Written by **Joe Wolverton, II, J.D.** on October 25, 2015

DHS Lobbying for Passage of CISA; Cotton Calls for Expanded Data Sharing

Officials at the Department of Homeland Security (DHS) are lobbying the Senate to pass the Cybersecurity Information Sharing Act of 2015 (CISA), seeing it as a sure way to get their hands on critical customer data.

During his keynote address at an event sponsored by the Atlantic Council in Washington, D.C., entitled "Big Data, Bad Actors Conference," DHS Deputy Secretary Alejandro Mayorkas said Oct. 22 that the purported cybersecurity bill would assist the government in obtaining critical data from private service providers. This cooperation, he insists, would make us all safer.

"In the cyber arena, specifically, we look to the private sector as a partner," Mayorkas said. "We don't actually view ourselves as leading, as opposed to viewing ourselves as co-leading with the private sector in developing an ecosystem … that raises the level of cybersecurity."

The DHS deputy explained that although private companies control much of the traffic on the internet, Homeland Security can make better use of the data, collecting it and interpreting it in a way that will protect Americans from international bad guys.

"We can take that information, divest it of personal information and disseminate it very broadly to raise the ecosystem," Mayorkas said.

Given its track record, however, one imagines that the divesting of personal information will be overlooked in the rush to gain control of the digital coming and going on the internet.

In a statement released on the same day as his subordinate's speech, DHS Secretary Jeh Johnson urged the Senate to pass CISA, saying it was "an opportunity we cannot afford to lose."

Despite pressure from DHS leadership, a few senators have tried to amend the bill, protecting private data and relieving companies of liability for the misuse (by government or otherwise) of clients' personal information stored on servers owned and operated by businesses.

One of these amendments was offered by presidential candidate and senator from Kentucky, Rand Paul. Paul's colleagues killed the amendment, as well as another by Senator Jeff Flake (R-Ariz.) that would have required the bill to expire in six years.

There is one senator, however, who offered an amendment that would have expanded the scope of mandatory private data sharing between private businesses and the federal government.

Senator Tom Cotton (R-Ark.), neocon water carrier, sponsored an added provision to CISA that would have provided access to private data to the FBI and Secret Service, as well as Homeland Security.

The blog Tom's Guide explained how CISA could be used by the federal government more as a platform

for expanded surveillance than as a protection against cyberterrorism:

> "At its core, it's more about surveillance than it is about cybersecurity," Nathaniel Turner, a lobbyist assistant in the ACLU's Washington Legislative Office, told Tom's Guide.
>
> Critics contend that the bill describes cyberthreat indicators quite broadly, and includes any attribute of a cyberthreat.
>
> "This means the information [forwarded to the government] can include email, text messages or other communications, together with personally identifiable information or PII," Turner said.
>
> "Companies are only required to scrub out this kind of PII if they know at the time of sharing that the PII is not directly related to a cybersecurity threat."
>
> Privacy advocates say the bill would let companies freely share any collected information that had been designated as a "cyberthreat indicator" with intelligence and law-enforcement agencies, such as the FBI or the NSA.
>
> "Such sharing will occur because under this bill, DHS would no longer be the lead agency making decisions about the cybersecurity information received, retained, or shared to companies or within the government," Mark M. Jaycox, legislative analyst for the Electronic Frontier Foundation (EFF), told Tom's Guide.

CISA's threat to our most fundamental rights is real and irreversible if passed by the Senate and signed by the president (the president has repeatedly insisted that he would veto the bill, however).

For example, CISA would obliterate (and invalidate) all internet privacy laws presently in force. Companies large and small would be permitted to turn over to the federal government users' e-mails, usernames, passwords, browsing history, and most other forms of electronically stored information.

That's not all. According to information distributed by CISA's two largest opponents — the Electronic Frontier Foundation (EFF) and the ACLU — the data the government is targeting with CISA includes medical records, credit reports, and most other "personally identifiable information" that might be caught in a cybersecurity net.

And, should Senator Cotton's amendment make it into the final version of the bill, the various agencies of the the domestic surveillance mammoth would need no warrant before approaching Internet companies with requests for their customers' otherwise private information.

Although proponents of the bill point out that Internet companies could redact their customers' most private information, the text of CISA contains no provision for such protection of privacy.

Notably, Microsoft, Google, and Apple have come out in opposition to the bill.

"The trust of our customers means everything to us and we don't believe security should come at the expense of their privacy," Apple said in a statement to the *Washington Post*.

Of course, even the president's plan to veto CISA should it ever arrive on his desk is based not on his belief in the sanctity of the right to be free from such intrusion and violations of the rights protected by the Fourth Amendment. His problem with the bill in its current form is that it doesn't do enough to hold corporations accountable to Washington for their adherence to the bill's mandates.

In this case, as with so many other federal programs that are steadily and stealthily chipping away at our civil liberties that are the very foundation of our Republic, the will in Washington is to place every

aspect of the lives of every American under the close watch of the federal government.

And, contrary to the president's declaration that American prosperity depends on cybersecurity, friends of freedom know that to perpetuate our Republic, we must return to first principles of liberty and a fearless defense of the Constitution, which stands as sentinel of those timeless rights granted to all men by their Creator.

After voting 83-14 on October 22 to end debate on amendments, the Senate will likely vote on the final version of the bill sometime early this week.