Obama could use bill to kill Internet

A controversial bill that will empower President Barack Obama to switch off privately-owned computer systems during a "national cyber-emergency," and to prohibit any review of such an act by the court system, will return to congress this year.

The idea of creating what some critics have called an Internet "kill switch" that the president could flip in an emergency is not exactly new.

In August 2009, a draft Senate proposal authorized the White House to "declare a cyber-security emergency." Meanwhile, another Senate proposal would have explicitly given the government the power to "order the disconnection" of certain networks or Web sites.

House Democrats have taken a similar approach in their own proposals.

Civil libertarians and some industry representatives have repeatedly raised concerns about the various proposals to give the executive branch such broad emergency power.

HIGHLIGHTS

The new U.S. Senate bill would grant the president far-reaching emergency powers to seize control of or even shut down portions of the Internet.

The legislation announced on Thursday says that companies such as broadband providers, search engines, or software firms that the government selects "shall immediately comply with any emergency measure or action developed" by the Department of Homeland Security. Anyone failing to comply would be fined.

That emergency authority would allow the federal government to "preserve those networks and assets and our country and protect our people," Joe Lieberman, the primary sponsor of the measure and the chairman of the Homeland Security committee, told reporters on Thursday. Lieberman is an independent senator from Connecticut who caucuses with the Democrats.

Because there are few limits on the president's emergency power, which can be renewed indefinitely, the densely worded 197-page bill is likely to encounter stiff opposition.

TechAmerica, probably the largest U.S. technology lobby group, said it was concerned about "unintended consequences that would result from the legislation's regulatory approach" and "the potential for absolute power." And the

Center for Democracy and Technology publicly worried that the Lieberman bill's emergency powers "include authority to shut down or limit Internet traffic on private systems."

The idea of an Internet "kill switch" that the president could flip is not new. A draft Senate proposal that CNET obtained in August allowed the White House to "declare a cyber-security emergency," and another from Sens. Jay Rockefeller (D-W.V.) and Olympia Snowe (R-Maine) would have explicitly given the government the power to "order the disconnection" of certain networks or Web sites.

Under the proposal, the federal government's power to force private companies to comply with emergency decrees would become unusually broad. Any company on a list created by the Homeland Security that also "relies on" the Internet, the telephone system, or any other component of the U.S. "information infrastructure" would be subject to command by a new National Center for Cyber-security and Communications (NCCC) that would be created inside Homeland Security.

Lieberman's proposal would form a powerful and extensive new Homeland Security bureaucracy around the NCCC, including "no less" than two deputy directors, and liaison officers to the Defense Department, Justice Department, Commerce Department, and the Director of National Intelligence. (How much the NCCC director's duties would overlap with those of the existing assistant secretary for infrastructure protection is not clear.)

The NCCC also would be granted the power to monitor the "security status" of private sector Web sites, broadband providers, and other Internet components. Lieberman's legislation requires the NCCC to provide "situational awareness of the security status" of the portions of the Internet that are inside the United States -- and also those portions in other countries that, if disrupted, could cause significant harm.

Selected private companies would be required to participate in "information sharing" with the Feds. They must "certify in writing to the director" of the NCCC whether they have "developed and implemented" federally approved security measures, which could be anything from encryption to physical security mechanisms, or programming techniques that have been "approved by the director." The NCCC director can "issue an order" in cases of noncompliance.

The prospect of a vast new cyber-security bureaucracy with power to command the private sector worries some privacy advocates. "This is a plan for an auto-immune reaction," says Jim Harper, director of information studies at the libertarian Cato Institute. "When something goes wrong, the government will attack our infrastructure and make society weaker."

A new White House office would be charged with forcing federal agencies to take cyber-security more seriously, with the power to jeopardize their budgets if they fail to comply. The likely effect would be to increase government agencies' demand for security products. CNET

FACTS & FIGURES

In 2001, the NSA installed specialized eavesdropping equipment around the country to wiretap calls, faxes, and emails and collect domestic communications originally targeted at Arab-Americans.

Over 25 eavesdropping facilities exist in San Jose, San Diego, Seattle, Los Angeles, and Chicago among other cities.

In 2009, as part of the Cyber Command the NSA built a one million square feet data warehouse at a cost of $1.5 billion at Camp Williams in Utah, as well as another massive data warehouse in San Antonio.

After the September 11 attacks, the government permitted the use of technical means to hack into the e-mails and internet communications of American citizens.

The U.S. and its intelligence authorities monitor whoever they want, and erase any information that they claim might threaten U.S. national interests.

The Patriot Act allows law enforcement agencies to search telephone, email communications, medical, financial and other records.

On July 9, 2008, the Foreign Intelligence Surveillance Act Amendments Act passed by the Senate, grants legal immunity to telecommunication companies that take part in wiretapping programs.

From 2002 to 2006, the FBI collected thousands of phone records of U.S. citizens through mails, notes and phone calls.

In September 2009, the U.S. set up an Internet security supervision body, which allows the U.S. government the use of Internet security as an excuse to monitor and interfere with personal systems.

In 2009, the NSA had intercepted private email messages and phone calls of Americans beyond the broad legal limits established by the U.S. Congress the year before.

RG/SM/KA