Communications Daily

Free-Market Groups Urge Caution in CISPA Debate

By: Jimm Phillips - March 19, 2013

Congress should take its time in considering the Cyber Intelligence Sharing and Protection Act (CISPA) and other cybersecurity legislation that may involve information sharing, said Ryan Radia, the Competitive Enterprise Institute's (CEI) associate director-technology studies, at a joint CEI-TechFreedom event Monday. Both groups were part of a free market-oriented coalition that opposed CISPA when it was being considered last year (WID April 24/12 p5). The bill passed the House then but did not get a vote in the Senate amid strong White House opposition. There has been pressure for Congress to move quickly on legislation to augment President Barack Obama's recent cybersecurity executive order, but a slower process won't make the situation "much worse off" than it is already, Radia said. "This is the time to do something, but let's do something right. This is going to be on the books for a long time, and a problematic law ... will create bad precedent." Radia and other experts said they were concerned about the implications of information sharing provisions in the current version of CISPA.

CISPA is not specific on key issues, such as the cybersecurity problems it will actually solve or the kinds of information that need to be collected, said Julian Sanchez, a Cato Institute research fellow. Cato was also a part of the coalition that opposed CISPA. The result is a bill that's heavy on vague terms like "cyberthreat indicators," he said. CISPA's vagueness is intentional, as policymakers wanted to keep the bill tech-neutral, so it would remain applicable as technology changed, Sanchez said. Since companies are likely to push vague definitions to their absolute limits, the final bill needs to be narrowly crafted to deal with a "demonstrable problem," he said.

The liability immunity provision in CISPA is particularly problematic, since it removes the incentive for companies to be careful about the information they share with the government, potentially exposing personal information as a result of oversharing, said Jerry Brito, a Mercatus Center senior research fellow. Industry is already allowed to share cyberthreat data with the government, though there are limits based on a company's contractual obligations to its customers that prevent the disclosure of personally identifiable information, he said. Though it's likely that companies are sincere when they say they will not share customers' personal information with the government, the liability immunity provision removes the "backstop" that legally prevents them from doing so, Brito said. Without that incentive, their behavior will "change over time," he said.

"Willy-nilly" increases in government access to data set a "dangerous precedent" for the rest of the world, said TechFreedom President Berin Szoka. Other countries would "love to have moral legitimacy" to justify actions like the "Great Firewall of China," he said. "We too often forget that what we do in this country sets the model for everyone else." The CISPA debate is "particularly ironic" given that the E.U. has become more "feverish" in ensuring privacy protections, Szoka said.