

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee -
Subcommittee on Crime & Terrorism:
Cyber Security: Responding to the Threat of Cyber Crime & Terrorism
April 12, 2011

Question To Entire Panel II:

As you know, there are multiple Senate Committees that are exploring how best to proceed on cyber security policy. I've been following this issue very closely and would appreciate learning your views on some the legislative proposal that are pending? What are some of the issues we should avoid and others we should embrace?

Stewart Baker Response:

In general, I believe that the Collins-Lieberman approach to regulation is the best compromise between laissez-faire and traditional regulation. That approach would allow DHS to challenge the private sector to come up with its own plans, but would reserve for DHS the right to demand more in response to particular threats (or a failure of responsibility by the sector in question).

I would also like to raise one other legislative proposal that raises cybersecurity concerns and falls squarely within Judiciary's jurisdiction. James Baker of the Justice Department recently testified to the Senate Judiciary Committee about ECPA reform, and in the process he touched on the provision of ECPA that prohibits ISPs from sharing subscriber data with the government in the absence of a court order. Mr. Baker hinted that this provision should perhaps be expanded to restrict ISPs from sharing subscriber data with third parties, at least where a commercial purpose is present:

A sixth potentially appropriate topic for legislation is the disclosure by service providers of customer information for commercial purposes. Under § 2702(c)(6) of ECPA, there are currently no explicit restrictions on a provider disclosing non-content information pertaining to a customer or subscriber "to any person other than a government entity." This approach may be insufficiently protective of customer privacy. Congress could consider whether this rule strikes the appropriate balance between providers and customers.

http://www.wired.com/images_blogs/threatlevel/2011/04/bakerepca.pdf

This strikes me as a dangerous step from the point of view of cybersecurity. Let me give one example. In a distributed denial of service attack, infected consumer machines are instructed to send packets to a victim site, which is then overwhelmed by malicious traffic. An ISP can often tell which of their customers' machines have been infected just by looking at the nature of the signals the machines are sending. If the ISP passes that information on to the victim site, the victim site or its service provider can shunt aside or drop signals from the infected computers as part of the target's defenses. This is just one of many ways in which it may be important for cybersecurity reasons to have quick, unimpeded sharing of information about subscribers who are engaged in activities that endanger others on the Internet.

Mr. Baker's casual proposal to extend the ECPA bar on disclosure would discourage such defensive moves. Before giving weight to Mr. Baker's views, Judiciary Committee should demand a formal, cleared legislative proposal from the administration, and it should look carefully at the security consequences before taking action on any such proposal.