

April 15, 2013

Dear Representative:

Earlier this year, many of our organizations wrote to state our opposition to H.R. 624, the Cyber Intelligence Sharing and Protection Act of 2013 (CISPA). We write today to express our continued opposition to this bill following its markup by the House Permanent Select Committee on Intelligence (HPSCI). Although some amendments were adopted in markup to improve the bill's privacy safeguards, these amendments were woefully inadequate to cure the civil liberties threats posed by this bill. In particular, we remain gravely concerned that despite the amendments, this bill will allow companies that hold very sensitive and personal information to liberally share it with the government, including with military agencies.

CISPA creates an exception to all privacy laws to permit companies to share our information with each other and with the government in the name of cybersecurity. Although a carefully-crafted information sharing program that strictly limits the information to be shared and includes robust privacy safeguards could be an effective approach to cybersecurity, CISPA lacks such protections for individual rights. CISPA's information sharing regime allows the transfer of vast amounts of data, including sensitive information like internet records or the content of emails, to any agency in the government including military and intelligence agencies like the National Security Agency or the Department of Defense Cyber Command.

Developments over the last year make CISPA's approach even more questionable than before. First, the President recently signed Executive Order 13636, which will increase information sharing from the government to the private sector. Information sharing in this direction is often cited as a substantial justification for CISPA and will proceed without legislation. Second, the cybersecurity legislation the Senate considered last year, S. 3414, included privacy protections for information sharing that are entirely absent from CISPA, and the Obama administration, including the intelligence community, has confirmed that those protections would not inhibit cybersecurity programs. These included provisions to ensure that private companies send cyber threat information only to civilian agencies, and a requirement that companies make "reasonable efforts" to remove personal information that is unrelated to the cyber threat when sharing data with the government. Finally, witnesses at a hearing before the House Permanent Select Committee on Intelligence confirmed earlier this year that companies can strip out personally identifiable information that is not necessary to address cyber threats, and CISPA omits any requirement that reasonable efforts be undertaken to do so.

We continue to oppose CISPA and encourage you to vote 'no.'

Sincerely,

Access
Advocacy for Principled Action in Government
American Arab Anti-Discrimination Committee
American Association of Law Libraries
American Civil Liberties Union
American Library Association

Amicus
Association of Research Libraries
Bill of Rights Defense Committee
Breadpig.com
Center for Democracy & Technology
Center for National Security Studies
Center for Rights
Competitive Enterprise Institute
The Constitution Project
Council on American-Islamic Relations
CREDO Action
Daily Kos
Defending Dissent Foundation
Demand Progress
DownsizeDC.org, Inc.
Electronic Frontier Foundation
Fight for the Future
Free Press Action Fund
Government Accountability Project
Liberty Coalition
Mozilla
National Association of Criminal Defense Lawyers
New American Foundation's Open Technology Institute
OpenMedia.org
PolitiHacks
Reddit
RootsAction.org
Tech Freedom