

THE CONSTITUTION PROJECT



Safeguarding Liberty, Justice & the Rule of Law

FOR IMMEDIATE RELEASE - May 10, 2012

Contact: Larry Akey, Director of Communications, (202)580-6922 [o] or (202)580-9313 [c], lakey@constitutionproject.org

Privacy and Civil Liberties Threatened by Senate Cyber Bill

***Groups: Urge "No" Vote on S. 2105's Current Version,
Support 'Significant' Amendments***

WASHINGTON, D.C. -- A diverse coalition of 34 privacy and civil liberties groups from across the ideological spectrum [wrote to Congress](#) expressing their deep concerns with the Cyber Security Act of 2012, S. 2105. The groups urged senators to vote against the bill in its current form, and to support significant amendments addressing fundamental privacy and civil liberties concerns identified in [their letter](#).

The bill, which is expected to be debated by the Senate in coming weeks, is meant to improve cybersecurity by allowing companies - such as Facebook, Microsoft, and Verizon - to share information about their customers with the government, in an effort to collaboratively identify and address cyber threats.

"However, in the push to increase security, the bill would essentially bypass all existing privacy laws and allow companies to share private, and potentially sensitive, communications and records with the government, even if that personal information is not necessary to describe a cybersecurity threat," TCP's Senior Counsel Sharon Bradford Franklin said.

She also noted that the legislation would permit the government to use the information shared with it in a criminal investigation unrelated to cybersecurity if the information merely "appears to relate to a crime which has been, is being or is about to be committed."

"Not only does this allow uses well beyond the cybersecurity purposes of the bill, but this is a shockingly low bar that fails to incorporate any Fourth Amendment safeguards," she said.

The legislation, co-sponsored by Senators Joe Lieberman (I-CT) and Susan Collin (R-ME), would give the Department of Homeland Security the authority to determine which government agencies would receive the information. As currently drafted, however, the bill would not preclude military agencies - like the NSA and other defense agencies - from receiving these data, thereby allowing companies to share private information about Americans directly with the military.

"Unfortunately, the threats to personal privacy and civil liberties are greatly increased by the lack of meaningful oversight provisions and expansive immunity for businesses sharing the data," Franklin

said.

The Privacy and Civil Liberties Oversight Board - which currently does not exist as it waits for a full slate of members to be confirmed - must submit a single report; no other independent oversight is outlined by the bill.

According to Franklin, "Without sufficient privacy, oversight, or accountability safeguards, this bill has the potential to cause more problems than it solves, and we are calling on the Senate to defeat it."

To learn more about the constitutional threats posed by cybersecurity proposals and recommendations for addressing them, read TCP's bipartisan Liberty and Security Committee report [Recommendations for the Implementation of a Comprehensive Constitutional Cybersecurity Policy](#).

[About The Constitution Project](#)

Created out of the belief that we must cast aside the labels that divide us in order to keep our democracy strong, The Constitution Project (TCP) brings together policy experts and legal practitioners from across the political spectrum to foster consensus-based solutions to the most difficult constitutional challenges of our time. TCP seeks to reform the nation's broken criminal justice system and to strengthen the rule of law through scholarship, advocacy, policy reform and public education initiatives. Established in 1997, TCP is based in Washington, D.C.

