Senate completes its business today, it adjourn until 10 a.m., Tuesday, October 27; that following the prayer and pledge, the morning hour be deemed expired, the Journal of proceedings be approved to date, and the time for the two leaders be reserved for their use later in the day; that following leader remarks, the Senate resume consideration of S. 754, with the time until 11 a.m. equally divided between the two leaders or their designees; finally, that notwithstanding the provisions of rule XXII, there be 2 minutes of debate equally divided prior to each vote, and that all votes after the first vote in each series be 10 minutes each.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

ORDER FOR ADJOURNMENT

Mr. PORTMAN. Madam President, if there is no further business to come before the Senate, I ask unanimous consent that it stand adjourned under the previous order, following the remarks of Senator FRANKEN.

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

The Senator from Minnesota.

Mr. FRANKEN. Madam President, I ask unanimous consent to speak for 6 minutes.

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

CYBERSECURITY INFORMATION SHARING BILL

Mr. FRANKEN. Madam President, tomorrow we will vote on my amendment to the Cybersecurity Information Sharing Act, or CISA. I am proud to be joined on this amendment by Senators LEAHY, DURBIN, and WYDEN, each of whom has worked to try to ensure that any cyber legislation passed by this body is effective and adequately safeguards the privacy and civil liberties of the American people.

My amendment tightens the definitions of the terms ''cyber security threat'' and ''cyber threat indicator'' in the bill. These changes will help ensure that CISA's broad authorities are not triggered in circumstances where no real cyber threats are present. This makes the bill more privacy protected and more likely to work effectively.

The amendment is supported by more than 30 civil society organizations, from the American Civil Liberties Union to prominent Libertarian groups like R Street. As I will describe, it addresses specific concerns that have been raised by security experts, major tech companies, and even the Department of Homeland Security.

Under CISA, companies are authorized to monitor users online, share information with one another and with the Federal Government, and deploy defensive measures—all to protect against ''cyber security threats.'' Any action that may result in any unauthorized effort to adversely impact cyber security can be deemed a cyber security threat; that is, may result. That sets the lowest possible standard for determining when actions under CISA are justified, and that is a problem. It sets us up for the oversharing of information, or worse it jeopardizes privacy and threatens to hinder our cyber defense efforts by increasing the noise-to-signal ratio.

My amendment would clarify that a threat is any action at least reasonably likely—reasonably likely—to result in an unauthorized effort to adversely impact cyber security. That definition gives companies ample flexibility to act on threats and ensures Americans that CISA isn't a free pass to share people's personal information when there is no threat.

CISA's definition of cyber threat indicator has also been criticized by security experts, by companies such as Mozilla and, again, even by DHS, which has called the definition ''expansive'' and said that expansive definition heightens concerns raised by the bill.

My amendment addresses the two parts of the definition that experts have suggested are the most likely to open the door to the sharing of extraneous information. First, as drafted, CISA would let companies share people's communications if they believe that the files have been harmed in a cyber attack or could potentially—potentially—be harmed by a perceived threat. The latter is especially problematic. The range of information that could be shared as evidence of potential harm is vast, and, as experts have explained, unnecessary to the technical work of identifying cyber threats. My amendment continues to allow companies to share information that reveals harms caused by a cyber incident but doesn't extend this to conjecture about hypothetical potential harms, which is unnecessarily broad.

Finally, my amendment eliminates a troubling loophole in the cyber threat indicator definition. In addition to letting companies share information that reveals certain specified attributes or features of cyber threats, CISA also lets them share information that reveals ''any other attribute of a cybersecurity threat'' if the disclosure of that attribute is legal. Bill supporters claim that this final clause adequately limits the scope of this provision, but looking at whether disclosure of a threat attribute is lawful is an unclear and unhelpful standard. Privacy law is about protecting information, not threat attributes. So my amendment clarifies that companies can share information in this catchall category only if it is legal to share the information being provided. It is a technical change, but it matters.

This amendment represents a real effort to find common ground for moving forward. Quite frankly, it doesn't do all the work that needs to be done to limit the definitions in this act, but it makes necessary changes—necessary changes—to improve the legislation, both for the sake of privacy and ultimately security.

I urge my colleagues to support amendment No. 2612.

I yield the floor.

ADJOURNMENT UNTIL 10 A.M. TOMORROW

The PRESIDING OFFICER. Under the previous order, the Senate stands adjourned until 10 a.m. tomorrow.

Thereupon, the Senate, at 6:13 p.m., adjourned until Tuesday, October 27, 2015, at 10 a.m.

CONFIRMATION

Executive nomination confirmed by the Senate October 26, 2015:

THE JUDICIARY

LAWRENCE JOSEPH VILARDO, OF NEW YORK, TO BE UNITED STATES DISTRICT JUDGE FOR THE WESTERN DISTRICT OF NEW YORK.