OPEN LETTER TO TECHNOLOGY COMPANIES SUPPORTING OR CONSIDERING SUPPORTING CISPA

As your users and customers, we want to thank you for the services that enrich our lives and allow us to share and create in new ways.

We also want you to know that we understand your concerns about cyber security threats. They originate at home and abroad, relentlessly attack network stability and data privacy, and impede your ability to do business.

We get the positives of the Cyber Intelligence Sharing and Protection Act of 2011 (CISPA). It shields you from liability in your attempts to deal with the threats to your companies and livelihood. It encourages you to freely and efficiently share information with each other and the government.

But our privacy is also very important. We want you to protect us, but not at the expense of our privacy. The lack of respect for our Constitutional and international human rights to privacy and free expression in CISPA alarms us. Here's why:

1. The bill allows virtually any company to "use cybersecurity systems to identify and obtain cyber threat information," and to share that info with unlimited private and government entities. As the EFF suggests, “us[ing] cybersecurity systems” is incredibly vague, and could be interpreted to mean monitoring email, filtering content, or even blocking access to sites. These methods violate our trust, and likely conflict with most companies’ privacy policies. Yet CISPA allows them, without even requiring notification to users, for the purpose of uncovering cyber threats, another vague concept.

2. Cyber threats are so broadly defined as to possibly include misappropriation of intellectual property. Given the confusion and lack of guidelines to intellectual property rights, especially online, companies should not be deputized with a sweeping power to violate personal privacy and deliver personally identifiable information to unlimited numbers of private or government entities – all in the name of unproven copyright claims or the like. After seeing attempts to block website and even internet access in bills like SOPA and PIPA, we are wary of more restrictive intellectual property enforcement.

3. CISPA does little to protect our privacy or civil liberties. The Lieberman-Feinstein and Lungren bills before Congress mandate efforts be made to remove personally identifiable info

about people unrelated to a cyber-attack. CISPA doesn't. Both the McCain bill and Lungren's require a submission to the public of a statement of procedures respecting privacy and civil liberties. The first draft of CISPA didn't require that, either, choosing to put all of its protections in one discredited entity: the Privacy and Civil Liberties Oversight Board. The Board has not been active since early 2008 and currently has no confirmed members. While a newer draft of CISPA calls on the Inspector General of Intelligence Agencies to issue annual reports to Congress, and deliver "appropriate metrics to determine the impact of the sharing… on privacy and civil liberties," yearly retrospective reports will not remedy the immediate threats to civil liberties and privacy posed by cyber security methods each day.

4. CISPA threatens free expression and the press. The First Amendment protects disseminating even information that publishers – from bloggers to the New York Times – know was gotten illegally. Another law protecting "government information" from theft or misappropriation is more likely to target Wikileaks than any foreign government's malicious hacker. Meanwhile, domestic publishers will be less likely to publish risky information. A cybersecurity bill is not the place to alter free speech jurisprudence, and doing so would only threaten whistleblowers and journalists.

5. CISPA is not accountable to civilian or political oversight. First, the bill exempts all shared cyber threat information from FOIA requests. The Freedom of Information Act already exempts trade secrets, confidential financial or commercial data, and any law enforcement related information that impinges on personal privacy or is gotten pursuant to a national security investigation or from a confidential source. Each exemption has been abused, and adding one more to this comprehensive list is unnecessary and harmful. Second, the bill shifts cybersecurity oversight to unaccountable military and intelligence agencies. These agencies do not offer the necessary transparency for proper assessment of the cybersecurity program and its treatment of civil liberties.

CISPA is not the correct path forward. But companies do need guidance in confronting digital security threats. Any cybersecurity legislation should include these mandates:

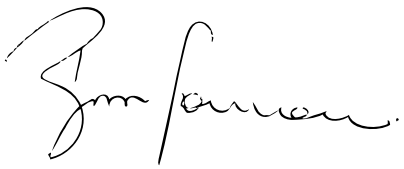
- The coordination and sharing of malware threat information
- Civilian, multistakeholder and inter-agency oversight and control, offering more transparency than military or intelligence services, and regular audits by trusted third parties
- Actions taken under cybersecurity legislation should be publicly disclosed to the fullest extent possible and subject to the FTC Act's prohibitions on unfair and deceptive practices
- Any government agency empowered under cybersecurity legislation should

publicly detail its policy and procedures with respect to civil liberties and privacy
- Precisely defined threats to national security and types of information to be shared
- Release of as little information as necessary to the government, anonymized and scrubbed of personally identifiable data wherever possible, especially of unrelated third parties
- Protection and promotion of digital security measures, including anonymity devices and encryption tools

Based on this analysis, and because of the serious threats to civil liberties CISPA poses, Access believes companies should not support this bill, even with the latest round of revisions from April 12. Access will continue to work to make sure that cyber security concerns by companies are addressed.

For more information or to discuss, please do not hesitate to contact me at the contact details below.

Sincerely,



Brett Solomon
Executive Director | Access
accessnow.org | rightscon.org
+1 917 969 6077