THE CONSTITUTION PROJECT

Safeguarding Liberty, Justice & the Rule of Law

FOR IMMEDIATE RELEASE - April 11, 2012
Contact: Larry Akey, Director of Communications, (202)580-6922 [o] or (202)580-9313 [c], lakey@constitutionproject.org

ISSUE ALERT: Cybersecurity Bills Pending in U.S. House Threaten Privacy Rights and Civil Liberties

TO: Editorial Page Editors and Writers
FR: Virginia Sloan, President
The Constitution Project

The Constitution Project (TCP) believes cybersecurity legislation currently pending before Congress poses major risks to civil liberties that must be addressed before any bill is enacted into law. The U.S. House of Representatives intends to take up this issue later this month (most likely during the week of April 23) and the Senate is also poised to act this year. Therefore, I urge you to editorialize on the need for Congress to include strong civil liberties protections in any cybersecurity legislation it adopts.

Cybersecurity is important to all Americans, both as a way to protect critical economic and physical infrastructure, and because it can make the internet a safer place to shop, conduct business, and communicate with others. The four major cybersecurity bills before Congress would all establish information sharing programs that authorize the sharing of cybersecurity threat information between and among the federal government and the private sector, permitting the federal government to share classified cyber-threat information with the private sector, and allowing the private sector to share information about cyber-attacks on their network with other members of the private sector and with the federal government. This is the correct approach to cybersecurity, but only if proper safeguards are incorporated to protect individual constitutional rights.

Without adequate safeguards, information sharing programs create real risks to constitutional freedoms in the same way a perpetual wiretap on your phone, or a government agency opening and reading all your mail, would. Although with information sharing the government would not directly monitor private internet usage, if private companies turn over all their internet traffic to the government, this would simply amount to government surveillance with a time lag. Under the very broad definitions in some of the congressional cybersecurity bills of what information can be shared with the government, an internet service provider that monitors its networks for cyber-attacks could share all its email traffic with the federal government. Without proper requirements for data minimization and anonymization, the federal government would then have access to the personally identifiable information ("PII") of the senders and recipients, as well as the content of the communications, including potentially sensitive constitutionally protected information, such as religious beliefs or political opinions. Moreover, without strict use limits, the government could share this PII and the content of communications with any other agency and do so

for purposes completely unrelated to cybersecurity.

Earlier this year, TCP's bipartisan Liberty and Security Committee released Recommendations for the Implementation of a Comprehensive and Constitutional Cybersecurity Policy, a report containing its proposals regarding oversight, privacy, and use restrictions for any future federal cybersecurity initiatives, and particularly information sharing programs. Members of the Committee include former members of Congress, retired judges and military officers, eminent academics and legal practitioners, and public policy analysts from across the ideological spectrum.

Based upon the recommendations of TCP's Liberty and Security Committee, it is critical that any federal cybersecurity program include the following protections:

- All cybersecurity programs that rely on information sharing between the government and the private sector should limit the sharing of PII and content of communications between the private sector and government actors. Data shared between the government and the private sector should have sensitive PII removed and sanitized.
- Any cybersecurity legislation, regulation, or agency directive regarding information sharing should require (1) strict time limits for data retention, (2) data anonymization whenever possible, and (3) polices to diminish the risk of inadvertent or improper disclosure of PII. PII should only be collected, retained or disseminated when it is necessary to protect against or mitigate a cybersecurity threat.
- Only civilian agencies should be recipients of the information being shared by the private sector, to ensure proper incorporation of privacy safeguards and to promote transparency and accountability to the public for any failure or abuse. Congress should resist efforts to make the National Security Agency -- a military intelligence-gathering entity that by its very nature operates in secret -- a recipient of cyber-threat information from the private sector.
- Independent oversight of the U.S. cybersecurity program should be established to ensure that Americans' privacy rights and civil liberties are protected. The bills' reliance on the Privacy and Civil Liberties Oversight Board (PCLOB) is appropriate - but only if and when the Senate confirms its members, and it actually comes into existence. In addition, Congress should require periodic mandatory audits by the Inspectors General of all agencies involved in maintaining cybersecurity in the United States. These reports should include a discussion of the types and amount of information being shared with the federal government and how the information is used.
- Congress should require that content obtained by the federal government through the cybersecurity program only be used as necessary to prevent cyber-attacks and protect networks. Content should not be shared with other law enforcement agencies, or relied upon as evidence of a non-cybercrime, unless the content was a necessary component of data flagged as a possible cybersecurity threat, or there is probable cause of a non-cybercrime.

The Constitution Project agrees that our nation's critical network infrastructures must be protected from the threat of cyber-attacks. We think it is essential, however, that any legislation to combat this growing problem must preserve our most basic constitutional liberties. We urge your paper to take a strong position in support of Congress preserving privacy rights and civil liberties when it adopts cybersecurity legislation.

This memorandum provides links to our report, a FAQ on cybersecurity and privacy and a side-by-side comparison of provisions of the four major legislative proposals prepared by the Center for Democracy and Technology. If you need additional information or wish to speak to me, please do not hesitate to contact TCP's Director of Communications, Larry Akey, at (202)580-6922. Additionally, if you would like to talk to any of the members of the Committee that developed our recommendations, please let us know so we may help facilitate such a contact.

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.