

# THE FINANCIAL SERVICES ROUNDTABLE

*Impacting Policy. Impacting People.*



1001 PENNSYLVANIA AVE., NW  
SUITE 500 SOUTH  
WASHINGTON, DC 20004  
TEL 202-289-4322  
FAX 202-628-2507

E-Mail [info@fsround.org](mailto:info@fsround.org)  
[www.fsround.org](http://www.fsround.org)

March 5, 2007

The Honorable Mary Bono  
U.S. House of Representatives  
Washington, DC 20515

Dear Congresswoman Bono:

I am writing to provide comments to you on H.R. 964, the SPY Act. We appreciate your work on this issue.

Spyware is a problem that affects us all – both at home and at work – and one which undermines the utility of the internet as a platform for conducting legitimate business. Legislation that will help enforcement agencies identify and prosecute bad actors would be welcomed by every individual consumer and business that uses a computer. At the same time, legislation that restricts the legitimate needs of online commerce such as the way businesses identify customers who are visiting their websites, or that could hamper the ability of a financial services company to effect, enforce or administer a customer's requested transaction, could do irreparable harm. Legislation must be appropriately balanced to ensure that only bad actors are ensnared. It is difficult to imagine that a statute dealing with such complex technological issues could long stay ahead of advances in technology. As it is currently drafted, we are concerned that H.R. 964 could have a negative impact on legitimate businesses.

While section 2 does an excellent job of defining illegal spyware, it does not and cannot contemplate all future advances in technology. For example, there is no exception for employers who are monitoring activity on a company network. Under current business models, our members may own the computers that their employees or agents use and not allow vendors to attach non-company equipment to their network. Some, however, could consider changing business models so that employees, agents or vendors could attach non-company equipment to the network, and do not wish to rule out that advances in technology could make this a viable option in the future. If the bill is passed, as written, companies could not take action to monitor the activities of employees, agents or vendors connected to their network on non-company owned computers or devices which could open companies up to additional liabilities and security threats based on activities of employees, agents or vendors. Section 5 does contain an exemption for security related activities, but it is limited as to who can take advantage of the exemption and does not cover employers. In addition, section 5 fails to address other legitimate activities including those designed to authenticate customers.


Section 3 imposes a consent regime on top of the prohibited activities and their exceptions, but we do not believe that a consent regime is necessary. No information is being furnished by the customer, and actions taken to "steal" information are clearly prohibited and subject to penalties and damages. In this instance, a consent regime will, at best, inconvenience customers, and at worst, sanction non-defined pernicious activities such as "gating." It should not be the result of spyware legislation to create a regime where individuals could "opt-in" to spyware.

In terms of enforcement, I have strong concerns with the inclusion of the “good Samaritan” provision which, in essence, exempts from liability the removal of legitimate software by third-party service providers. This provision, coupled with the limitations on liability in section 3(e), places the online relationships of financial firms and their customers in the hands of service providers without redress should the service provider inadvertently or affirmatively take action that corrupts the relationship.

Over the last several years, the financial services industry has invested a great deal in technology meant to close the digital divide and provide those who seek it the convenience of an “online” relationship. In Gramm-Leach-Bliley, E-SIGN, CAN- SPAM, and Fair and Accurate Transactions Act, Congress and the financial regulators defined how companies must protect personally identifiable information online and provide customers with notice and choice by offering them an opportunity to opt-out. H.R. 964 would go beyond all of these other acts of Congress to require an opt-in. However, in this instance, there is no need to provide customers the ability to provide affirmative consent for practices that Congress intends to prohibit.

We continue to prefer an approach more narrowly tailored to address bad practices and to punish those who engage in prohibited activities. Such an approach will help ensure that the internet remains a viable conduit to conduct business.

Best regards,

A handwritten signature in blue ink that reads "Steve". The signature is written in a cursive style and is underlined with a single horizontal stroke.

Steve Bartlett  
President and CEO

Cc: The Honorable Joe Barton