FIGHT FOR THE FUTURE

Privacy and Cybersecuity Bills: CISPA, Cybersecurity Act of 2012, and SECURE IT Act
According to Majority Leader Reid, the Senate will soon take up S.2105, the "Cybersecurity Act of 2012." As advocates for basic rights, we are firmly opposed to language in this bill that would eliminate privacy protections on the internet and treat all internet users like criminals. We urge you to **vote NO** on this and any cybersecurity bill without sufficient privacy protections.

These bills would cripple online innovation and have a chilling effect on free speech on the internet. Any cybersecurity legislation should focus on securing networks, not on criminalizing the civilian internet infrastructure. Until our concerns are addressed, Fight for the Future, the viral organizers behind the SOPA and PIPA protests, and its allied groups and individuals will strongly oppose this bill.

- **Reverses privacy laws.** Specifically, we are opposed to the "Information Sharing" provisions in the bills, which through a giant "notwithstanding" clause would nullify decades of consumer privacy laws and establish legal immunity for companies to share personal information of virtually all internet users with the federal government.

- **Wholesale data sharing.** Legal immunity can be used to pressure companies into a program of wholesale user-data sharing with the government. If they were willing to do it when it was illegal (i.e. Bush Admin. warrantless wiretapping program), they'll certainly do it with preemptive legal immunity.

- **Removes protections for non-suspects.** The bills claims to establish "affirmative authority to monitor and defend against cybersecurity threats." However, sharing cybersecurity threat information is already perfectly legal, provided that the parties involved follow basic, well-established legal guidelines for protecting the privacy of non-suspects. The bills remove those protections when there is a "reasonable belief" that information is indicative of a broadly-defined cybersecurity threat. That language is far too expansive for such a drastic civil liberties loophole.

- **No limits on inter-agency sharing.** Under S.2105, personal information would be shared with the Department of Homeland Security, but the bill does not prevent DHS from sharing the information with other government and military agencies, like the National Security Agency. There are no limitations as to what purposes the information can be used for.

- **Violates net neutrality.** Sec. 701 of S.2105 violates net neutrality principles by giving ISPs new authority to block traffic in order to protect against actions that might result in a breach of any information system.

This info sheet was prepared by Fight for the Future, a project of the Center for Rights. For further information or to find out more, contact: team@fightforthefuture.org, 508-474-5248.