quite clear to me, having listened to two colleagues—whom I respect very much—that they are very much aware that their bill has attracted widespread opposition. The comment was made that Apple, Google, everyone should be for this.

I would say again—respectfully to my colleagues, the authors, with whom I have served since we all came to the committee together—even with the managers' amendment, the core privacy issues are not being dealt with.

I would just read now from a few of the comments—maybe I am missing something. Maybe I heard a list of all the privacy issues that had been addressed. I haven't seen any privacy groups the Democrats or Republicans look to saying they support the privacy protections in the bill, but let me give you an example of a few who surely don't.

This is what Yelp says: ''Congress is trying to pass a 'cyber security' bill that threatens your privacy.''

This is what the American Library Association is saying. I will admit, Mr. President, I am a little bit tilted toward librarians because my late mother was a librarian. We all appreciate the librarians we grew up with. The librarians say that this bill ''de facto grants broad new mass data collection powers to many federal, as well as state and even local government agencies.''

Salesforce, a major player in the digital space located in California, says:

At Salesforce, trust is our number one value and nothing is more important to our company than the privacy of our customers' data. . . . Salesforce does not support CISA and has never supported CISA.

They have a hashtag.

Follow #StopCISA for updates.

This is the group that represents the Computer and Communications Industry Association—this is Google, Amazon, and Microsoft, the biggest major tech companies. Again, these are companies with millions of customers, and the companies are worried that this bill lacks privacy protections and their customers are going to lose confidence in some of what may be done under this. They say they support the goals, of course—which we all do—of dealing with real threats and sharing information. They state: ''But such a system should not come at the expense of users' privacy, need not be used for purposes unrelated to cyber security, and must not enable activities that might actively destabilize the infrastructure the bill aims to protect.''

Mr. President, we heard my colleague, the chair of the committee, a member of the Committee on Finance whom I have worked with often, say that the most important feature of the legislation is that it is voluntary. The fact is that it is voluntary for companies. It will be mandatory for their customers. And the fact is that companies can participate without the knowledge and consent of their customers, and they are immune from customer oversight and lawsuits if they do so. I am all for companies sharing information about malware and foreign hackers with the government, but there ought to be a strong requirement to filter out unrelated personal information about customers.

I want to emphasize this because this is probably my strongest point of disagreement with my friends who are the sponsors. There is not in this bill a strong requirement to filter out unrelated personal information about these millions of customers who are going to be affected. This bill would allow companies to hand over a large amount of private and personal information about millions of their customers with only a cursory review. In my judgment, information about those who have been victims of hacks should not be treated in essentially the same way as information about the hackers. Without a strong requirement to filter out unrelated personal information, that is unfortunately what this bill does.

At the outset of this discussion, we were told this bill would have substantial security benefits. I heard for days, for example, that this bill would have prevented the OPM attack, that it would have stopped the serious attack on government personnel records. After technologists reviewed that particular argument, that claim has essentially been withdrawn.

There is a saying now in the cyber security field: If you can't protect it, don't collect it. If more personal consumer information flows to the government without strong protections, my view is it is going to end up being a prime target for hackers.

Sharing information about cyber security threats is clearly a worthy goal, and I would like to find ways to encourage more of that responsibly. Yet if you share more information without strong privacy protections, millions of Americans will say: That is not a cyber security bill; it is a surveillance bill. My hope is that, working in a bipartisan way, by the time we have completed this legislation on the floor, that will not be the case.

Mr. President, I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

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

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

Mr. BURR. Mr. President, I listened patiently to my friend and colleague, and we are on the committee together, so this is not the first time we have had a frank discussion. But let me say to those companies that have reached out to him, and he listed them—I am not going to bother going through 53 associations and the number of companies that are represented because there are hundreds and hundreds. They are sectors of our economy. It is the financial industry. It is automotive. It is practically everybody in retail.

There are a couple of things that still shock me because I really can't make the connection. A technology company has a tremendous amount of users, and those users put their personal data on that—pick one—and the company says there is nothing more important than protecting the data of their users. It strikes me, because I was in business for 17 years before I came to this insane place, that any business in the world would say: I don't have a problem with putting this in place as long as I don't have to use it. I can make a decision whether I use it or whether I don't.

It may be that when they get an opportunity to see the final product and it is in place, they may say: Well, you know what, this isn't so bad. This actually took care of some of the concerns we have.

But to make a blanket statement for a company whose No. 1 concern is the protection of its customers' data—to ignore the threat today that is real and will be felt by everybody, if it hasn't been felt by them, and not have something in place is irresponsible by those companies.

Again, I point to the fact that if this were a mandatory program, I could understand why they might, for market share reasons or marketing reasons, go out and say: We are not covered by this. But this is voluntary for everybody. There is not a soul in the world who has to participate. But the ones that are really concerned about their customers' data, the ones that really understand there are companies, individuals, and countries trying to hack their systems will succumb to the fact that something is better than nothing.

It is sort of like going home to North Carolina—and I see the leader is coming—where this year we have had a rash of sharks. It is one thing to know there are sharks out there and swim and say: How could one bite me? Well, you know you have hackers out there. It seems as if you take precautions when you go swimming, and it seems as if you should take precautions to keep from being hacked.

With that, I yield the floor.

The PRESIDING OFFICER. The majority leader.

CYBERSECURITY INFORMATION SHARING ACT of 2015

Mr. MCCONNELL. Mr. President, under the order of August 5, 2015, I ask that the Chair lay before the Senate S. 754.

The PRESIDING OFFICER. Under the previous order, the Senate will proceed to the consideration of S. 754, which the clerk will report.

The senior assistant legislative clerk read as follows:

A bill (S. 754) to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

The PRESIDING OFFICER. The Senator from North Carolina.

AMENDMENT NO. 2716

(Purpose: In the nature of a substitute)

Mr. BURR. Mr. President, as under the previous order, I call up the Burr-Feinstein amendment, which is at the desk, and I ask unanimous consent that it be reported by number.

The PRESIDING OFFICER. Without objection, the clerk will report the amendment by number.

The senior assistant legislative clerk read as follows:

The Senator from North Carolina [Mr. BURR] proposes an amendment numbered 2716.

(The amendment is printed in today's RECORD under ''Text of Amendments.'')

Mr. BURR. Mr. President, for the information of all Senators, this substitute includes agreed-upon language on the following amendments: Carper, No. 2615; Carper, No. 2627; Coats, No. 2604; Flake, No. 2580; Gardner, No. 2631; Kirk, No. 2603; Tester, No. 2632; Wyden, No. 2622, and, I might add, a handful of amendments that have been worked out in addition to those which were part of that unanimous consent agreement by both the vice chair and myself.

The vice chair and I have a number of amendments to be made pending under the previous consent order, and I ask unanimous consent that they be called up and reported by number.

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

AMENDMENT NO. 2581, AS MODIFIED, TO AMENDMENT NO. 2716

Mr. BURR. Mr. President, I call up the Cotton amendment No. 2581, as modified, to correct the instruction line.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from North Carolina [Mr. BURR], for Mr. COTTON, proposes an amendment numbered 2581, as modified, to amendment No. 2716.

The amendment is as follows:

(Purpose: To exempt from the capability and process within the Department of Homeland Security communication between a private entity and the Federal Bureau of Investigation or the United States Secret Service regarding cybersecurity threats)

On page 31, strike line 13 and insert the following:

authority regarding a cybersecurity threat; and

(iii) communications between a private entity and the Federal Bureau of Investigation or the United States Secret Service regarding a cybersecurity threat;

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Mr. President, let me add at this time that the vice chairman and I have worked aggressively, as have our staffs, to incorporate the suggestions and the concerns Members and companies have raised with us. If we believed they made the legislation stronger—stronger from the standpoint of minimizing data loss and stronger from the standpoint of the privacy concerns—let me assure my colleagues we have accepted those and we have incorporated them in the managers' amendment. If, in fact, we couldn't agree or felt that it in any way was detrimental to the legislation, the vice chair and I have agreed to oppose those amendments.

I think it is important that this bill represent exactly what we have sold: an information sharing bill, a bill that is voluntary.

So I would suggest to those who hear this debate and say ''I don't really understand all this cyber stuff. I hear about it and don't really understand it,'' let me put it in these terms. What this legislation does is it creates a community watch program, and like any neighborhood watch program, the spirit of what we are trying to do is to protect the neighborhood. It doesn't mean that every resident on every street in that community in that neighborhood is going to be a participant, but it means that neighborhood is committed to making sure that if crimes are happening, they are out there to stop them, to report them, and maybe through reporting them, the number of crimes over time will continue to decrease.

Well, I would share with you that is what we are doing with the cyber security bill. We are out now trying to set up the framework for a community watch program, one that is voluntary, that doesn't require every person to participate, but it says: For those of you who can embrace this and can report the crimes, it is not only beneficial to you, it is beneficial to everybody.

So I respect the fact there are a few companies out there saying: This is no good; we shouldn't have this. Really? Do you want to deny this to everybody? There are a heck of a lot of businesses that have made the determination that this is beneficial to their business, that it is beneficial to their sector.

This is beneficial to the overall U.S. economy. That is what the Senate is here to do. We are not here to pick winners and losers; we are here to create a framework everybody can operate in that advances the United States in the right direction.

Shortly we will have an opportunity to make pending some additional amendments, and I encourage all Members, if your amendment is pending, to come down and debate it. If you have additional amendments, please come down and offer them and debate them. With the cooperation of Members, we can process these in a matter of days and we can then send this out of the Senate and be at a point where we could conference with the House.

With that, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mrs. FEINSTEIN. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Ms. AYOTTE). Without objection, it is so ordered.

AMENDMENT NO. 2552, AS MODIFIED, TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Coons amendment No. 2552, as modified.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Mr. COONS, proposes an amendment numbered 2552, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To modify section 5 to require DHS to review all cyber threat indicators and countermeasures in order to remove certain personal information)

Beginning on page 23, strike line 3 and all that follows through page 33, line 10 and insert the following:

(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines required by subsection (b), the policies and procedures developed and promulgated under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4 that are received through the process described in subsection (c) of this section and that satisfy the requirements of the guidelines developed under subsection (b)—

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 4 in a manner other than the process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(C) consistent with this Act, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled ''National Strategy for Trusted Identities in Cyberspace'' and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this Act, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and

(D) ensure there is—

(i) an audit capability; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this Act in an unauthorized manner.

(4) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this Act.

(B) CONTENTS.—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this Act that would be unlikely to include personal information of or identifying a specific person not necessary to describe or identify a cyber security threat.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be necessary to describe or identify a cybersecurity threat.

(iii) Such other matters as the Attorney General considers appropriate for entities sharing cyber threat indicators with Federal entities under this Act.

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Attorney General considers relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically review the guidelines promulgated under subparagraph (A).

(3) CONTENT.—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the impact on privacy and civil liberties of activities by the Federal Government under this Act;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or identifying specific persons, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this Act; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) protect the confidentiality of cyber threat indicators containing personal information of or identifying specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this Act; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

(A) shall accept from any entity in real time cyber threat indicators and defensive measures, pursuant to this section;

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this Act that are shared by a private entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator; and

(ii) communications by a regulated entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) shall require the Department of Homeland Security to review all cyber threat indicators and defensive measures received and remove any personal information of or identifying a specific person not necessary to identify or describe the cybersecurity threat before sharing such indicator or defensive measure with appropriate Federal entities;

(D) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators as quickly as operationally possible from the Department of Homeland Security;

(E) is in compliance with the policies, procedures, and guidelines required by this section; and

(F) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) reporting of known or suspected criminal activity, by an entity to any other entity or a Federal entity;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

(2) CERTIFICATION.—Not later than 10 days prior to the implementation of the capability and process required by paragraph (1), the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, certify to Congress whether such capability and process fully and effectively operates—

(A) as the process by which the Federal Government receives from any entity a cyber threat indicator or defensive measure under this Act; and

(B) in accordance with the policies, procedures, and guidelines developed under this section.

(3) PUBLIC NOTICE AND ACCESS.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures as quickly as operationally practicable with receipt through the process within the Department of Homeland Security.

The PRESIDING OFFICER. The Senator from North Carolina.

AMENDMENT NO. 2582 TO AMENDMENT NO. 2716

Mr. BURR. Madam President, I call up the Flake amendment No. 2582.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from North Carolina [Mr. BURR], for Mr. FLAKE, proposes an amendment numbered 2582 to amendment No. 2716.

The amendment is as follows:

(Purpose: To terminate the provisions of the Act after six years)

At the end, add the following:

SEC. 11. EFFECTIVE PERIOD.

(a) IN GENERAL.—Except as provided in subsection (b), this Act and the amendments made by this Act shall be in effect during the 6-year period beginning on the date of the enactment of this Act.

(b) EXCEPTION.—With respect to any action authorized by this Act or information obtained pursuant to an action authorized by this Act, which occurred before the date on which the provisions referred to in subsection (a) cease to have effect, the provisions of this Act shall continue in effect.

The PRESIDING OFFICER. The Senator from California.

AMENDMENT NO. 2612, AS MODIFIED, TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Franken amendment No. 2612, as modified.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Mr. FRANKEN, proposes an amendment numbered 2612, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To improve the definitions of cybersecurity threat and cyber threat indicator)

Beginning on page 4, strike line 12 and all that follows through page 5, line 21, and insert the following:

system that is reasonably likely to result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term ''cybersecurity threat'' does not include any action that

solely involves a violation of a consumer term of service or a consumer licensing agreement.

(6) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such information is not otherwise prohibited by law; or

The PRESIDING OFFICER. The Senator from North Carolina.

AMENDMENT NO. 2548, AS MODIFIED, TO AMENDMENT NO. 2716

Mr. BURR. Madam President, I call up the Heller amendment No. 2548, as modified, to correct the instruction line.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from North Carolina [Mr. BURR], for Mr. HELLER, proposes an amendment numbered 2548, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To protect information that is reasonably believed to be personal information or information that identifies a specific person)

On page 12, line 19, strike ''knows'' and insert ''reasonably believes''.

The PRESIDING OFFICER. The Senator from California.

AMENDMENT NO. 2587, AS MODIFIED, TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Leahy amendment No. 2587, as modified.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Mr. LEAHY, proposes an amendment numbered 2587, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To strike the FOIA exemption)

Beginning on page 35, strike line 1 and all that follows through page 35, line 13.

The PRESIDING OFFICER. The Senator from North Carolina.

AMENDMENT NO. 2564, AS MODIFIED, TO AMENDMENT NO. 2716

Mr. BURR. Madam President, I call up the Paul amendment No. 2564, as modified, to correct the instruction line.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from North Carolina [Mr. BURR], for Mr. PAUL, proposes an amendment numbered 2564, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To prohibit liability immunity to applying to private entities that break user or privacy agreements with customers)

On page 40, after line 24, insert the following:

(d) EXCEPTION.—This section shall not apply to any private entity that, in the course of monitoring information under section 4(a) or sharing information under section 4(c), breaks a user agreement or privacy agreement with a customer of the private entity.

The PRESIDING OFFICER. The Senator from California.

AMENDMENT NO. 2557 TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Mikulski amendment No. 2557.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Ms. MIKULSKI, proposes an amendment numbered 2557 to amendment No. 2716.

The amendment is as follows:

(Purpose: To provide amounts necessary for accelerated cybersecurity in response to data breaches)

At the appropriate place, insert the following:

SEC. _____. FUNDING.

(a) IN GENERAL.—Effective on the date of enactment of this Act, there is appropriated, out of any money in the Treasury not otherwise appropriated, for the fiscal year ending September 30, 2015, an additional amount for the appropriations account appropriated under the heading ''SALARIES AND EXPENSES'' under the heading ''OFFICE OF PERSONNEL MANAGEMENT'', $37,000,000, to remain available until September 30, 2017, for accelerated cybersecurity in response to data breaches.

(b) EMERGENCY DESIGNATION.—The amount appropriated under subsection (a) is designated by the Congress as an emergency requirement pursuant to section 251(b)(2)(A)(i) of the Balanced Budget and Emergency Deficit Control Act of 1985, and shall be available only if the President subsequently so designates such amount and transmits such designation to the Congress.

AMENDMENT NO. 2626 TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Whitehouse amendment No. 2626.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Mr. WHITEHOUSE, proposes an amendment numbered 2626 to amendment No. 2716.

The amendment is as follows:

(Purpose: To amend title 18, United States Code, to protect Americans from cybercrime)

At the end, add the following:

SEC. ___. STOPPING THE SALE OF AMERICANS' FINANCIAL INFORMATION.

Section 1029(h) of title 18, United States Code, is amended by striking ''if—'' and all that follows through ''therefrom.'' and inserting ''if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other Territory of the United States.''.

SEC. ___. SHUTTING DOWN BOTNETS.

(a) AMENDMENT.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting ''**and abuse**'' after ''**fraud**'';

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking ''or'' at the end;

(ii) in subparagraph (C), by inserting ''or'' after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

''(D) violating or about to violate paragraph (1), (4), (5), or (7) of section 1030(a) where such conduct would affect 100 or more protected computers (as defined in section 1030) during any 1-year period, including by denying access to or operation of the computers, installing malicious software on the computers, or using the computers without authorization;''; and

(B) in paragraph (2), by inserting '', a violation described in subsection (a)(1)(D),'' before ''or a Federal''; and

(3) by adding at the end the following:

''(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—

''(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

''(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in complying with the restraining order, prohibition, or other action.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of section for chapter 63 is amended by striking the item relating to section 1345 and inserting the following:

''1345. Injunctions against fraud and abuse.''.

SEC. ___. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer, if such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with such computer.

''(b) PENALTY.—Any person who violates subsection (a) shall, in addition to the term of punishment provided for the felony violation of section 1030, be fined under this title, imprisoned for not more than 20 years, or both.

''(c) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place any person convicted of a violation of this section on probation;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for the felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such violation to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, if such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

''(d) DEFINITIONS.—In this section

''(1) the terms 'computer' and 'damage' have the meanings given the terms in section 1030; and

''(2) the term 'critical infrastructure' has the meaning given the term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).''.

(b) TABLE OF SECTIONS.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. ___. STOPPING TRAFFICKING IN BOTNETS.

(a) IN GENERAL.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a), by striking paragraph (6) and inserting the following:

''(6) knowing such conduct to be wrongful, intentionally traffics in any password or similar information, or any other means of access, further knowing or having reason to know that a protected computer would be accessed or damaged without authorization in a manner prohibited by this section as the result of such trafficking;'';

(2) in subsection (c)—

(A) in paragraph (2), by striking '', (a)(3), or (a)(6)'' each place it appears and inserting ''or (a)(3)''; and

(B) in paragraph (4)—

(i) in subparagraph (C)(i), by striking ''or an attempt to commit an offense''; and

(ii) in subparagraph (D), by striking clause (ii) and inserting the following:

''(ii) an offense, or an attempt to commit an offense, under subsection (a)(6);''; and

(3) in subsection (g), in the first sentence, by inserting '', except for a violation of subsection (a)(6),'' after ''of this section''.

AMENDMENT NO. 2621, AS MODIFIED, TO AMENDMENT NO. 2716

Mrs. FEINSTEIN. Madam President, I call up the Wyden amendment No. 2621, as modified.

The PRESIDING OFFICER. The clerk will report the amendment by number.

The bill clerk read as follows:

The Senator from California [Mrs. FEINSTEIN], for Mr. WYDEN, proposes an amendment numbered 2621, as modified, to amendment No. 2716.

The amendment, as modified, is as follows:

(Purpose: To improve the requirements relating to removal of personal information from cyber threat indicators before sharing)

On page 17, strike lines 9 through 22 and insert the following:

(A) review such cyber threat indicator and remove, to the extent feasible, any personal information of or identifying a specific individual that is not necessary to describe or identity a cybersecurity threat; or

(B) implement and utilize a technical capability configured to remove, to the extent feasible, any personal information of or identifying a specific individual contained within such indicator that is not necessary to describe or identify a cybersecurity threat.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, as the vice chair and I have said numerous times this afternoon, nothing would make us happier than for Members to come to the floor. We have amendments pending. We have a managers' amendment. Everybody knows exactly what is in this bill. Let's start the debate. Let's vote on amendments. Let's end this process in a matter of days. We are prepared to vote on every amendment.

So at this time, I ask unanimous consent that on Thursday, October 22, at 11 a.m., the Senate vote on the pending amendments to the Burr-Feinstein substitute to S. 754, with a 60-vote threshold for those amendments that are not germane; and that following the disposition of the amendments, the substitute, as amended, if amended, be agreed to, the bill, as amended, be read a third time, and the Senate vote on passage with a 60-vote threshold for passage.

The PRESIDING OFFICER. Is there objection?

Mr. WYDEN. Reserving the right to object.

The PRESIDING OFFICER. The Senator from Oregon.

Mr. WYDEN. Madam President, I certainly support most of the amendments that were just described. However, I am especially troubled about amendment No. 2626, which would significantly expand a badly outdated Computer Fraud and Abuse Act. I have sought to modernize the Computer Fraud and Abuse Act, and I believe that amendment No. 2626 would take that law—the Computer Fraud and Abuse Act—in the wrong direction. I would object to any unanimous consent request that includes that amendment. Therefore, I object to this request.

The PRESIDING OFFICER. Objection is heard.

The Senator from North Carolina.

Mr. BURR. Madam President, the Senate functions best when Members are free to come to the floor and offer amendments, debate the amendments, and have a vote on the amendments. I might even share Senator WYDEN's concerns about that particular piece of legislation. I am not sure. It is a judiciary issue. The vice chair is on the Judiciary Committee. It is an amendment that we were not able to pass in the managers' amendment. But as the vice chair and I said at the beginning of this process, we would like the Senate to function like it is designed, where every Member feels invested, and if they have a great idea, come down, introduce it as an amendment, debate it, and let your colleagues vote up or down against it. If we can't move forward with a process like that, then it is difficult to see how in a reasonable amount of time we are going to complete this agenda.

So I would only urge my colleague from Oregon that there is nothing to be scared about. This is a process we will go through, and a nongermane amendment, which I think this would be listed as—I look for my staff. It would be a nongermane amendment—requiring 60 votes, a threshold that the Senate designed to pass practically anything.

So I urge him to reconsider at some point, and I will make a similar unanimous consent request once he has had an opportunity to think about it. But also, we will work to see if in fact that amendment might be modified in a way that might make it a little more acceptable for the debate and for colleagues to vote on it.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from Utah.

Mr. HATCH. Madam President, as the Senate turns its focus to legislation related to the critical issue of our Nation's cyber security and in the light of Chinese President Xi Jinping's state visit last month, I would like to reflect on America's security in cyber space.

As the global economy becomes increasingly dependent on the Internet, the exponential increase in the number and scale of cyber attacks and cyber thefts are straining our relationship with international trading partners throughout the world. This is especially true for our important trade relationship with China. This year alone, the United States has experienced some of the largest cyber attacks in our Nation's history—many of which are believed to have been perpetrated by the Chinese. Just last February, hackers breached the customer records of the health insurance company Anthem Blue Cross Blue Shield. Many news sources reported that China was responsible for the attack. This cyber attack resulted in the theft of approximately 80 million customers' personally identifiable information, including Social Security numbers and information that can be used for identity theft.

In the early summer, cyber criminals also hacked United Airlines, compromising manifest data that detailed the movement of millions of Americans. According to the news media, China was again believed to have been responsible.

But the most devastating cyber attack this year was on the U.S. Government's Office of Personnel Management. This past June, sources report that the OPM data breach, considered the worst cyber intrusion ever perpetrated against the U.S. Government,

affected about 21.5 million Federal employees and contractors. Hackers successfully accessed sensitive personal information, including security clearance files, Social Security numbers, and information about employees' contacts and families. Again, China was the suspected culprit.

Most troubling, the OPM breach included over 19.7 million background investigation records for cleared U.S. Government employees. The exposure of this highly sensitive information not only puts our national security at risk but also raises concern that foreign governments may be keeping detailed databases on Federal workers and their associations.

I was pleased during the Chinese President's visit to Washington last month that President Obama expressed his ''very serious concerns about growing cyber threats'' and stated that the cyber theft of intellectual property and commercial trade secrets ''has to stop.'' President Obama and President Xi Jinping came to an agreement not to ''conduct or knowingly support'' cyber theft of intellectual property or commercial trade secrets.

Even so, Director of Intelligence James Clapper expressed doubts about the agreement in a hearing before the Senate Armed Services Committee last week. When Chairman MCCAIN asked Mr. Clapper if he was optimistic about the deal, he told members of the committee he was not. I add my skepticism of this agreement to the growing chorus of lawmakers, military leaders, and intelligence community personnel who have voiced similar concerns.

As Admiral Rogers, head of the National Security Agency and U.S. Cyber Command, has said, ''China is the biggest proponent of cyberattacks being waged against the U.S.'' We must do more to defend ourselves against this growing threat. Unfortunately, I have been disappointed in this administration's inability to protect our Federal computer systems from cyber intrusions and to hold criminals accountable for their participation in cyber attacks committed against the United States. Sadly, the cyber threats facing our Nation are not limited to China. Investigators believe Russia, North Korea, Iran, and several other nations have also launched cyber attacks against our government, U.S. citizens, and of course companies. These attacks are increasing both in severity and in number.

In April, Russian hackers accessed White House networks containing sensitive information, including emails sent and received by the President himself.

In May, hackers breached IRS servers to gain access to 330,000 American taxpayers' tax returns. That same month a fraudulent stock trader manipulated U.S. markets, costing the stock exchange an estimated $1 trillion in just 36 minutes. In July, it was reported that a Russian spear phishing attack shut down the Joint Chiefs of Staff email system for 11 days. Just 1 month ago, hackers stole the personal data of 15 million T-Mobile customers by breaching Experian, the company that processes credit checks for prospective customers. This stolen data includes names, birth dates, addresses, Social Security numbers, and credit card information.

These breaches have a serious and real cost for the victims. According to the Federal Trade Commission, the average identity fraud victim in 2012 incurred an average of $365 in losses. Incredibly, all of these high-profile breaches have occurred this year, making 2015 perhaps the worst year ever in terms of attacks on our national cyber security.

Prior to 2015, we also saw several high-profile breaches at large American corporations, including Target, Home Depot, Sony, and others. Our lack of effective cyber security policies and procedures threatens the safety of our people, the strength of our national defense, and the future of our economy. We must be more vigilant in reinforcing our cyber infrastructure to better defend ourselves against these attacks. In doing so, Congress must create a deterrent for those who seek to commit cyber attacks against our Nation. Our adversaries must know they will suffer dire consequences if they attack the United States. Finding a solution to this critical problem must be an urgent priority for the Senate.

I agree with Leader MCCONNELL that we must move forward in the Senate with legislation to improve our Nation's cyber security practices and policies. I am supportive of the objectives outlined in Chairman BURR and Vice Chairperson FEINSTEIN's bipartisan Cybersecurity Information Sharing Act, CISA.

I was pleased to see the Senate Select Committee on Intelligence pass the Burr-Feinstein CISA bill out of the committee by an overwhelming bipartisan vote of 14 to 1. This important legislation incentivizes and authorizes private sector companies to voluntarily share cyber threat information in real time that can be useful in detecting cyber attacks and in preventing future cyber intrusions.

I also commend Chairman BURR and Vice Chairman FEINSTEIN's efforts to include provisions in CISA to protect personal privacy, including a measure that prevents a user's personally identifiable information from being shared with government agencies. Additionally, CISA sets limits on information that can be collected or monitored by allowing information to be used only for cyber security purposes.

As the American economy grows ever more dependent on the Internet, I believe CISA represents an important first step in protecting our Nation's critical infrastructure from the devastating impact of cyber attacks. Congress must do more to adequately protect and secure America's presence in cyber space.

In light of recent revelations highlighting our Federal Government's inability to adequately protect and secure classified data and other sensitive information, I joined Senator CARPER, the ranking member of the Homeland Security and Governmental Affairs Committee, in introducing the Federal Computer Security Act.

The Hatch-Carper bill shines light on whether our Federal Government is using the most up-to-date cyber security practices and software to protect Federal computer systems and databases from both external cyber attackers and insider threats. Specifically, this legislation requires Federal agency inspectors general to report to Congress on the security practices and software used to safeguard classified and personally identifiable information on Federal computer systems themselves.

This bill also requires each Federal agency to submit a report to each respective congressional committee with oversight jurisdiction describing in detail to each committee which security access controls the agency is implementing to protect unauthorized access to classified and sensitive, personally identifiable information on government computers.

Requiring an accounting of each Federal agency's security practices, software, and technology is a logical first step in bolstering our Nation's cyber infrastructure. These reports will guide Congress in crafting legislation to prevent future large-scale data breaches and ensure that unauthorized users are not able to access classified and sensitive information.

Agencies should be employing multifactor authentication policies and should be implementing software to detect and monitor cyber security threats. They should also be using the most up-to-date technology and security controls. The future of our Nation's cyber security starts with our Federal Government practicing good cyber hygiene. In strengthening our security infrastructure, the Federal Government should be accountable to the American people, especially when cyber attacks affect millions of taxpayers.

I have heard from many constituents who have expressed concerns about the state of America's cyber security. I am honored to represent a State that is an emerging center of technological advancement and innovation, with the growing hub of computer companies expanding across a metropolitan area known as Silicon Slopes. The people of Utah recognize that our Nation's future depends on America's ability to compete in the digital area. They understand we must create effective cyber security policies so we can continue to lead the world in innovation and technology advancement.

I am pleased to announce that an amended version of the Federal Computer Security Act is included in Chairman BURR and Vice Chairman

FEINSTEIN's managers' package. I wish to express my appreciation to both the chairman and vice chairman for their willingness to work with me in fine-tuning this legislation. I appreciate it. I wish to also thank Chairman RON JOHNSON and Ranking Member TOM CARPER of the Homeland Security and Governmental Affairs Committee for their efforts in this endeavor as well.

In addition to broad bipartisan support in the Senate, the Federal Computer Security Act enjoys support from key industry stakeholders. Some of our Nation's largest computer security firms support the bill, including Symantec, Adobe, and CA Technologies. Several industry groups have also voiced their support, including the Business Software Alliance and the IT Alliance for the Public Sector.

I commend Intelligence Committee Chairman BURR and Vice Chairman FEINSTEIN for their leadership in managing this critical cyber security legislation. As Leader MCCONNELL works to restore the Senate to its proper function, I am grateful we have been able to consider this legislation in an open and transparent fashion. By reinstating the open amendment process, we have not only been able to vote on dozens of amendments this year, we have been able to refine legislation through robust consideration and debate. I think we voted on approximately 160-plus amendments so far this year, and they are about evenly split between Democrats and Republicans.

With the renewal of longstanding Senate practices, we are passing meaningful laws that will better serve the needs of the American people. May we build on the foundation of success as we work to improve this critically important Cybersecurity Information Sharing Act.

I wish to again thank the distinguished leaders of this Intelligence Committee. Having served 18 years on the Intelligence Committee, I really appreciate the work that both of them have done, especially on this bill, and I look forward to its passage.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from California.

Mrs. FEINSTEIN. Madam President, I thank the distinguished Senator from Utah for his words. They are much appreciated, as is his friendship as well. I think he knows that. I believe the chairman feels certainly as strongly if not more strongly than I do.

I rose to be able to make a brief statement about the sanctuary bill as in morning business, if that is possible.

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

STOP SANCTUARY POLICIES AND PROTECT AMERICANS BILL

Mrs. FEINSTEIN. Madam President, I voted against Senator VITTER's bill. I believe it goes much too far. My longer statement is in the RECORD, but I want to respond to some of what I heard today. I do believe we should ensure that there is a notification prior to release of a dangerous individual with a criminal record, just as Senator SCHUMER said on this floor. I do believe we could take a narrow action to do just that. We could focus on dangerous individuals and not on all undocumented immigrants who happen to be taken into State or local custody. We could require notification without threatening vital law enforcement and local government funding, as Senator VITTER's bill does.

I had an amendment prepared for the Judiciary Committee's consideration when the committee had scheduled the bill for markup over a series of weeks, but the committee canceled its markup, so we were on the floor today with a bill that has never been heard in full by the Judiciary Committee.

Senator VITTER's bill includes a notification requirement and a detention requirement. It is not limited to those who are dangerous or have particular criminal records. It would cover a farmworker who was detained for a broken taillight or a mother who was detained for similar reasons, taking her away from her children. This is a standard that could be abused in another administration, and it is potentially a huge unfunded mandate to impose on States and localities.

The bill would also impose lengthy criminal sentences at the Federal level for individuals coming across the border to see their families or to perform work that is vital to the economy of California and the Nation. For example, in California, virtually the majority, if not all, of the farmworkers are undocumented. It happens to be a fact. It is why the agriculture jobs bill was part of the immigration reform act which was before this body and passed this body and went to the House and had no action.

Although Members on the other side state that this bill has support among law enforcement, I will note that the Major Cities Chiefs Association, the Major County Sheriffs' Association, the Fraternal Order of Police, the United States Conference of Mayors, and the National League of Cities are opposed to this bill or have submitted letters opposing threats to Federal law enforcement funding over this issue.

So, bottom line, I do believe we should do something about the circumstance that led to the tragic murder of Kate Steinle, which occurred in my city and State, and the tragic murder of Marilyn Pharis, which happened in the middle part of my State. I will support a reasonable effort to do just that, but this is not a targeted effort. It is too broad, and so I opposed it. My full statement is in the RECORD, but because it was spoken about on the floor, I did want to add these words.

I thank the Presiding Officer, and I yield the floor.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Madam President, moving back to cyber security, we now have S. 754 before the Senate, and we have a managers' package that is pending. We have a number of amendments that have been accepted and incorporated in the managers' package. We have several amendments that we could not reach agreement on, but those Members have the opportunity to come to the Senate floor. The amendments are already pending. They can debate those amendments, and they can have a vote on their amendment. For Members who might just now be engaging or who have had an opportunity to further read the bill, there are still present opportunities to offer perfecting amendments.

Let me suggest to my colleagues that when the vice chairman and I started down this road, we knew we couldn't reach unanimous consent of every company in the country and every Member of Congress. It was our goal, and I think we are pretty close to it when we look at the numbers. But there will be companies that object to this bill for some reason that I might not recognize.

The vice chairman has said this and I have said it and I want to reiterate it another time: This bill is voluntary. It does not require any company in America to participate in this. It does not require any entity to turn over information to the Federal Government for purposes of the Federal Government partnering with that company to determine who hacked their system, who penetrated, and who exfiltrated personal data. If a company has made the determination that they don't want to support this bill for whatever reason, I am resigned to the fact that that is a debate between their customers and themselves. It is, in fact, their customers that have to question the actions of the company.

I can confidently tell my colleagues that Senator FEINSTEIN and I have done everything to make sure there is wholesome participation by companies on a voluntary basis. We see tremendous value in those parts of our government that are experts at processing attacks like this to be able to identify who did it and what tools were used but, more importantly, what software defensive mechanism we can put on our systems to limit any additional exfiltration of data and, more broadly, to the rest of the business community say: Here is an attack that is in progress. Here is the tool they are using. Here is how you defend your data.

Now, we leave open, if we pass it, that there may be a company that decides they don't support this legislation. They can still participate in this program. Do we think if they get a call from the Department of Homeland Security or from the National Security Agency saying ''Here is an attack that is happening; here is the tool they are using,'' they are going to look at their system and say ''Is it in our system?'' They get the benefit of still participating and partnering with the Federal Government, even though they didn't support the legislation.

I know over the next day or so the vice chairman and I will concentrate on sharing with Members what is actually in the managers' package. We don't leave it up to staff just to cover it.

Let me just briefly share 15 points that I would make about the managers' package.

No. 1, it eliminates the government's uses for noncyber crimes; in other words, a removal of the serious violent felonies.

No. 2, it limits the authorizations to share cyber threat information for cyber security purposes, period.

No. 3, it eliminates new FOIA exemptions. In other words, everybody is under the same FOIA regulations that existed prior to this legislation being enacted.

No. 4, it ensures defensive measures are properly limited. We can't get wild and put these things in places that government shouldn't be, regardless of what the threat is.

No. 5, it includes the Secretary of Homeland Security as coauthor—coauthor—of government-sharing guidelines. I think this is an incredibly important part. The individual who is in charge of Homeland Security, that Secretary, is actively involved in the guidelines that are written.

No. 6, it clarifies exceptions to the DHS portal entry point for the transfer of information.

No. 7, it adds a requirement that the procedures for government sharing include procedures for notifying U.S. persons whose personal information is known to have been shared in violation—in violation—of this act. In other words, if a company mistakenly transmits information, the government is required to notify that individual. But, additionally, the government is statutorily required not to disseminate that information to any other Federal agency once it comes in and is identified.

No. 8, it clarifies the real-time automated process for sharing through that DHS portal.

No. 9, it clarifies that private entities are not required to share information with the Federal Government or another private entity.

No. 10, it adds a Federal cyber security enhancement title.

No. 11, it adds a study on mobile device security.

No. 12, it adds a requirement for the Secretary of State to produce an international cyber space policy strategy.

No. 13, it adds a reporting provision concerning the apprehension and prosecution of international cyber criminals.

No. 14, it improves the contents of the biannual report on CISA's implementation. My colleagues might remember, as some have raised issues on this, they have said: Why are there not more reports? There are biannual reports on the implementation and how it is done.

No. 15, and last, is additional technical and conforming edits.

Now, we didn't get into detail. We will get into detail later, but I say that because if that has in any way triggered with somebody who felt they were opposed to the bill because of something they were told was in it, maybe it was covered by one of those 15 things that I just talked about. They are things that were brought to the attention of the vice chairman and me, and we sat down and looked at it. If we didn't feel as though it changed the intent of the bill—and we have always erred on the side of protecting personal data, of not letting this legislation extend outside of what it was intended to do. Where we have drawn the line is when we believed that the effort was to thwart the effectiveness of this legislation.

I will remind my colleagues one last time: This legislation does not prevent cyber attacks. This legislation is designed to minimize the loss of the personal data of the customers of the companies that are penetrated by these cyber actors.

As we stand here today, we have had some rather significant breaches within the United States. I remind my colleagues that just today it was proposed that a high school student has hacked the unclassified accounts, the personal email, of the Secretary of the Department of Homeland Security and the Director of the CIA. Is there anybody who really thinks that this is going to go away because we are having a debate in the Senate and in the Congress of the United States, that the people who commit these acts and go without any identification are going to quit? No. It is going to become more rampant and more rampant and more rampant. From the standpoint of 2 of 15 Members who are designated by the U.S. Senate and its leadership to, on behalf of the other 85, look at the most sensitive information that our country can accumulate about threats, as many threads of threats as we look at today on the security of the American people, I think I can speak for the vice chairman: We are just as concerned about the economic security of the United States based upon the threat that we are faced with from cyber actors here at home and, more importantly, around the world.

I urge my colleagues, if you have something to contribute, come to the floor and contribute it. If you have an amendment already pending, come to the floor and debate it and vote on it. Give us the ability to work through the great thoughts of all 100 Members, but recognize the fact that those individuals whom you have entrusted to represent you with the most sensitive information that exists in our country came to a 14-to-1 vote when they passed this originally out of the Intelligence Committee. That is because of how grave we see the threat and how real the attackers are.

I thank the vice chairman. She has been absolutely wonderful to work with through this process. We are going to have a long couple of days if we process all of this, but I am willing to be here as long as it takes so that we can move on to conference with the House.

I yield the floor.

The PRESIDING OFFICER. The Senator from California.

Mrs. FEINSTEIN. Madam President, I thank the chairman for those words. I have one little duty left.

AMENDMENT NO. 2626

Madam President, I call for the regular order with respect to Whitehouse amendment No. 2626.

The PRESIDING OFFICER. The amendment is now pending.

AMENDMENT NO. 2626, AS MODIFIED

Mrs. FEINSTEIN. I ask that the amendment be modified with the changes that are at the desk.

The PRESIDING OFFICER. The amendment is so modified.

The amendment, as modified, is as follows:

At the end, add the following:

SEC. ___. STOPPING THE SALE OF AMERICANS' FINANCIAL INFORMATION.

Section 1029(h) of title 18, United States Code, is amended by striking ''title if—'' and all that follows through ''therefrom.'' and inserting ''title if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other Territory of the United States.''.

SEC. ___. SHUTTING DOWN BOTNETS.

(a) AMENDMENT.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting ''**and abuse**'' after ''**fraud**'';

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking ''or'' at the end;

(ii) in subparagraph (C), by inserting ''or'' after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

''(D) violating or about to violate section 1030(a)(5) where such conduct has caused or would cause damage (as defined in section 1030) without authorization to 100 or more protected computers (as defined in section 1030) during any 1-year period, including by—

''(i) impairing the availability or integrity of the protected computers without authorization; or

''(ii) installing or maintaining control over malicious software on the protected computers that, without authorization, has caused or would cause damage to the protected computers;''; and

(B) in paragraph (2), by inserting '', a violation described in subsection (a)(1)(D),'' before ''or a Federal''; and

(3) by adding at the end the following:

''(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—

''(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

''(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in

complying with the restraining order, prohibition, or other action.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of section for chapter 63 is amended by striking the item relating to section 1345 and inserting the following:

''1345. Injunctions against fraud and abuse.''.

SEC. ___. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer, if such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with such computer.

''(b) PENALTY.—Any person who violates subsection (a) shall, in addition to the term of punishment provided for the felony violation of section 1030, be fined under this title, imprisoned for not more than 20 years, or both.

''(c) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place any person convicted of a violation of this section on probation;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for the felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such violation to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, if such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

''(d) DEFINITIONS.—In this section

''(1) the terms 'computer' and 'damage' have the meanings given the terms in section 1030; and

''(2) the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have catastrophic regional or national effects on public health or safety, economic security, or national security.''.

(b) TABLE OF SECTIONS.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. ___. STOPPING TRAFFICKING IN BOTNETS.

(a) IN GENERAL.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (7), by adding ''or'' at the end; and

(B) by inserting after paragraph (7) the following:

''(8) intentionally traffics in the means of access to a protected computer, if—

''(A) the trafficker knows or has reason to know the protected computer has been damaged in a manner prohibited by this section; and

''(B) the promise or agreement to pay for the means of access is made by, or on behalf of, a person the trafficker knows or has reason to know intends to use the means of access to—

''(i) damage the protected computer in a manner prohibited by this section; or

''(ii) violate section 1037 or 1343;'';

(2) in subsection (c)(3)—

(A) in subparagraph (A), by striking ''(a)(4) or (a)(7)'' and inserting ''(a)(4), (a)(7), or (a)(8)''; and

(B) in subparagraph (B), by striking ''(a)(4), or (a)(7)'' and inserting ''(a)(4), (a)(7), or (a)(8)'';

(3) in subsection (e)—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) the term 'traffic', except as provided in subsection (a)(6), means transfer, or otherwise dispose of, to another as consideration for the receipt of, or as consideration for a promise or agreement to pay, anything of pecuniary value.''; and

(4) in subsection (g), in the first sentence, by inserting '', except for a violation of subsection (a)(8),'' after ''of this section''.

Mrs. FEINSTEIN. I thank the Chair and yield the floor.

Mr. BURR. I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

SANCTUARY CITIES BILL

Mr. PERDUE. Madam President, I rise to speak very briefly about the Stop Sanctuary Cities Act, which I was proud to cosponsor in the Senate. Simply put, this legislation protects American citizens from criminal illegal immigrants. Today, at least 340 cities across our country are choosing not to enforce our Nation's immigration laws. These sanctuary cities have become a safe haven for criminals who are not only in the United States illegally but also are committing additional crimes and repeatedly reentering trying our country after being deported. This summer we witnessed the tragic impact this lawlessness has on American citizens when Kate Steinle was murdered in San Francisco, a sanctuary city, by a felon living in our country illegally and who was previously deported five separate times. Three months prior to Kate's tragic death, the Department of Homeland Security actually asked San Francisco to detain her murderer, but the sanctuary city refused to cooperate and released the criminal back into the community. Had they not done that, had they turned that person over to Homeland Security as they were requested, Kate might still be with us.

This is unconscionable. I do not think I can overstate the importance of this Stop Sanctuary Cities Act to the American people and to the people of my home State of Georgia. The fact is that Kate Steinle did not have to die at the hands of a seven-time convicted felon and a five-time deportee. Kate and many others would not have died if our country had a functional immigration system and a government that actually enforces our laws.

This is why it is absolutely crucial that we stop sanctuary cities and address this illegal immigration crisis, which has also become a national security crisis. This bill would have done just that, and yet we were not able to even get it on the floor to have a debate. This is what drives people in my home State absolutely apoplectic. We want to get these bills to the floor, have an open debate, and let's let Americans see how we all vote on critical issues like this.

It is a very sad day, indeed, when this body cannot come together to stop rogue cities from breaking our Nation's laws, protecting the livelihood of American citizens, and support our law enforcement officials. I thank Senator VITTER and Chairman GRASSLEY for working closely with the victims' families and law enforcement to produce this legislation. I hope we can continue to debate this and get this bill back on the floor. I will keep fighting to stop this lawlessness and protect all Americans.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER (Mr. GARDNER). The clerk will call the roll.

The legislative clerk proceeded to call the roll.

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

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

Mr. WHITEHOUSE. Mr. President, I ask unanimous consent to speak as in morning business for up to 20 minutes.

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

CLIMATE CHANGE

Mr. WHITEHOUSE. Mr. President, last week the former head of the National Oceanic and Atmospheric Administration, Robert M. Hoyt, passed away at the age of 92. Dr. Hoyt served this Nation under five Presidents and pioneered the peaceful use of satellites to understand our weather and climate. He said:

> We do have environmental problems and they're serious ones, the preservation of species among them, but the climate is the environmental problem that's so pervasive in its effects on the society. . . . The climate is really the only environmental characteristic that can utterly change our society and our civilization.

That was in 1977. That same year, James F. Black, a top scientific researcher at the Exxon Corporation,

gave that company's executives a similar warning. ''[T]here is general scientific agreement,'' he told Exxon's Management Committee, ''that the most likely manner in which mankind is influencing the global climate is through carbon dioxide release from the burning of fossil fuels.'' According to emerging reports, Exxon executives kept that warning a closely guarded company secret for years.

I rise today for the 115th time to urge that we wake up to the threat of climate change. I rise in the midst of a decades-long purposeful corporate campaign of misinformation, which has held this Congress and this Nation back from taking meaningful action to prevent that utter change.

Scrutiny of the corporate campaign of misinformation intensifies, and scrutiny of the fossil fuel polluters behind it intensifies, and the regular cast of rightwing climate denier attack dogs have their hackles up.

On May 6 I gave a speech on the floor of the Senate. The speech compared the misinformation campaign by the fossil fuel industry about the dangers of carbon pollution to the tobacco industry's misinformation campaign about the dangers of its product. The relevance of that comparison is that the U.S. Department of Justice, under the civil provisions of the Federal racketeer influenced and corrupt organizations statute—RICO for short—brought an action against the tobacco industry. The United States alleged that the tobacco industry's misinformation campaign was fraudulent, and the United States won in a lengthy and thorough decision by U.S. District Judge Gladys Kessler.

You can go ahead and read them. DOJ's complaint and Judge Kessler's decision can be found at the Web sites of the Justice Department and the Public Health Law Center, respectively, and they are linked on my Web site, whitehouse.senate.gov/climate change. I will warn you that Judge Kessler's decision is a long one, but it makes good reading.

The comparison is strong. There are whole sections of the Department of Justice civil RICO complaint and whole sections of Judge Kessler's decision where you can remove the word ''tobacco'' and put in the word ''carbon'' and remove the word ''health'' and put in the word ''climate,'' and the parallel with the fossil fuel industry climate denial campaign is virtually perfect.

This is not an idea I just cooked up. Look at the academic work of Professor Robert Brulle of Drexel University and Professor Riley Dunlap of Oklahoma State University. Look at the investigative work of Naomi Oreskes' book ''Merchants of Doubt,'' David Michaels' book ''Doubt is Their Product,'' and Gerald Markowitz and David Rosner's book ''Deceit and Denial,'' describing this industry-backed machinery of deception.

Look at the journalistic work of Neela Banerjee, Lisa Song, David Hasemyer, and John Cushman, Jr., in the recent reporting of InsideClimate News about what Exxon knew about climate change versus the falsehoods that Exxon chose to tell the public. Look at a separate probe by journalists Sara Jerving, Katie Jennings, Masako Melissa Hirsch, and Susanne Rust in the Los Angeles Times.

From all their work, we know now that Exxon, for instance, knew about the effect of its carbon pollution as far back as the late 1970s but ultimately chose to fund a massive misinformation campaign rather than tell the truth. ''No corporation,'' said professor and climate change activist Bill McKibben, ''has ever done anything this big and this bad.''

Just today, the person who probably knows the most about the tobacco litigation, the assistant attorney general of the United States who prosecuted that case as a civil matter and won it in the U.S. District Court, Sharon Eubanks, said about the climate denial RICO idea: ''I think a RICO action is plausible and should be considered.''

This is how Judge Kessler depicted the culpable conduct of the tobacco industry in her decision in that case: ''Defendants have intentionally maintained and coordinated their fraudulent position on addiction and nicotine as an important part of their overall efforts to influence public opinion and persuade people that smoking is not dangerous.''

Now compare that to the findings of Dr. Brulle, whose research shines light on the dark-money campaigns that fund and support climate denial. This climate denial operation, to quote Dr. Brulle, is ''a deliberate and organized effort to misdirect the public discussion and distort the public's understanding of climate.''

The parallels between what the tobacco industry did and what the fossil fuel industry is doing now are so striking, I suggested in my speech of May 6, that it was worth a look, that civil discovery could reveal whether the fossil fuel industry's activities cross that same line into racketeering.

I said that again in an op-ed piece I wrote in the Washington Post on May 29 regarding the civil RICO action against tobacco. Oh my, what a caterwauling has ensued from the fossil fuel industry trolls. Here is a quick highlight reel of the tempest of rightwing invective.

One climate denier, Christopher Monckton, declared: ''Senator WHITEHOUSE is a fascist goon.''

Another denier compared me to Torquemada, the infamous torturer of the Inquisition.

The official Exxon responder got so excited about this suggestion that he used a word I am not even allowed to use on the Senate floor. He forgot rule No. 1 in crisis management: Don't lose your cool.

The rightwing Web site breitbart.com responded by calling me ''the preposterous Democrat senator for Rhode Island'' and saying the notion that there is an industry-led effort to mislead the American people about the harm caused by carbon pollution is ''a joke,'' a conspiracy theory on par with Area 51 or the faking of the Moon landing. Well, tell that to the tobacco industry.

Paul Gigot, the editorial page editor of the Wall Street Journal, said global warming concerns ''are based on computer models, not by actual evidence, not by actual evidence of what we've seen so far.'' Tell that to the scientists who measure the effects of climate change every day, particularly in our oceans.

The polluter-funded George C. Marshall Institute, a longtime climate denial outfit—and who knows how they got to take respectable George C. Marshall's name and slap it on the front of a climate denial industry front—they wrote that this was an attack on constitutional rights. Well, that kind of presumes the answer because there is no constitutional right to commit fraud.

Similarly, Calvin Beisner, founder of another phony baloney industry front called the Cornwall Alliance, said the same: The mere suggestion of considering this action represents a ''direct attack on the rights to freedom of speech and the press guaranteed by the First Amendment'' and is ''horrifically bad for science.'' Coming from a science-denial outfit, that concern for science is rich. Again, fraud is not protected by the First Amendment.

In the National Review, I was accused of wanting to launch ''organized crime investigations . . . against people and institutions that disagree with [me] about global warming'' in order to ''lock people up as Mafiosi.'' Crime? Lock people up? Let's remember, we are talking about civil RICO, not criminal. No one went to jail in the tobacco case. Investigating the organized climate denial scheme under civil RICO is not about putting people in jail.

Query why the National Review would mislead people about such an obvious fact, and they are not alone. The rightwing blogosphere has lit up with nonsense about how this is a criminal charge. Read the tobacco complaint. It is on the Department of Justice Web site. Even people who purport to be legal scholars are misleading folks that way. All a civil RICO case does is get people to actually have to tell the truth under oath in front of an actual impartial judge or jury and under cross-examination, which the Supreme Court has described as ''the greatest legal invention ever invented for the discovery of truth.'' No more spin and deception—but that is exactly the audience polluters and their allies cannot bear, so the flacks set off criminal smokescreens and launch fascist goon and Torquemada hysterics.

A few weeks ago, 20 scientists agreed with me and wrote a letter to Attorney General Lynch supporting the idea of using civil RICO. That was too much for the troll-in-chief for the fossil fuel

industry, the Wall Street Journal editorial page. The Wall Street Journal editorial page has long been an industry science-denial mouthpiece. They use the same playbook every time: one, deny the science; two, question the motives of reformers; and three, exaggerate the costs of reforms.

For example, when scientists warned that chlorofluorocarbons could break down the atmosphere's ozone layer, the Wall Street Journal ran editorials—for decades—devaluing the science, attacking scientists and reformers, and exaggerating the costs associated with regulating CFCs. It turns out they were dead wrong.

When acid rain was falling in the Northeast, the Wall Street Journal editorial page questioned the science, claimed the sulphur dioxide cleanup effort was driven by politics, and said fixing it carried a huge price tag. Ultimately, the Journal's editorial page, after years of this, had to recant and admit that the cap-and-trade program for sulphur dioxide ''saves about $700 million annually compared with the cost of traditional regulation and has been reducing emissions by four million tons annually.''

Now, on climate change, the Journal is back to the same pattern: Deny the science, question the motives of climate scientists, exaggerate the costs of tackling carbon pollution.

For decades, the Journal has been persistently publishing editorials against taking any action to prevent manmade climate change. On this, the editorial page said that by talking about civil RICO, I am trying to ''forcibly silence'' the denial apparatus. Forcibly silence? First of all, against the billions of the Koch brothers and the billions of ExxonMobil, fat chance that I have much ''force'' to use. And silence? I don't want them silent. I want them testifying in a forum where they have to tell the truth.

Is the Journal really saying that in a forum where climate deniers have to tell the truth, their only response would have to be silence? Making them tell the truth ''forcibly silences'' them? The only thing civil RICO silences is fraud.

By the way, the Journal editorial never mentions that the government won the civil RICO case against tobacco and on very similar facts. That would detract from the fable. Whom does the Journal cast as their victim in their fable? None other than Willie Soon, whom they said I singled out for—this is what they said—having ''published politically inconvenient research on changes in solar radiation.'' Politically inconvenient research.

Actually, what is inconvenient for Dr. Soon is that the New York Times reported that he got more than half his funding from big fossil fuel interests such as ExxonMobil and the Charles Koch Foundation to the tune of $1.2 million and didn't disclose it. Dr. Soon's research contracts even gave his industry backers a chance for comment and input before he published, and he referred to the papers he produced for them as ''deliverables.'' In case anyone listening doesn't know this, that is not how real science works. Of course, none of this sordid financial conflict is even mentioned by the Wall Street Journal editorial page. They would rather pretend that Dr. Soon is being singled out for ''politically inconvenient'' views. Please.

It gets better. In the editorial, the role of neutral expert commenting on all of this goes to Georgia Tech's Judith Curry. She offers the opinion that my ''demand . . . for legal persecution . . . represents a new low in the politicization of science.'' This is a particularly rich and conflict-riddled opinion, as Ms. Curry is herself a repeat anti-climate witness performing regularly in committees for Republicans here in Congress. Again, there is no mention of this interest of Ms. Curry's in the Wall Street Journal editorial.

The fossil fuel industry's climate denial machine rivals or exceeds that of the tobacco industry in size, scope, and complexity. Its purpose is to cast doubt about the reality of climate change in order to forestall moves toward cleaner fuels and to allow the Kochs and the Exxons of the world to continue making money at everybody else's expense. And the Wall Street Journal editorial page plays its part in this machine.

Even though it is only the editorial page and not the Journal's well-regarded newsroom, facts and logic are supposed to matter. Ignoring the successful tobacco litigation, omitting the salient fact of Dr. Soon being paid by the industry involved in his research, and bringing in a climate denier as their neutral voice without even disclosing that conflict—I would like to see the Wall Street Journal editorial page get that editorial by the editorial standards of their own newsroom.

So why all the histrionics on the far right? Why all the deliberate subterfuge between civil and criminal RICO? Why all the name-calling? Have we perhaps touched a little nerve? Have we made the hit a bit too close to home? Maybe a civil RICO case is indeed plausible and should be considered. Are the cracks in the dark castle of climate denial as it crumbles beginning to maybe rattle the occupants?

Whatever the motivation of the Wall Street Journal and other rightwing climate denial outfits, it is clearly long past time for this climate denial scheme to come in from the talk shows and the blogosphere and have to face the kind of truth-testing audience a civil RICO investigation could provide. It is time to let the facts take their place and let climate denial face that greatest legal engine ever invented for the discovery of truth.

Mr. President, I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

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

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

CLOTURE MOTION

Mr. MCCONNELL. Mr. President, I send a cloture motion to the desk for the Burr-Feinstein amendment No. 2716.

The PRESIDING OFFICER. The cloture motion having been presented under rule XXII, the Chair directs the clerk to read the motion.

The bill clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of rule XXII of the Standing Rules of the Senate, do hereby move to bring to a close debate on the amendment No. 2716 to S. 754, a bill to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

Mitch McConnell, John Cornyn, Johnny Isakson, Richard Burr, John McCain, Shelley Moore Capito, Orrin G. Hatch, John Thune, Chuck Grassley, Pat Roberts, John Barrasso, Jeff Flake, Lamar Alexander, Bill Cassidy, Deb Fischer, Susan M. Collins, Patrick J. Toomey.

CLOTURE MOTION

Mr. MCCONNELL. Mr. President, I send a cloture motion to the desk for the underlying bill, S. 754.

The PRESIDING OFFICER. The cloture motion having been presented under rule XXII, the Chair directs the clerk to read the motion.

The bill clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of rule XXII of the Standing Rules of the Senate, do hereby move to bring to a close debate on S. 754, an original bill to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

Mitch McConnell, John Cornyn, Johnny Isakson, Richard Burr, John McCain, Shelley Moore Capito, Orrin G. Hatch, John Thune, Chuck Grassley, Pat Roberts, John Barrasso, Jeff Flake, Lamar Alexander, Bill Cassidy, Deb Fischer, Susan M. Collins, Patrick J. Toomey.

MORNING BUSINESS

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the Senate be in a period of morning business, with Senators permitted to speak therein for up to 10 minutes each.

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

VOTE EXPLANATION

Mr. RUBIO. Mr. President, on September 28, 2015, I was unable to vote on the motion to proceed to a short-term budget—continuing resolution—that, among other measures, denied taxpayer funding to Planned Parenthood. I would have voted no.

On September 30, 2015, I was unable to vote on final passage of a short-term budget—continuing resolution—to fund