HOW DID TWO CISA BENEFICIARIES AND NUMEROUS AGNOSTICS COME TO SUPPORT CISA?

When the Business Software Alliance released this letter a while back, I was perplexed.

In addition to its call for Congress to pass a set of designated bills, including ECPA reform, that would give assurances to international customers that US services weren't more exposed to US spying, the letter also called for passage of cybersecurity sharing legislation.

> Cyber Threat Information Sharing Legislation will promote cybersecurity and protect sensitive information by enabling private actors in possession of information about vulnerability and intrusions to more easily share that information voluntarily with others under threat, thus enabling the development of better solutions faster.

As TechDirt noted, the letter didn't name any particular cyber sharing bill, but there are three and all expand US government access to data. Even if some or all tech companies that make up BSA wanted such a bill it seemed odd to include in a call for legislation that would reassure international customers. I asked around and the impression was it was just convenience to include a CISA-type legislation (but why include it at all)?

So then Fight for the Future went to work. It got thousands of activists to complain to the companies directly about their stated support for a CISA-type legislation. And also announced their intention to stop using Heroku, which is part of Salesforce, as their host.

That led first Salesforce then BSA more generally to deny they had ever supported CISA. The BSA language pretended their original letter called for balanced legislation. And it also claimed to consistently advocate for strong privacy protections on such legislation — which of course they didn't do in the letter.

> There have been questions about our views of the current CISA legislation. For clarity, BSA does not support any of the three current bills pending before Congress, including the Cybersecurity Information Sharing Act (CISA), the Protecting Cyber Networks Act (PCNA), and the National Cybersecurity and Communications Integration Center (NCCIC) Act.
>
> Consistent with this view, BSA's September 14 data agenda letter to Congressional leaders identified five key areas where Congress can pass legislation to strengthen the policy environment around digital commerce, including voluntary information sharing, and highlighted the need for balanced legislation in this area.
>
> BSA has consistently advocated for strong privacy protections in all information sharing bills currently pending before the Congress.
>
> We will continue to work with the Congress, others in industry and the privacy community to advance legislation that effectively deals with cyber threats, while protecting individual privacy.

All of raises more questions about how the endorsement for cyber sharing at a time when all the cyber sharing bills before Congress don't balance privacy interests got into the letter.

Especially given the signatories. The signatories include companies — like Apple —

that have fought hard to protect their customers' privacy. It included several — notably Adobe and Siemens — that could significantly benefit from any kind of immunity, given that their products are among the most consistent targets of hacks. Most interesting, it includes several companies — including IBM and Symantec — that will benefit when a CISA bill makes it easier for cybersecurity contractors to get more data with which to serve customers.

Indeed, the language from the original bullet support cyber sharing — "enabling private actors in possession of information about vulnerability and intrusions to more easily share that information voluntarily with others under threat" — might well describe how cybersecurity contractors will get a boost from CISA.

Some members of BSA probably do, individually, support CISA for the immunity and data it would give them. Others neither need it nor want the stigma.

So how did it get in this letter?