WASHINGTON
LEGISLATIVE OFFICE

April 15, 2013

Vote NO on H.R. 624, the Cyber Intelligence Sharing and Protection Act (CISPA)

Dear Representative:

On behalf of the American Civil Liberties Union (ACLU), its over half a million members, countless additional supporters and activists, and 53 affiliates nationwide, we urge you to vote "NO" on H.R. 624, the Cyber Intelligence Sharing and Protection Act (CISPA). Despite last week's markup in the House Permanent Select Committee on Intelligence, the bill still allows companies to broadly share sensitive and personal information, even directly with military agencies like the National Security Agency (NSA). The bill is a threat to Americans' privacy and civil liberties and we strongly urge you to vote NO when the bill comes to the House floor this week.

1. CISPA Allows Sharing of Personally Identifiable Information

CISPA allows companies to share data they determine to be cyber threat information notwithstanding any other provision of law. Because the longstanding privacy laws that now protect personally identifiable information (PII) would no longer apply, and CISPA itself does not require companies to extract it before they distribute data, companies would be able to share it with each other and the government. This information could include the content of communications, email addresses, location data, contact information or internet use records and could reflect intensely private information like what people read, where they go, how they worship, the political organizations they belong to, their health and financial status and more. This fatal flaw persists despite testimony by industry representatives before the House Intelligence and Homeland Security Committees that such information is not generally needed to fight cyber threats.[1]

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

[1] Advanced Cyber Threats Facing Our Nation, Hearing Before the House Permanent Select Committee on Intelligence, U.S. House of Representatives, 113th Cong. 2013. Paul Smocer from the Financial Services Roundtable, testified before the Intelligence Committee that, "the kind of information we're talking about sharing here seldom, if ever, actually does contain any private information." More quotes from the hearing may be found at http://www.aclu.org/blog/national-security/government-doesnt-need-your-private-info-cybersecurity-members-congress-still.

During markup, the House Intelligence Committee rejected an amendment that would have required the private sector to make reasonable efforts to pull PII from shared data, including by automated processes. If an amendment to protect PII is offered on the floor we strongly urge you to vote "yes" on such an amendment.

2. CISPA Allows Information to Be Shared Directly With Military Agencies Like the NSA

CISPA states that companies may share cyber threat information with each other or with the government. There is no restriction on who the recipients may be and companies could therefore share information directly with the NSA or other military agencies, even when the information pertains to an American citizen exercising his or her rights in the United States.

Under longstanding American legal requirements and policy traditions, the military is restricted from surveilling Americans on American soil. Yet, CISPA would empower military agencies like the NSA to collect more information about internet users in order to respond to online threats. Doing so would create a significant new threat to Americans' privacy, and must be avoided. The NSA has developed extraordinary powers and has been granted broad legal leeway, under the premise that its spying would be focused outside the confines of the territorial United States. Setting it free to collect American information for cybersecurity purposes would be unprecedented, and incredibly dangerous.

None of this is to say that the NSA should have no role whatsoever in protecting US cybersecurity or that companies that currently work with the NSA should stop doing so. However, it is critically important that the broad, new information sharing programs contemplated by CISPA and other information sharing legislation be routed through civilian agencies in the first instance. An amendment that would have prevented new sharing authorities under CISPA to funnel information directly to the military was defeated during committee markup. If such an amendment is offered on the House floor, we strongly urge you to vote "yes" on such an amendment.

3. CISPA Allows Companies to "Hack Back"

CISPA grants immunity to businesses - not just for broad information-sharing of highly personal information, but for any "decisions made" based on information shared under the proposed law. This broad and undefined term could include aggressive measures or "hack backs" that some have termed cyber vigilantism and arguably violate existing criminal law. However, there is little information about what types of countermeasures companies currently take and there have been no hearings or public discussions on what new behavior this section is intended to authorize. This is a controversial and unsettled area of criminal law with serious implications for computer security.

An amendment accepted at markup last week stated that CISPA does not immunize behavior with the "intent to injure, defraud or otherwise endanger", but there is still enough ambiguity in the bill to invite overzealous behavior that could affect sensitive personal information or access to information on the internet. This section still grants full criminal and

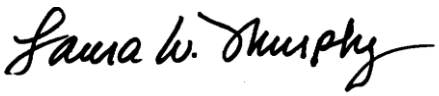
civil immunity to a company that recklessly or unreasonably "hacks back" and unintentionally causes great damage. We strongly recommend that this section be removed from the bill altogether and this issue be addressed only after careful consideration and precise legislative drafting.

4. <u>Recent CISPA Amendments Do Not Mitigate the Fundamental Privacy and Civil Liberties Problems Described Above</u>

Important amendments were accepted at markup that would limit the use of information collected under CISPA, but post-collection protections on information are not a substitute for limiting the sharing of information in the first place or ensuring that it goes to civilian agencies. Use limitations and minimization procedures are an important part of any information-sharing program, but the most significant privacy protections happen at the front end, and not after the fact.

For these reasons, we strongly urge you to vote NO on CISPA when it comes to the House floor this week. Please contact Legislative Counsel Michelle Richardson for more information.

Sincerely,



Laura W. Murphy
Director, Washington Legislative Office

Michelle Richardson
Legislative Counsel