



WASHINGTON STATE ATTORNEY GENERAL
ROB MCKENNA
AG REQUEST LEGISLATION - 2008 SESSION

PROTECTING CONSUMERS FROM SPYWARE

THE PROBLEM

Washington's Computer Spyware Statute, RCW 19.270, has several loopholes and weaknesses. These include an intent requirement for certain violations that burdens enforcement authorities, murkiness in some of the definitions of unlawful practices, a lack of enforcement authority against those who knowingly facilitate or procure the sending of spyware, and the absence of language in the statute prohibiting deceptive conduct that has emerged since the statute was originally passed.

BACKGROUND

- Washington's Computer Spyware Statute, RCW 19.270, was approved by the Legislature in 2005. Washington was one of the first states in the country to pass legislation to help stop this widespread consumer problem.
- Among other things, the law makes it illegal to install software that would take control of a consumer's computer, modify its security settings, collect the user's personal identification information, interfere with its own removal, disable antispyware programs or falsely entice someone to download software by claiming it is necessary for security or privacy.
- Since the law was enacted, the Attorney General's Office has brought five lawsuits under the act.
- The existing spyware statute states that a spyware sender's actions must be intentionally deceptive for a violation of the law to occur. In some instances, this burden of proof restricts the ability of the Attorney General's Office and others who file lawsuits against spyware senders to take effective action. Proving intent makes enforcement cumbersome, and can give violators of the law a loophole for avoiding liability.
- The existing statute needs to be updated to adequately address new types of deceptive behaviors and third-parties such as Web hosting companies and merchants that permit others to send spyware.

PROTECTING CONSUMERS FROM SPYWARE

The Attorney General's Office has requested legislation to remedy loopholes and weaknesses in the state's Computer Spyware Statute. The proposed legislation would do the following:

Remove the following requirements:

- parties who bring actions under the act must prove defendants "intended to deceive" for any of the following violations to have occurred:
 - unauthorized modification of computer settings (i.e. settings for opening pages, search engines, bookmarks and toolbars);
 - misrepresentation that computer software will be uninstalled or disabled by an owner's action;
 - misrepresentation that software is necessary for security, maintenance, repair or privacy reasons;
- "all" keystrokes must be logged in order to prove a violation, or that the information obtained through keystroke-logging be correlated with the Web sites visited by the owner or operator; and
- in order to prove a violation based on preventing a computer owner or operator from disabling or blocking the installation of software, the software must be automatically reinstalled after the attempt to block or disable it.

Create liability for:

- Web-hosting companies who know or consciously avoid knowing their services are being used to violate the statute, and who participate or ratify the unlawful activities; and
- those who procure the transmission of spyware (i.e. merchants who pay others to send spyware on their behalf).

Add violations for:

- disabling a computer software program's ability to automatically update;
- changing the toolbars or buttons on an Internet browser;
- using the computer as part of a bonnet;
- using the computer as a proxy to send commercial email or a computer virus; and
- inducing an owner to install software by sending a message whose source is misrepresented.

Clarify:

- the standards for proof of violations by collapsing two current sections of the statute into one provision; and
- the circumstances a software provider, trademark owner and Web site owners may bring an action.