

June 25, 2013

Dear Senator,

The recent revelations regarding the vast scope of Americans' data being collected under two NSA surveillance programs have heightened our concerns regarding the upcoming Senate debate over cybersecurity legislation. The newly disclosed NSA programs clearly illustrate that the government will interpret any surveillance laws aggressively, and that any new legislation to permit government access to Americans' communications information must include robust and meaningful privacy safeguards to avoid intrusions into our civil liberties and constitutional rights.

Therefore, we, the undersigned organizations, write to urge you to ensure that any new cybersecurity information sharing bill considered in the Senate in 2013 at least maintains the privacy protections from Title VII, the information sharing title of S. 3414, the Cybersecurity Act of 2012. Our organizations agree that the protections in Title VII of S. 3414 last year should be considered the *privacy floor*, and not the ceiling for any cybersecurity legislation. To that end, we would strongly oppose any effort to bring to the Senate floor the information sharing provisions of last year's SECURE IT bill, or otherwise weaken privacy safeguards.

The privacy safeguards included in Title VII of S. 3414 were carefully crafted in an effort to minimize the potential intrusion on Americans' civil liberties. We urge you to maintain the following provisions from last year's bill as the minimum privacy safeguards needed:

- A requirement that information shared with the government as part of a cybersecurity information sharing program be directed only to civilian agencies – recent disclosures about the NSA's misuse of the Patriot Act and the FISA Amendments Act to justify broad and intrusive surveillance programs make it clear that the NSA should not be the direct recipient of private sector cybersecurity information and that strong protections must be built into the law;
- Strict limits to prevent information collected under cybersecurity programs to be used for general criminal prosecutions or national security purposes unrelated to cybersecurity;
- A requirement that companies make reasonable efforts to remove personally identifiable information that is irrelevant to cyber threats before they share threat information;
- Robust oversight and accountability provisions such as independent audits and reports or private rights of action against the government for willful or intentional misconduct;

We believe these provisions from the information sharing title of S. 3414 from last year are the minimum safeguards necessary to protect privacy and civil liberties in any information sharing legislation. We would support expansion of those protections and vigorously oppose any backtracking on them. We urge you to ensure that they are incorporated into any new cybersecurity legislation to be considered by the Senate.

Sincerely,

Access
Advocacy for Principled Action in Government
American Civil Liberties Union
American Library Association
American Arab Anti-Discrimination Committee
Amicus
Association of Research Libraries
Bill of Rights Defense Committee
Breadpig
Center for Democracy & Technology
Center for Media and Democracy
Center for Rights
Competitive Enterprise Institute
The Constitution Project
Council on American-Islamic Relations
CREDO Action
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress
Electronic Frontier Foundation
Entertainment Consumers Association
Fight for the Future
Floor64
Free Press Action Fund
Government Accountability Project
Liberty Coalition
Mozilla
National Association of Criminal Defense Lawyers
OpenMedia.org
OpentheGovernment.org
PEN American Center
Personal Democracy Forum
PolitiHacks
Privacy Rights Clearinghouse
Reddit
RootsAction.org
TechFreedom
U.S. PIRG