

Larry Vilardo on the bench. I congratulate Larry Vilardo on this milestone of his career.

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 President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Mr. COATS). Without objection, it is so ordered.

CONCLUSION OF MORNING BUSINESS

The PRESIDING OFFICER. Morning business is closed.

EXECUTIVE SESSION

EXECUTIVE CALENDAR

The PRESIDING OFFICER. Under the previous order, the Senate will proceed to executive session to consider the following nomination, which the clerk will report.

The senior assistant legislative clerk read the nomination of Lawrence Joseph Vilardo, of New York, to be United States District Judge for the Western District of New York.

The PRESIDING OFFICER. Under the previous order, there will be up to 30 minutes of debate.

The Senator from Oregon.

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

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

CYBERSECURITY INFORMATION SHARING BILL

Mr. WYDEN. Mr. President, tomorrow we will be turning to the cyber security bill, which the Presiding Officer is familiar with as a member of the committee, and I wish to speak about my amendment No. 2621 to that legislation. I also intend to address the amendments of our colleagues Senator FRANKEN, Senator HELLER, and Senator COONS because I believe all four of these amendments seek to achieve the same goal, and that goal—the goal of all four of these amendments—is to reduce the unnecessary sharing of Americans' private and personal information.

The Senate has had a robust debate on the cyber security bill over the past week, and I think it is fair to say that Senators agree on a fair number of points. For example, the sponsors of the legislation have now acknowledged that the cyber security bill we will shortly vote on would not have prevented sophisticated cyber attacks, such as the Target and Home Depot hacks, and it would not have prevented the theft of millions of personnel records at the Office of Personnel Management.

As for my part, I agree that sharing information about cyber security threats is generally a constructive idea. If private companies identify samples of malicious code or information that identifies foreign hackers, I would absolutely encourage them to share that information. However, I think companies should also take reasonable steps—and I underline “reasonable steps”—to remove unrelated personal information about their customers before sharing that data with the government. It is important to understand that this legislation simply does not require companies to do that, and Senators can see that for themselves. As Senators can see for themselves, on page 17 of the bill, companies are allowed to conduct only a cursory review of the information they provide and would only be required to remove data that they know is personal information unrelated to cyber security.

When it comes to customers' personal information, the message behind this bill is, when in doubt, hand it over. Once that data is shared—and this is not widely known—the Department of Homeland Security would be required to send it on to a broad range of government agencies, from the NSA to the FBI.

The amendment I have offered to the legislation we will vote on tomorrow would give companies a real responsibility for safeguarding their customers' information. It would say that in order for a company to receive liability protection before a company shares data with the government, it has to make efforts to the extent feasible to remove any personal information that is not necessary to identify or describe a cyber security threat. In my view, that would give this legislation a straightforward standard that could give consumers real confidence that their privacy is actually being protected.

Let me give an example of how this might work in practice. Imagine that a health insurance company finds out that millions of its customers' records have been stolen. If that company has any evidence about who the hackers were or how they stole this information, of course it makes sense to share that information with the government. But the company shouldn't simply say “Well, here you go” and hand millions of its customers' financial and medical records over for distribution to a broad array of government agencies, such as the FBI and the NSA.

The records of the victims of a hack should not be treated the same way information about the hacker is treated. Companies should be required to make reasonable efforts to remove personal information that is not needed for cyber security before they hand that information over to the government. That, in short, is what my amendment seeks to achieve.

The sponsors of the legislation have argued that my amendment would somehow hold companies to an almost impossible standard. I say respectfully

that the language of this amendment is quite measured. Companies are required to remove unrelated personal information and the legislation specifically states “to the extent feasible.” The language certainly doesn't require perfection; it creates a reasonable and flexible approach for companies to make a real effort to remove unrelated personal information about their customers instead of simply performing the sort of cursory review that would be permitted under the current language of the bill.

A quick reading through the list of the pending amendments to the bill will make it clear that I am not the only Member of this body who is concerned about the unnecessary sharing of personal information.

Our colleague from Nevada, Senator HELLER, has a similar amendment that would seek to create a stronger requirement for companies to remove personal information.

Our colleague from Delaware, Senator COONS, has crafted a very constructive amendment that would strengthen the requirement for review by the Department of Homeland Security. His amendment would create a stronger obligation for the Homeland Security Department to filter out unnecessary personal information before passing cyber security data on to other parts of our government.

Senator FRANKEN has drafted a strong amendment that would clarify the bill's definition of “cyber security threat information” to ensure that it focuses on information about real threats.

It is important to remember that reducing unnecessary sharing of personal information will make any information sharing program more effective and easier to focus on the genuine threats involved.

Finally, our colleague from Arizona, Senator FLAKE, has drafted an amendment that would require the Congress to come back and review this information sharing approach after 6 years to evaluate how it has worked in practice and whether privacy protections ought to be strengthened.

I have cited amendments by Democrats and Republicans. The Presiding Officer knows that I feel strongly about working in a bipartisan way whenever I possibly can, and that is why I thought it was important to mention, as we go through these amendments, that all of these amendments I have described have sought to ensure this body would make it clear that cyber security is a very real problem. Cyber security, in terms of tackling it, which involves information sharing, can be very constructive, and we ought to try to find ways to do it. Each of these amendments is designed to make sure that when Americans hear about cyber security legislation—my colleague and I have discussed it—we don't have millions of Americans walking away and saying: They are sharing all of this unnecessary personal and unrelated information; I