Written by **Michael Tennant** on June 14, 2010

Senate Considers Making the President King of Cyberspace

The Internet is a wonderful invention that has allowed for the dissemination of a wide variety of ideas. Not surprisingly, politicians, never ones to brook dissent cheerfully, are not terribly fond of it. In 1998, then-First Lady Hillary Clinton said, "We're all going to have to rethink how we deal with the Internet. As exciting as these new developments are, there are a number of serious issues without any kind of editing function or gatekeeping function."

Recently President Obama lamented the fact that the smorgasbord of news sources now available to Americans can "reinforce and even deepen the political divides in this country" because people can choose only to listen to those with whom they agree; he was particularly concerned with rhetoric that speaks of "our government" as "some menacing, threatening foreign entity."

The only question for the politicians, then, is how to implement a "gatekeeping function" without running afoul of Americans' natural preference for freedom of speech and of the press.

The Federal Trade Commission is proposing government licensing of news organizations, accompanied by taxes on other websites that link to these government-approved sources and taxes on electronic news-reading devices to prop up dying government-approved newspapers.

The U.S. Senate, for the third time in the last year, is attempting to go even further, putting forth legislation that would, according to CNET News, "grant the president far-reaching emergency powers to seize control of or even shut down portions of the Internet." The 197-page bill, called the Protecting Cyberspace as a National Asset Act (PCNAA), was announced on June10 by Sen. Joe Lieberman (I-Conn.). (The previous two attempts were draft proposals to do substantially the same thing as PCNAA.)

Under PCNAA, the President may unilaterally "issue a declaration of national cyber emergency to covered critical infrastructure." Once the declaration has been issued, says CNET, "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." Furthermore, this also applies to "any company on a list created by Homeland Security that also 'relies on' the Internet, the telephone system, or any other component of the U.S. 'information infrastructure,'" according to CNET. These entities will come under the command of a new bureaucracy, the National Center for Cybersecurity and Communications

(NCCC), housed within Homeland Security.

Once issued, the cyber emergency declaration ostensibly expires at the end of 30 days. However, given that the President, with the consent of the Director of Cyberspace Policy (head of the proposed White House Office of Cyberspace Policy who is appointed by the President), can extend the emergency for another 30 days at will, the "emergency" can, for all practical purposes, continue indefinitely.

It's not hard to imagine a scenario in which an embattled President seizes upon a minor incident — one, perhaps, that he says he can't even reveal because to do so would compromise U.S. national security — to declare such an emergency and then uses that emergency to crush dissenting websites under the theory that such websites "send signals to the most extreme elements of our society that perhaps violence is a justifiable response," as Obama said in the speech referenced earlier.

Even if a cyber emergency is never declared, PCNAA still provides for a vast increase in the federal government's control over cyberspace. CNET reports:

> 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.

Among those selected private companies will surely be large, established firms who can bear the costs of compliance, knowing that those same costs will keep competitors from springing up.

These and other companies' compliance will also be procured by the immunity from civil lawsuits that PCNAA offers. Once the President has declared a cyber emergency, any company that complies with NCCC's directives cannot be sued for economic harm. Moreover, says CNET, "if the harm is caused by an emergency order from the Feds, not only does the possibility of damages virtually disappear, but the U.S. Treasury will even pick up the private company's tab."

For those cybersecurity producers that still look askance at federal oversight, there's also language in the bill requiring federal agencies to beef up their cybersecurity, which will surely mean increased federal purchases of security products. Lieberman is leaving nothing to chance.

If PCNAA becomes law, Clinton will finally have her "gatekeeping function," and Obama and future Presidents will have it within their power to silence critics on the Web in the name of national security. Meanwhile, the independence of websites and Internet service providers and the privacy of their customers will be severely compromised, emergency or no emergency. It makes one long for the days when politicians merely claimed to have invented the Internet, not to *own* it.

Photo: Internet monitoring room in South Korea: AP Images