The Washington Times

CREWS: An industry, not a bureaucracy

Competitive market can make the Internet more secure than regulators

By Wayne Crews

-

The Washington Times

6:21 p.m., Tuesday, September 21, 2010

Online security problems are real, but the increasing tendency to treat cybersecurity as a government-spearheaded function asks for big trouble.

Case in point is the new bipartisanProtecting Cyberspace as a National Asset Act of 2010, which establishes severa new federal acronyms and is lately accused, perhaps unfairly, of granting the feds a "kill switch" for the Internet. The bill, supported by many tech firms, sets up public-private partnerships for "best practices" and risk-based security requirements, mandates reporting certain breaches to government and grants liability protections to industry.

Ironically, vulnerabilities in the government's own information-security policies have long been noted. A solid act might instead in its entirely read "Title I: Stop losing federal laptops." And "Title II: Stop hooking critical infrastructure to the Internet." That's too flip, but consider that there are cybersecurity risks to proscriptive cybersecurity legislation (and the resultant regulation) that industry and policymakers may not appreciate.

Cyberspace is not a "national" asset, it's a conglomeration of them. There are cyberspaces, many of them yet to come. Policymakers and the tech community should be cautious about proposals to overly collectivize and centralize regulation of any frontier industry. There is little case for government steering while forcing the market row.

Politicians often take the easy path of setting up redundant cybersecurity agencies and programs and seeking massive sums to establish taxpayer-funded subsidies and research grants for politically favored initiatives. Promoting one set of technological standards or class of providers at the expense of others steers cybersecurity research away from its natural, safer course and undermines public and private information and infrastructure-security investment decisions. Careless liability waivers can undermine crucial private incentives to innovate in security.

Online security is an immensely valuable and important industry unto itself. We need better digital equivalents of barbed wire and door locks - which private companies are constantly competing to improve - not just cybergovernmental "police and tanks," so to speak. Vastly expanding federal oversight is not the same as actually bolstering security. Government must coexist with, rather than crowd out, private-sector security technologies and practices.

The Internet that will evolve if government can resort to a "kill switch" will be vastly different from - and inferior - the safer one that will emerge otherwise.

Here's how to strengthen cybersecurity without centralizing it:

c Emphasize securing government networks: As lead offender in network vulnerabilities, Washington should focus on protecting the government's own networks and setting security standards for its own agencies and, beyond that,

arresting actual computer criminals.

c Stop interfering with privacy and cybersecurity guarantees: In a free society, individuals present different faces t the world in different contexts, but government is disdainful of the sanctity of individual privacy. Too often, firms want to make ironclad privacy and security guarantees but cannot do so on account of lax protections against governmental access to sensitive data that the market otherwise would protect. Examples include coercive data-retention mandates, national identification schemes and warrantless Internet surveillance.

Story Continues →

‹‹ previous12next ››