

FINAL BILL REPORT

SHB 2879

C 66 L 08

Synopsis as Enacted

Brief Description: Modifying provisions regulating spyware.

Sponsors: By House Committee on Technology, Energy & Communications (originally sponsored by Representatives Morris, Ericksen, Hasegawa, Morrell and Kelley; by request of Attorney General).

House Committee on Technology, Energy & Communications
Senate Committee on Consumer Protection & Housing

Background:

Spyware. The term "spyware" generally describes any software that is placed on a user's computer to monitor, collect, and transmit personally identifiable information without the user's knowledge or consent. Spyware programs can be difficult to identify and remove, and they can cause problems ranging from advertisements to computer viruses to identity theft. Frequently, spyware is hidden within a larger software package that the consumer purposely installs, but spyware also can be installed by visiting a web site.

Computer Spyware Law. In 2005 a state spyware law was enacted. The law generally prohibits the unauthorized installation of computer spyware if installed through intentionally deceptive means. Several types of computer spyware activities are prohibited, including collecting web browsing histories, taking control of a user's computer to send electronic mail or viruses, creating bogus financial charges, opening multiple pop-up advertisements, and modifying security settings.

The Attorney General, a provider of computer software, or an owner of a Website or trademark may bring a civil action to enjoin further violations and recover either actual damages or \$100,000 per violation, whichever is greater. The maximum allowable damage award is \$2 million. In addition, a court may increase the damage award up to three times if the defendant has engaged in a pattern and practice of engaging in the prohibited activities. The court may also award costs and reasonable attorneys' fees to the prevailing party.

Summary:

Additions to the Computer Spyware Law. Several computer-related actions, collectively known as "spyware," are added to the computer spyware law. The following spyware activities are prohibited:

- disabling the ability of anti-spyware or anti-virus software to update automatically, if the disabling is done through intentionally deceptive means;

- using the owner or operator's computer as part of an activity performed by a group of computers for the purpose of causing damage to another computer or person, including, but not limited to, launching a denial of service attack;
- transmitting or relaying commercial e-mail or a computer virus from the owner or operator's computer if initiated by a person other than the owner or operator;
- modifying toolbars or buttons of the owner or operator's Internet browser used to access and navigate the Internet, if the disabling is done through deceptive means; and
- inducing an owner to install software by displaying a pop-up, web page, or other message whose source is misrepresented.

These prohibitions also apply to those persons who know or consciously avoid knowing that their services are being used to procure or transmit spyware.

Exceptions. These prohibitions do not apply to any monitoring of a subscriber's Internet service by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service for network or computer security purposes.

Changes to the Computer Spyware Law. The following computer spyware provisions are modified to prohibit "deceptive" actions rather than "intentionally deceptive" actions:

- modifying settings for opening web pages, search engines, bookmarks, and toolbars;
- misrepresenting that software will be uninstalled or disabled by an owner or operator's actions; and
- misrepresenting that software is necessary for security, maintenance, repair, or privacy reasons.

"Deceptive" is defined as: (1) a materially false or fraudulent statement; or (2) a statement or description that omits or misrepresents material information in order to deceive an owner or operator.

Some provisions of the existing computer spyware law are removed relating to: (1) keystroke logging; and (2) preventing an owner from disabling or blocking the installation of software.

These exemptions must not be construed as: (1) a defense to liability under the common law or any other state or federal law; or (2) an affirmative grant of authority to engage in certain computer monitoring or remote disablement activities.

Standing to Sue. A provider of computer software or owner of a Website or trademark may bring a civil action only if the action arises directly out of the person's status as a provider or owner.

The computer spyware statute is reorganized.

Votes on Final Passage:

House	95	0
Senate	49	0

Effective: June 12, 2008