



December 1, 2011

The Honorable Mike Rogers, Chairman  
The Honorable C. A. "Dutch" Ruppertsberger, Ranking Member  
House Permanent Select Committee on Intelligence  
HVC-304 Capitol Building  
Washington, DC 20515

AMERICAN CIVIL  
LIBERTIES UNION  
WASHINGTON  
LEGISLATIVE OFFICE  
915 15th STREET, NW, 6<sup>TH</sup> FL  
WASHINGTON, DC 20005  
T/202.544.1681  
F/202.546.0738  
[WWW.ACLU.ORG](http://WWW.ACLU.ORG)

Re: ACLU Opposition to H.R. 3523, the Cyber Intelligence Sharing and Protection Act of 2011

Dear Chairman Rogers and Ranking Member Ruppertsberger:

LAURA W. MURPHY  
DIRECTOR

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

OFFICERS AND DIRECTORS  
SUSAN N. HERMAN  
PRESIDENT

ANTHONY D. ROMERO  
EXECUTIVE DIRECTOR

ROBERT REMAR  
TREASURER

On behalf of the American Civil Liberties Union, a non-partisan organization with over half a million members, countless additional activists and supporters, and 53 affiliates nationwide, we write in opposition to H.R. 3523, the Cyber Intelligence Sharing and Protection Act of 2011. We ask that you delay markup to consider the privacy implications of the bill that would allow companies to share private data with the government. We urge you to amend the bill to include explicit collection and use limitations and rigorous oversight mechanisms. In the absence of such amendments, we will vigorously oppose this legislation as inconsistent with the long tradition of Americans' reasonable expectations of privacy.

The Cyber Intelligence Sharing and Protection Act would create a cybersecurity exception to all privacy laws and allow companies to share the private and personal data they hold on their American customers with the government for cybersecurity purposes. The bill would not limit the companies to sharing only technical, non-personal data. Instead, it would give the companies discretion to decide the type and amount of information to turn over to the government. If shared in good faith compliance with the statute, these entities would receive full liability protection and would be immune from criminal or civil liability, even after an egregious breach of privacy. Further, once an individual's information is shared with the government, there would be no restriction on the use of that information. It could be used for any purpose whatsoever and shared with any agency. While such data might be used for cybersecurity purposes, there would be no bar on the government also using it to conduct fishing expeditions for criminal, immigration or other purposes.

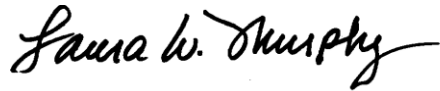
Beyond the potential for massive data collection authorization, the bill would provide no meaningful oversight of, or accountability for, the use of these new information-sharing authorities. Congressional reporting would be delegated to the Privacy and Civil Liberties Oversight Board (PCLOB). But the PCLOB has never been activated, therefore making it likely that no regular, institutionalized and substantive reporting will happen at all. Moreover, no federal agency or official has been tasked with issuing guidance to companies and government agencies as to how best protect privacy.

Writing a statute to govern the sharing of cybersecurity information is a complex and challenging task. But any new programs simply must respect privacy. The White House's May legislative draft, the Recommendations of the House Republican Cybersecurity Task Force, and the Privacy Impact Assessment of Einstein 3 all contained more explicit privacy protections than the new bill. We encourage the committee to borrow from any of these documents in improving the privacy provisions of the legislation. Any new information-sharing legislation must at a minimum do the following:

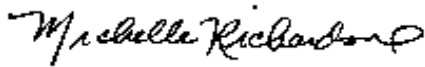
- Narrowly define the privacy laws it will contravene. The committee must carefully consider what privacy laws truly inhibit necessary information-sharing and craft narrow exceptions limited to just those critical circumstances.
- House domestic cybersecurity efforts in a civilian agency. Congress must not empower military or intelligence agencies such as the National Security Agency to collect the internet usage data of Americans. Cybersecurity efforts on American soil should be led by the private sector, and any government information collection must be coordinated by a civilian government agency.
- Require companies to remove personally identifiable information (PII) from data they share with the government. While sharing technical data can take place without implicating civil liberties, a presumption of privacy should protect PII. Sharing PII should be an exception and not the norm, even if there could be certain limited exceptions to cover legitimate emergencies or other narrowly defined situations.
- Limit government use of information shared for cybersecurity purposes. Cybersecurity information-sharing should not become a windfall of data for the federal government to use as it pleases. Any information shared with the government must have strict use limitations to ensure that this new program doesn't become an end run around privacy laws that would otherwise offer stronger protections.
- Create an oversight and accountability structure that includes public and congressional reporting. The executive branch must provide regular, substantive and public reporting, ideally by multiple Inspectors General and/or privacy officers.

We appreciate your consideration and look forward to working with you in the coming months as cybersecurity legislation advances through the House. Please contact Legislative Counsel Michelle Richardson if you should have questions or comments about this correspondence.

Sincerely,



Laura W. Murphy  
Director, Washington Legislative Office



Michelle Richardson  
Legislative Counsel

CC: Members of the House Permanent Select Committee on Intelligence