New American

Written by Joe Wolverton, II, J.D. on February 12, 2013



Will Obama Take Control of the Internet This Week?

As early as Wednesday, President Obama could issue an executive order granting the federal government expansive and unprecedented power over one of the few remaining outposts of uncensored information — the Internet.

Various news agencies are reporting that a cybersecurity executive order has been drafted and will be issued by the president this week. <u>A story on NextWeb</u> indicates that the president will address the issue (and announce the executive order) in Tuesday's State of the Union address.



<u>Bloomberg adds credibility</u> to the speculation, quoting "two former White House officials briefed on the administration's plans" who corroborate the Wednesday release date for the executive order.

<u>The Wall Street Journal reports</u> that unnamed White House officials disclosed that the order will indeed be issued Wednesday and that it "would create a federal-government led group to work with the private sector to create and implement voluntary standards for companies running critical infrastructure. It would also take additional measures to improve information sharing and bolster cybersecurity through current regulatory authorities."

Voluntary is a word — like so many others — that doesn't have the same meaning in Washington, D.C., as it does in the rest of the country.

Given the federal government's penchant for vague language, however, it is likely that despite the denial of compulsory cooperation with the government there will be a loophole just large enough to force through a requirement of corporate cooperation with the intelligence agencies of the Obama administration.

According to information obtained by *The New American*, the executive order will resemble in almost every detail a cybersecurity bill that will be introduced to Congress on Wednesday.

That bill, <u>as reported by the American Civil Liberties Union (ACLU)</u>, will empower the "National Security Agency (NSA) and the military to collect your private internet records." All in the name of national security, of course.

The measure that will be offered in the House of Representatives on Wednesday will be nothing less than a resurrection of the Cyber Intelligence Sharing and Protection Act (CISPA), that was passed by the House in April of last year.

<u>According to *The Hill*</u>, House Intelligence Committee Chairman Mike Rogers (R-Mich.) and ranking member Representative Dutch Ruppersberger (D-Md.) will re-introduce an unamended CISPA this week during a speech at the Center for Strategic and International Studies in Washington, D.C.

That bill<u>, H.R. 3523</u>, established an exemption to all privacy laws allowing companies to transmit private user/subscriber information with other companies and with the government for the purpose of

New American

Written by Joe Wolverton, II, J.D. on February 12, 2013



protecting cybersecurity. In exchange for their compliance with the "voluntary" delivery of users' private data to the NSA and Department of Homeland Security (DHS), the federal government will shield participating companies for any liability stemming from challenges to the government's use of the electronic communication of its customers.

The <u>AP reported last October</u> that "selected employees at critical infrastructure companies would receive security clearances allowing them to receive the information."

CISPA is yet another example of the cooperation between industry and government that threatens to squeeze the life out of the Constitution and place every actual and virtual activity of every American under the constant surveillance of government.

There is a curb on that power, however. CISPA mandates that the government may use the information it obtains only for "lawful purposes," defined in the bill as preventing anything that could potentially threaten the nation's national or Internet security.

There is no time limit on this power and the only oversight will be an annual audit by the inspector general of the federal intelligence community.

Despite these extraordinary and chilling abridgments of the Fourth Amendment, there is broad bipartisan support for CISPA, despite its unpopularity outside the Beltway. As <u>The New American</u> reported after the House passage last year, "Passage in the House was assured with more than 70 percent of those supported by the Tea Party voting for it."

When the measure moved to the Senate it was voted down and President Obama threatened to veto it. That could be, of course, because the White House preferred to set the boundaries of the authority to monitor the traffic on the Internet.

President Obama has consistently added one document after another to his bulging dossier of dictatorship.

As early as last fall, President Obama began work on the fiat that will, according to a draft of the executive order obtained by the Associated Press, order "U.S. spy agencies to share the latest intelligence about cyberthreats with companies operating electric grids, water plants, railroads and other vital industries to help protect them from electronic attacks."

For some time, government officials have insisted that Iran is planning a cyberattack on the electronic communications infrastructure of the United States. The AP reports that Defense Secretary Leon Panetta said that the U.S. armed forces are "ready to retaliate" should Iran — or any other country — attempt an attack on U.S. cybersecurity.

Those reports as well as recent allegations of Chinese cyberattacks against the <u>New York Times</u>, the <u>Wall Street Journal</u>, and the <u>Washington Post</u>, and attacks by <u>Anonymous on the Federal Reserve's</u> cyberstructure have given the president the threats of a "cyber 9/11" that he needs to justify his issuing of an edict with all the unconstitutional assaults on civil liberty of a "cyber Patriot Act."

President Obama's administration has been prepping members of Congress for some time on their irrelevance in the upcoming electronic information monitoring scheme.

<u>In a hearing held last September</u> before the Senate Committee on Homeland Security and Governmental Affairs, Department of Homeland Security Secretary Janet Napolitano testified that assuming control of the nation's Internet infrastructure is a DHS responsibility.

New American

Written by Joe Wolverton, II, J.D. on February 12, 2013



"DHS is the Federal government's lead agency for securing civilian government computer systems and works with our industry and Federal, state, local, tribal, and territorial government partners to secure critical infrastructure and information systems," she informed senators.

Napolitano's report on the role of DHS squares with the information revealed in the seven-page version of the <u>executive order obtained last year by the AP</u>. According to the report of their findings:

The draft order would put the Department of Homeland Security in charge of organizing an information-sharing network that rapidly distributes sanitized summaries of top-secret intelligence reports about known cyberthreats that identify a specific target. With these warnings, known as tear lines, the owners and operators of essential U.S. businesses would be better able to block potential attackers from gaining access to their computer systems.

The president's de facto re-routing of all Internet traffic through federal intelligence officers deputizes more than just DHS as cybertraffic cops. The AP reports that "the Pentagon, the National Security Agency (NSA), the director of national intelligence, and the Justice Department" will all cooperate in the surveillance — again, the same agencies whose powers were either created or expanded in the Patriot Act.

Despite the anticipated similarities between CISPA, the Patriot Act, and President Obama's forthcoming cybersecurity executive order, there is one very significant difference. Legislation can be repealed. Constituents can unite and threaten the reelection hopes of lawmakers who vote for such a bill.

An executive order, on the other hand, is unassailable, and the president — particularly one in his final term — is beyond accountability for the edicts he hands down and for the irreparable harm they might do to civil liberties and to the Constitution that protects them.

Photo of President Barack Obama: AP Images

Joe A. Wolverton, II, J.D. is a correspondent for The New American and travels frequently nationwide speaking on topics of nullification, the NDAA, and the surveillance state. He can be reached at <u>jwolverton@thenewamerican.com</u>.



Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



Subscribe

What's Included?

24 Issues Per Year Optional Print Edition Digital Edition Access Exclusive Subscriber Content Audio provided for all articles Unlimited access to past issues Coming Soon! Ad FREE 60-Day money back guarantee! Cancel anytime.