



Our View: Congress messing with the Internet

March 15, 2012

Congress just won't let the Internet alone. In January, online companies such as Wikipedia and Google organized people to protest two bills, the Stop Online Piracy Act in the House of Representatives and the Protect Intellectual Property Act in the Senate. SOPA and PIPA would have allowed the government easily to shut down websites accused of violating intellectual-property protections.

At the time, Jim Harper said that Congress would cook up something similar; he's director of information and policy studies at the libertarian Cato Institute. He warned, "They perhaps want to teach the public a lesson. You don't tell them what to do. They tell you what to do."

The new mischief is H.R. 3523, the Cyber Intelligence Sharing and Protection Act of 2011, by Rep. Mike J. Rogers, R-Mich. Wait a minute. Weren't Republicans put back in charge of the House in November 2010 by an electorate that demanded less government?

According to the summary by the Electronic Frontier Foundation, H.R. 3523 "would let companies spy on users and share private information with the federal government and other companies with near-total immunity from civil and criminal liability. It effectively creates a 'cybersecurity' exemption to all existing laws." That means Google, Facebook or your phone company could collect your emails or phone messages for "cybersecurity purposes" — broadly defined — and share your information with other companies and government agencies.

Harper offered an update Monday. He said, "The upshot is that no law applies" to what government and companies can do with your information. "That has sent me through the roof. It would create a legal-free zone."

He explained that H.R. 3523 is a bit different from the bills spiked in January, which involved disabling websites. H.R. 3523 allows almost unlimited snooping. "But there are parallels. Both are examples of Congress mucking around with the Internet. Congress

doesn't know how the Internet works. It should not be passing legislation on these subjects."

Harper said that intelligence and police agencies already can obtain warrants to snoop on people, as required by Fourth Amendment, which stipulates: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." For example, police can obtain a warrant to snoop on a suspected terrorist. Unfortunately, the USA Patriot Act and other laws already have made it easier to snoop on people without a warrant.

But H.R. 3523 would go much further. "Cybersecurity is thousands of different problems," Harper said. "And Congress doesn't know what they are. They don't know what the information or what the law is. So, they write a new law that is extremely broad in defining cybersecurity."

Broad laws are the definition of tyranny. The American Revolution was fought, in part, to prevent them. The Virginia Declaration of Rights, written by George Mason early in 1776, explained why free Americans rejected a specific British tyranny, stipulating, "That general warrants, whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive."

The Fourth Amendment also spells out that a search warrant is only valid when "particularly describing the place to be searched, and the persons or things to be seized."