairman of the FCC confirmed this when he appeared before the Commerce Committee earlier this month. No matter what happens with this resolution, the FTC will continue to have its authority to police the rest of the online world.

It is my hope that once the Senate passes this resolution, the House will move quickly to take it up and send it to the President for his signature because, before our country can get back on the right track, we must first move past the damaging regulations adopted in the waning days of the Obama administration.

I thank Senator FLAKE for his leadership on this issue. Without his tireless efforts, we would not be here today, standing ready to move decisively toward a better future for the internet.

I urge my colleagues to support the resolution that we will vote on tomorrow at noon.

MORNING BUSINESS

COMMITTEE ON THE BUDGET

RULES OF PROCEDURE

Mr. ENZI. Mr. President, I ask unanimous consent that the rules of the Senate Committee on the Budget for the 115th Congress be printed in the RECORD.

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

RULES OF PROCEDURE

I. MEETINGS

(1) The committee shall hold its regular meeting on the first Thursday of each month. Additional meetings may be called by the chair as the chair deems necessary to expedite committee business.

(2) Each meeting of the committee, including meetings to conduct hearings, shall be open to the public, except that a portion or portions of any such meeting may be closed to the public if the committee determines by record vote in open session of a majority of the members of the committee present that the matters to be discussed or the testimony to be taken at such portion or portions—

(a) will disclose matters necessary to be kept secret in the interests of national defense or the confidential conduct of the foreign relations of the United States;

(b) will relate solely to matters of the committee staff personnel or internal staff management or procedure;

(c) will tend to charge an individual with crime or misconduct, to disgrace or injure the professional standing of an individual, or otherwise to expose an individual to public contempt or obloquy, or will represent a clearly unwarranted invasion of the privacy of an individual;

(d) will disclose the identity of any informer or law enforcement agent or will disclose any information relating to the investigation or prosecution of a criminal offense that is required to be kept secret in the interests of effective law enforcement; or

(e) will disclose information relating to the trade secrets or financial or commercial information pertaining specifically to a given person if—

(i) an act of Congress requires the information to be kept confidential by Government officers and employees; or

(ii) the information has been obtained by the Government on a confidential basis, other than through an application by such person for a specific Government financial or other benefit, and is required to be kept secret in order to prevent undue injury to the competitive position of such person.

(f) may divulge matters required to be kept confidential under other provisions of law or Government regulations.

(3) Notice of, and the agenda for, any business meeting or markup shall be provided to each member and made available to the public at least 72 hours prior to such meeting or markup.

II. CONSIDERATION OF BUDGET RESOLUTIONS

(1) If the chair of the committee makes proposed legislative text of a concurrent resolution on the budget available to all committee members by 12:00 p.m., five days prior to the start of a meeting or markup to consider the resolution, during that meeting or markup:

(a) it shall not be in order to consider a first degree amendment unless the amendment has been submitted to the chief clerk by 5:00 p.m. two days prior to the start of the meeting or markup, except that an amendment in the nature of a substitute offered by the chair of the committee shall not be required to be filed in advance, and

(b) it shall not be in order to consider a second degree amendment unless the amendment has been submitted to the chief clerk by 5:00 p.m. on the day prior to the start of the meeting or markup, and

(c) it shall not be in order to consider a side-by-side amendment unless the amendment has been submitted to the chief clerk by 5:00 p.m. on the day prior to the start of the meeting or markup, and the amendment is filed in relation to a particular first degree amendment that is considered by the committee.

(2) During consideration of a concurrent resolution on the budget, it shall not be in order to consider an amendment that would have no force or effect if adopted.

III. ORDER OF RECOGNITION

Those members who are present at the start of any meeting of the committee including meetings to conduct hearings, shall be recognized in order of seniority based on time served as a member of the committee. Any members arriving after the start of the meeting shall be recognized, in order of appearance, after the most junior member.

IV. QUORUMS AND VOTING

(1) Except as provided in paragraphs (2) and (3) of this section, a quorum for the transaction of committee business shall consist of not less than one-third of the membership of the entire committee: Provided, that proxies shall not be counted in making a quorum.

(2) A majority of the committee shall constitute a quorum for reporting budget resolutions, legislative measures or recommendations: Provided, that proxies shall not be counted in making a quorum.

(3) For the purpose of taking sworn or unsworn testimony, a quorum of the committee shall consist of one Senator.

(4)(a) The committee may poll—

(i) internal committee matters including those concerning the committee's staff, records, and budget;

(ii) steps in an investigation, including issuance of subpoenas, applications for immunity orders, and requests for documents from agencies; and

(iii) other committee business that the committee has designated for polling at a meeting, except that the committee may not vote by poll on reporting to the Senate any measure, matter, or recommendation, and may not vote by poll on closing a meeting or hearing to the public.

(b) To conduct a poll, the chair shall circulate polling sheets to each member specifying the matter being polled and the time limit for completion of the poll. If any member requests, the matter shall be held for a meeting rather than being polled. The chief clerk shall keep a record of polls; if the committee determines by record vote in open session of a majority of the members of the committee present that the polled matter is one of those enumerated in rule I(2)(a)–(e), then the record of the poll shall be confidential. Any member may move at the committee meeting following a poll for a vote on the polled decision.

V. PROXIES

When a record vote is taken in the committee on any bill, resolution, amendment, or any other question, a quorum being present, a member who is unable to attend the meeting may vote by proxy if the absent member has been informed of the matter on which the vote is being recorded and has affirmatively requested to be so recorded; except that no member may vote by proxy during the deliberations on Budget Resolutions unless a member is experiencing a health issue and the chair and ranking member agree to allow that member to vote by proxy on amendments to a Budget Resolution.

VI. HEARINGS AND HEARING PROCEDURES

(1) The committee shall make public announcement of the date, place, time, and subject matter of any hearing to be conducted on any measure or matter at least 1 week in advance of such hearing, unless the chair and ranking member determine that there is good cause to begin such hearing at an earlier date.

(2) At least 24 hours prior to the scheduled start time of the hearing, a witness appearing before the committee shall file a written statement of proposed testimony with the chief clerk who is responsible for circulating the proposed testimony to all members at the same time. The requirement that a witness submit testimony 24 hours prior to a hearing may be waived by the chair and the ranking member, following their determination that there is good cause for the failure of compliance.

VII. COMMITTEE REPORTS

(1) When the committee has ordered a measure or recommendation reported, following final action, the report thereon shall be filed in the Senate at the earliest practicable time.

(2) A member of the committee, who gives notice of an intention to file supplemental, minority, or additional views at the time of final committee approval of a measure or matter, shall be entitled to not less than 3 calendar days in which to file such views, in writing, with the chief clerk of the committee. Such views shall then be included in the committee report and printed in the same volume, as a part thereof, and their inclusions shall be noted on the cover of the report. In the absence of timely notice, the committee report may be filed and printed immediately without such views.