

H.R. 964 - Securely Protect Yourself Against Cyber Trespass Act

Floor Situation

H.R. 964 is being considered on the floor under suspension of the rules and will require a two-thirds majority vote for passage. This legislation was introduced by Representative Edolphus Towns (D-NY) on February 8, 2007. The bill was ordered to be reported from the Committee on Energy and Commerce, by voice vote, on May 10, 2007.

H.R. 964 is expected to be considered on the floor on June 6, 2007 with an amendment.

**Note: During the 109th Congress, Rep. Mary Bono (R-CA) introduced identical legislation, H.R. 29, which passed the House of Representatives by a recorded vote of 393-4 ([Roll no. 201](#)). The Senate received the bill, but took no further action.*

Summary

The SPY ACT takes steps to protect consumer computers from unwanted and unauthorized “spying” from spyware software. Spyware tracks a computer user’s keystrokes, web site history, and even steals protected passwords, and then this information is passed onto a third party.

Section 2 – Prohibition of Unfair or Deceptive Acts or Practices Relating to Spyware

H.R. 964 makes it unlawful for any person who is not the owner or authorized user of a protected computer to engage in deceptive acts or practices in connection with specified conduct. Specifically the bill prohibits:

- Taking control of the computer;
- Modifying settings related to use of the computer or to the computer's access to or use of the Internet by altering certain information;
- Collecting personally identifiable information through the use of a keystroke logging function;
- Inducing the owner or authorized user of the computer to disclose personally identifiable information by means of a Web page;
- Inducing the owner or authorized user to install a component of computer software onto the computer, or preventing reasonable efforts to block the installation or execution of, or to disable, a component of computer software;

- Misrepresenting that installing a separate component of computer software or providing log-in and password information is necessary for security or privacy reasons, or that installing a separate component of computer software is necessary to open, view, or play a particular type of content;
- Inducing the owner or authorized user to install or execute computer software by misrepresenting the identity or authority of the person or entity providing the computer software to the owner or user;
- Inducing the owner or authorized user to provide personally identifiable, password, or account information to another person;
- Removing, disabling, or rendering inoperative any security, anti-spyware, or anti-virus technology installed on the computer; and,
- Installing or executing on the computer one or more additional components of computer software with the intent to cause a person to use such components in a way that violates any other provision of this section.

Section 3 – Prohibition of Collection of Certain Information without Notice and Consent

The bill prohibits the transmission of an information collection program to a protected computer. This prohibition can be waived if the program provides a waiver for its application before the first use of the information collection program. This waiver is only required during the first use unless the information collected is “materially different” from the program’s initial purposes.

**Note: Information collection program is defined as: “computer software that performs either of the following functions:*

- *Collects personally identifiable information; and,*
 - *Sends such information to a person other than the owner or authorized user of the computer, or,*
 - *Uses such information to deliver advertising to, or display advertising on, the computer;*
- *Collects information regarding the user's Internet activity using the computer; and,*
- *Uses such information to deliver advertising to, or display advertising on, the computer.”*
- *Exception from definition for software that collects information regarding Internet activity within a particular web site if:*

- *The only information collected is information regarding the web pages access within a particular web site or the information is user supplied search terms necessary to complete a search;*
- *And the information is not sent to a person other than the web site accessed or a party authorized and the advertising is confined to that website.*
- *FTC study and additional exemption – study of applicability of consumer notice and consent regarding information collection for information input directly by users in a field provided by a website. The FTC may exempt such notice requirements if it finds users have adequate notice.*

Section 4 - Enforcement

This legislation requires the Federal Trade Commission (FTC) to enforce the Act under the Federal Trade Commission Act. The FTC may seek civil penalties for violations of this Act in 1 of 2 ways: 1) it may seek civil penalties of up to \$11,000 for each violation or 2) the FTC, in the case of a person who engages in a pattern or practice that violates sections 2 and 3 of this bill, may seek a civil penalty of \$3 million for each violation of Section 2 and \$1 million for each violation of Section 3.

The FTC or a court must determine that the action was committed with actual knowledge or knowingly fairly implied on the basis of objective circumstances that such act is unfair or deceptive or violates this Act to seek civil penalties.

Section 5 – Limitations

These provisions do not apply to:

- Any act taken by a law enforcement agent in the performance of official duties; or,
- The transmission or execution of an information collection program in compliance with a law enforcement, investigatory, national security, or regulatory agency or department of the United States or any State in response to a request or demand made under authority granted to that agency or department, including a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a court order, or other lawful process.

Nothing in this bill shall apply to any monitoring of, or interaction with, a protected computer to the extent that such monitoring or interaction is for the purpose of network security, computer security, diagnostics, technical support or repair, network management, authorized updates of software, or for the detection or prevention of fraudulent activities.

If a provider of computer software or interactive computer services attempts, in good faith, to remove or disable a program that violates this Act, that provider may not be held liable.

Section 7 – Report on Cookies

The FTC must file a report to Congress on the extent to which cookies are or may be used to transmit to a third party personally identifiable information of a computer owner or user, information regarding Web pages accessed by the owner or user, or information regarding advertisements previously delivered to a computer.

Section 8 – FTC Report on Information Collection Programs Installed Before Effective Date

H.R. 964 requires the FTC to report to Congress on the extent to which there are installed on protected computers information collection programs that are not covered by the notice and consent requirements of Section 3 because such programs were installed prior to the effective date of this Act.

Section 11 – Applicability and Sunset

This Act will take effect 12 months after the date of enactment and will sunset on December 31, 2013.

Background

The FTC defines spyware as software “that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer’s consent, or asserts control over a computer without the consumer’s knowledge.”

Spyware can be used to obtain personal information such as passwords to bank accounts, and it can record internet site history for targeted advertisements. The spyware collects this information and then transmits it to a remote user.

Unauthorized access to a computer is illegal under computer crime laws, such as the Computer Fraud and Abuse Act, which was signed into law in 1986. The PATRIOT Act increased the scope of computer laws in the United States.

On May 22, 2007, the House of Representatives passed the Internet Spyware (I-SPY) Prevention Act of 2007 (H.R. 1525), by a voice vote. For more information on H.R. 1525, please review the [Legislative Digest for H.R. 1525](#).

Cost

“CBO estimates that implementing the bill would increase spending by \$1 million in 2008 and \$7 million over the 2008-2012 period, assuming appropriation of the necessary amounts.” [Congressional Budget Office Cost Estimate](#)

Staff Contact

For questions or further information contact Chris Vieson at (202) 226-2302.