

May 10, 2012

Dear Senator,

We, the undersigned organizations, write to express our deep concerns with S. 2105, the Cyber Security Act of 2012. In particular, we are concerned that the information-sharing provisions in Title VII allow companies, “notwithstanding any law,” to share sensitive Internet and other information with the government without sufficient privacy safeguards, oversight or accountability.

We understand S. 2105 is scheduled to be on the Senate floor next week. We urge you to oppose S. 2105 in its current form and to support amendments that address each of the following threats to privacy and civil liberties:

- S. 2105 undermines privacy and cybersecurity by expanding without justification the authority for companies to monitor their clients' and customers' Internet usage for broadly-defined "cybersecurity threats," by authorizing ill-defined "countermeasures" against such "cybersecurity threats," and by immunizing companies against liability for monitoring activities that violate their own contractual obligations.
- S. 2105 creates an exemption from all existing privacy laws to allow companies to share communications and records with the government, even if those personal records are not necessary to describe a cybersecurity threat.
- S. 2105 directs the Department of Homeland Security to designate the government agencies that will serve as “exchanges” to receive the information from the private sector, yet the bill would still allow the NSA and other defense agencies to be designated as exchanges, thereby permitting companies to share private information directly with the military.
- S. 2105 allows information collected for cybersecurity purposes to be used in criminal investigations unrelated to cybersecurity if the information merely “appears to relate to a crime which has been, is being or is about to be committed”—thus circumventing longstanding Fourth Amendment protections that require warrants or other processes designed to protect privacy.
- S. 2105 lacks key meaningful oversight provisions such as mandatory Inspector General reviews; the only independent oversight required is a single report by the Privacy and Civil Liberties Oversight Board, an entity which will only come into existence if the Senate confirms the five nominees to the Board.
- S. 2105 grants legal immunity to entities that share information that is so broad that it overrides even the contracts companies make with their customers, preventing them from competing on privacy grounds through enforceable promises to their users to protect privacy and by failing to give customers effective legal recourse for violations of what little privacy protections the bill offers.

- S. 2105 bars the government from conditioning its disclosure of cybersecurity threat indicators to a private entity on the entity's provision of cybersecurity threat information to the government, but does not bar the government from using federal grants or contracts to coerce such sharing.

Therefore, we urge you to oppose S. 2105 in its current form and to support amendments to address each of these fundamental civil liberties issues.

Sincerely,

Access
The American Association of Practicing
Psychiatrists
American Booksellers Foundation for
Free Expression
American Civil Liberties Union
American Conservative Union
American Library Association
Americans for Limited Government
Association of Research Libraries
Bill of Rights Defense Committee
Hon. Bob Barr
Center for Democracy & Technology
Competitive Enterprise Institute
The Constitution Project
Consumer Federation of America
Cyber Privacy Project
Defending Dissent Foundation
Democrats.com

Electronic Frontier Foundation
Entertainment Consumers Association
Fight for the Future
FreedomWorks
Free Press Action Fund
Government Accountability Project
Less Government
Liberty Coalition
Muslim Public Affairs Council
National Association of Criminal
Defense Lawyers
OpenTheGovernment.org
O'Reilly Media
Privacy Times
Reporters Without Borders
The Republican Liberty Caucus
Startup Weekend
TechFreedom