GlobalResearch
Center for Research on Globalization

Destroying Online Privacy: Cyber Intelligence Sharing and Protection Act (CISPA) Is Back

By Stephen Lendman
Global Research, February 21, 2013

Region: USA
Theme: Law and Justice, Police State & Civil Rights

It shouldn't surprise. The 2011 Cyber Intelligence Sharing and Protection Act (CISPA) never really went away. It ducked and covered for another day.

It's more about destroying personal freedom than online security. It gives government and corporate supporters unlimited power to access personal/privileged information online.

Civil liberty protections are ignored. Security experts, academics, and other professionals expressed outrage. They called CISPA and John McCain's SECURE IT Act measures that "allow entities who participate in relaying or receiving Internet traffic to freely monitor and redistribute those network communications" unjustifiably.

They encourage transferring private communications to government agencies. Accountability and transparency are lacking. Vague language describes network security attacks, threat indicators, and countermeasures.

Innocuous online activities can be called cybersecurity threats. Eroded privacy laws will be gutted. Web sites visited, personal emails, and other online contact may be freely accessed.

Obama's State of the Union address stressed no-holds-barred cyberwar. Earlier he declared waging it globally.

In May 2009, he prioritized cybersecurity. He called cyber-threats "one of the most serious economic and national security challenges we face as a nation."

"America's economic prosperity in the 21st century will depend on cybersecurity," he claimed.

He ordered a top-to-bottom assessment. A Cyberspace Policy Review followed. He supports draconian cybersecurity bills. Passage threatens constitutional freedoms.

His February 12 Executive Order (EO) called for "Improving Critical Infrastructure Cybersecurity."

Threats continue to grow, it said. National security challenges must be met.

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

“We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.”

Following Obama’s EO, lawmakers revisited CISPA. On February 14, Rep. Mike Rogers (R. MI) and Dutch Ruppersberger (D. MD) reintroduced it.

Last April, it passed the House 248 – 168. Civil libertarian outrage gave senators second thoughts. The bill died in committee. It’s now back from the dead.

On February 13, the ACLU responded. It said CISPA “fails to protect privacy.”

Reintroducing it lets “companies share sensitive and personal American internet data with the government, including the National Security Agency and other military agencies.”

“CISPA does not require companies to make reasonable efforts to protect their customers’ privacy and then allows the government to use that data for undefined ‘national-security’ purposes and without any minimization procedures, which have been in effect in other security statutes for decades.”

On February 13, the Electronic Frontier Foundation (EFF) headlined “CISPA, the Privacy-Invading Cybersecurity Spying Bill, is Back in Congress.”

It’s the same “contentious bill civil liberties advocates fought last year.” It poorly defines cybersecurity exemptions to privacy law.”

It offers “broad immunities to companies (wishing) to share data with government agencies (including the private communications of users) in the name of cybersecurity.”

It lets companies share data with federal agencies. They include military intelligence ones like NSA.

EFF categorically opposes CISPA. It’s deeply flawed. According to the Project on Freedom, Security & Technology at the Center for Democracy & Technology:

“Under a broad cybersecurity umbrella, it permits companies to share user communications directly with the super secret National Security Agency and permits the NSA to use that information for non-cybersecurity reasons.”

“This risks turning the cybersecurity program into a back door intelligence surveillance program run by a military entity with little transparency or public accountability.”

“Members should seriously consider whether CISPA – which inflamed grassroots activists last year and was under a veto threat for these and other flaws – is the right place to start.”

Last October, Obama signed a secret directive. It addressed cyberattack defense. It set guidelines for confronting cyberspace threats. It lets military personnel act more aggressively.

Called Presidential Policy Directive 20, it’s “the most extensive White House effort to date to wrestle with what constitutes an ‘offensive’ and a ‘defensive’ action in the rapidly evolving world of cyberwar and cyberterrorism, where an attack can be launched in milliseconds by

unknown assailants utilizing a circuitous route."

"For the first time, (it) explicitly makes a distinction between network defense and cyber operations to guide officials charged with making often rapid decisions when confronted with threats."

The order updates Bush's 2004 presidential directive. It vets operations outside government owned systems.

Fiber operations previously considered offensive (because they go outside defended networks) are now called defensive. They include "severing the link between an overseas server and a targeted domestic computer."

Pentagon officials are expected to finalize new cyberwar rules of engagement. They set guidelines for military commanders. They'll be able to act outside government networks.

They'll be able to compromise personal privacy. Preventing cyberattacks will be claimed as pretext.

Last fall, Defense Secretary Leon Panetta warned of a "cyber Pearl Harbor." It could "cause physical destruction and loss of life," he said. It could "paralyze and shock the nation and create a new profound sense of vulnerability."

US officials never lack for hyperbole. Fear-mongering is longstanding policy. Lies substitute for truth and full disclosure.

CISPA 2.0 reflects old wine in new bottles. Troublesome issues remain. EFF addressed them.

New legislation lets business use cybersecurity systems. Doing so permits accessing alleged cybersecurity threat information (CTI).

Personal communications are included. Perceived threats to networks or systems are pretexts.

Imposed limitations are weak. They only involve acting for vaguely defined cybersecurity purposes.

At the same time, broad immunity from legal liability for monitoring, acquiring, or sharing CTI is extended. It's given as long as entities act "in good faith."

EFF expressed grave concerns. Provisions this broad will "override existing privacy laws." They include the Wiretap Act and Stored Communications Act.

The new law also provides immunity "for decisions made based on" CTI. Doing so makes bad legislation worse. "A rogue or misguided company could easily make bad 'decisions.' " They'll do lots more harm than good.

CISPA "raises major transparency and accountability issues." Information given Washington will be exempt from FOIA requests and state laws requiring disclosure.

Users probably won't know if their private data ends up compromised. They'll have little recourse either way.

If companies send information about users claimed unrelated to cyberthreats, government agencies getting it won't notify them. Companies alone may or not do it. Who monitors them to make sure?

"CISPA is a dangerous bill," said EFF. So is CISPA 2.0. It "equates cybersecurity with greater surveillance and information sharing."

It's little changed from its original form. It lets government and companies bypass existing laws, access what they wish, filter content, and potentially shut down online access for cybersecurity or national security reasons.

It assures unrestricted Big Brother spying. Government and business will take full advantage.

Many cybersecurity problems arise from software vulnerabilities. Human failings compound them. CISPA leaves these and other important issues unaddressed.

Obama's EO encourages government agencies to share cybersecurity information with companies. It leaves plenty of room for abusive practices. Business will take full advantage. So will government agencies.

Enacting CISPA 2.0 ensures abuse. Freedoms taken for granted will disappear. Any site, blog, or personal content can be called a cyber threat.

Online users will lose out. So will everyone. Police state harshness will be hardened. America's already hugely repressive. It's a hair's breath from full-blown tyranny.

Stephen Lendman lives in Chicago and can be reached at lendmanstephen@sbcglobal.net.

His new book is titled "Banker Occupation: Waging Financial War on Humanity."

http://www.claritypress.com/LendmanII.html

Visit his blog site at sjlendman.blogspot.com and listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network Thursdays at 10AM US Central time and Saturdays and Sundays at noon. All programs are archived for easy listening.

http://www.progressiveradionetwork.com/the-progressive-news-hour

http://www.dailycensored.com/cispa-is-back/

Articles by: Stephen Lendman

About the author:

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III." http://www.claritypress.com/LendmanIII.html Visit his blog site at sjlendman.blogspot.com. Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network. It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.