New American

Written by **Bob Adelmann** on April 26, 2012

CISPA Assumes Too Much Trust in Government

> The sharing of information [between private agencies and the federal government] must be conducted in a manner that preserves American's privacy, data confidentiality, and civil liberties and recognizes the civilian nature of cyberspace. Cybersecurity and privacy are not mutually exclusive…
>
> [CISPA]…repeal[s] important provisions of electronic surveillance law without instituting corresponding privacy, confidentiality, and civil liberties safeguards…
>
> The bill also lacks sufficient limitation on the sharing of personally identifiable information…and does not contain adequate oversight or accountability measures…to ensure that the data is used only for appropriate purposes…
>
> The bill effectively treats domestic cybersecurity as an intelligence activity and thus, significantly departs from longstanding efforts to treat the Internet and cyberspace as civilian spheres.

This is the first time in recent memory that the White House has expressed any such concerns. When signing into law the controversial National Defense Authorization Act [NDAA] the White House blithely ignored its trampling of those same civil liberties through its "indefinite detention" provisions. Nor did the White House raise any similar concerns when it issued its executive order commandeering all resources from American citizens in the event of an emergency to be declared by the president.

So the following from the White House's statement on CISPA makes perfect sense: the White House favors government regulation of the internet and invasion of privacy without following the Fourth Amendment. It just doesn't want to do it so blatantly:

> The Administration believes that a civilian agency — the Department of Homeland Security — *must have a central role in domestic cybersecurity*, including for conducting the overseeing the exchange of cybersecurity information with the private sector and with sector-specific Federal agencies. (emphasis added)

And just to make sure that the message is delivered, received and understood, the statement concluded:

> The Congress must also include authorit[y] to ensure our Nation's most vital critical infrastructure assets are properly protected…*Voluntary measures alone are insufficient responses* to the growing danger of cyber threats. (emphasis added)

There it is: only the government is able and competent to police the networks, all in the name of security.

Amendments to soften, limit and allegedly restrict government overreach are being offered. Rep. Bennie Thompson (D-Mich.) wants to increase the bill's privacy protection while an amendment from

Rep. Adam Schiff (D-Calif.) would limit the personal information the government would be able to monitor and which agencies would be allowed to do the snooping. The co-sponsors of the bill, Reps. Mike Rogers (a "conservative" Republican from Michigan) and Dutch Ruppersberger (a liberal Democrat from Maryland) are also offering amendments to "address" the White House's concerns.

Others, such as the ACLU and the Electronic Frontier Foundation, are dutifully complaining about the bill's incursions into private citizen's rights but the stage has been set for passage, regardless.

It took the ARS Technica blog to expose this sham and fraud:

> It's unclear why new legislation is needed to allow this kind of uncontroversial information sharing to occur. Network administrators and security researchers at private firms have shared threat information with one another for decades. And the law also allows information sharing between private firms and the government in many circumstances. For example, a private company is already free to notify the FBI if it detects an attempt to hack into its network…
>
> [This] legislation provides that companies are authorized to share "cyber threat information" with other private companies or the government "notwithstanding any other provision of law." That appears to mean that if a company decides that your private emails, your browsing history, your health care records, or any other information would be helpful in dealing with a "cyber threat," the company can ignore laws that would otherwise limit its disclosure. The legislation also immunizes firms who share "cyber threat information" from customer lawsuits.

CISPA is another example of how the game is played. A "threat" is exposed, a bill is offered to "defend" against the threat, objections are raised, amendments are presented to answer the objections, there is much debate, and the bill is finally passed. The net effect: more government surveillance, less individual privacy of individuals.

Related article: Proposed Amendment to CISPA Adds More Controversy to Bill