

# THE CONSTITUTION PROJECT



*Safeguarding Liberty, Justice & the Rule of Law*

FOR IMMEDIATE RELEASE - May 14, 2012

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

## **GOP Cyber Bill 'No Better' on Privacy Issues Than Others, Groups Say**

### *TCP Calls Civil Liberties Protections in SECURE IT 'Fundamentally Flawed'*

WASHINGTON, D.C. -- Many of the same groups that raised concerns about the privacy and civil liberties provisions of the lead cybersecurity bill in the Senate, the Cyber Security Act of 2012 (S. 2105), say the alternative put forward by key Republicans has many of the same problems and "in some respects poses even greater threats."

Writing to Senators about S. 2151, the SECURE IT Act of 2012, a [diverse coalition](#) of 33 advocacy organizations from across the ideological spectrum identified a number of privacy and civil liberties concerns with the legislation. In a [letter released today](#), the groups pressed the Senate to reject the bill in its current form.

"The groups joining this letter wanted to make it clear to the Senate that SECURE IT would in no way reduce the privacy and civil liberties threats posed by the Lieberman-Collins bill," said Sharon Bradford Franklin, senior policy counsel at The Constitution Project.

"In fact, both proposals are fundamentally flawed when it comes to privacy safeguards, oversight and accountability, and both bills require substantial amendments to address our concerns," she said.

Like other cybersecurity bills pending before Congress, the SECURE IT Act is intended to help prevent cyber-attacks 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, the groups told Senators the bill's information sharing provisions that allow companies to share sensitive personal data and communications "notwithstanding any law" are overly broad and lack adequate safeguards.

Franklin indicated TCP was particularly concerned the legislation allows private companies to provide the government with personal information that is not necessary to describe a cybersecurity threat, and permits the government to broadly share that information and use it for purposes well

beyond cybersecurity. She said the proposal permits information to be used for national security purposes unrelated to cybersecurity, as well as to investigate and prosecute a long list of crimes, thereby allowing law enforcement to avoid obtaining warrants or using other procedures designed to provide due process and to protect privacy.

"As currently drafted, this legislation should be completely unacceptable to all Americans because it would permit government agents to access personal data and use it for a range of purposes without any of the longstanding protections provided by the Fourth Amendment," Franklin said.

The groups also criticized the measure, which was introduced in March by Sen. John McCain (R-AZ) and several other key Republicans, for facilitating the sharing of private information directly with the NSA and other military agencies. They argued that even if a private company wanted to keep the information out of the hands of military agencies, under the provisions of S.2151 it could not. They noted that, while the Lieberman-Collins proposal permits sharing with military agencies, it does not require it.

The groups signing the letter also said the legislation lacks any meaningful, independent oversight, such as mandatory reviews by the Inspectors General of the affected agencies.

"The only oversight required is reports by the agencies involved, some of which must be coordinated with the Privacy and Civil Liberties Oversight Board, an entity which will come into existence only if the Senate confirms the five nominees to the Board," the groups wrote.

In addition to TCP, among the groups signing the letter are the American Civil Liberties Union, the American Library Association, the Center for Democracy & Technology, the Electronic Frontier Foundation, as well as free-market groups such as the Competitive Enterprise Institute, FreedomWorks, the Liberty Coalition, The Rutherford Institute and TechFreedom.

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.*



Try it FREE today.