Legal Opinion Letter

WLF Washington Legal Foundation

Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

Vol. 16 No. 23 August 18, 2006

WASHINGTON SPYWARE LAW ADDRESSES SERIOUS ONLINE COMMERCE THREAT

by
Attorney General Rob McKenna

Spyware has become arguably the biggest online threat to consumers and businesses since the advent of the Internet. Last year, Washington became one of the first states to adopt a law explicitly prohibiting spyware activities and imposing serious penalties on violators. The Washington Computer Spyware Act, Chapter 19.270 RCW (http://leg.wa.gov), gives the Attorney General's Office and businesses in our state a strong tool to discourage and prosecute spyware purveyors. It also penalizes those who attempt to deceive consumers into downloading software under the guise that the program is needed to protect themselves and their computers. The Attorney General's Office filed its first suit under the new statute earlier this year. Microsoft has also taken action since the law took effect on July 24, 2005.

Spyware: A Growing Threat. Broadly speaking, spyware is deceptive software that is installed on a computer, often without the user's knowledge or informed consent. Such software can collect and transmit personal information, change important privacy and security settings, and even take over the user's computer.

Twelve states now have laws that specifically address spyware. The need for such legislation is evidenced by staggering statistics, including industry reports that estimate spyware and other unwanted software reside on up to 80 percent of consumers' computers.[1] One study[2] by software providers found an average of 25 spyware programs per PC.

Most consumers are unclear how spyware ends up on their computers, but it can happen by simply downloading a program offered for free, such as a screensaver or an mp3 music file. Because spyware is frequently installed surreptitiously, frustrated consumers may not immediately attribute computer malfunctions to spyware. Some assume that hardware or software glitches are the "cost of doing business" and never seek to clean their computers of the harmful software. Depending on the situation, spyware can range from being merely a nuisance – causing unwanted pop-up ads or slow performance – to being a serious threat to online security and privacy that creates the potential for identity theft. Webroot Software recently reported that its employees uncovered a stash of tens of thousands of stolen identities from 125 countries apparently collected by a new variant of a Trojan horse. INFOWORLD, May 9, 2006.

Businesses are becoming plagued with compromised company security, overloaded networks, and significant user downtime. Earlier this year, Japanese police arrested an alleged spyware developer who, along with another suspect, is accused of stealing online banking passwords later used to withdraw money from ten company accounts.

As concerns about computer safety grow, consumer confidence in e-commerce and online financial transactions may be undermined. One effective way to keep the Internet market thriving is for the Attorney

[1]Separate 2004 studies by market researcher IDC and the National Cyber Security Alliance.
[2]Earthlink and Webroot Software's SpyAudit report released February 2005. http://www.earthlink.net/spyaudit/press/.

Rob McKenna is Attorney General of the State of Washington.

General's Office to approach high-tech cases as it does the "bricks-and-mortar world" and bring our law enforcement powers to bear when appropriate.

Washington's Spyware Act. Washington's Spyware Act prohibits collecting personally identifiable information through keystroke logging; collecting Web browsing histories; taking control of a user's computer to send unauthorized e-mail or viruses; creating bogus financial charges; orchestrating group attacks on other computers; opening aggressive pop-up advertisements; modifying security settings; and interfering with a user's ability to identify and remove the spyware. Our law doesn't stop at outlawing software programs that meet the traditional definition of "spyware," but also punishes those who seek to profit from computer users' fear of spyware by making false representations to induce users to install software. Our first lawsuit targeted individuals who exploited consumers' anxieties for financial benefit.

The Attorney General's Office – or any owner of a Web site or trademark who is adversely affected by spyware violations – may bring an action under our law. Defendants can be fined up to $100,000 per violation or actual damages, whichever is greater – and a court may increase damages threefold for repeat offenders up to a maximum of $2 million. A violation of the spyware act is also a violation of the state Consumer Protection Act, under which offenders may be subject to a civil penalty of up to $2,000 per violation.

While the new spyware law offers many benefits to state prosecutors, it also presents new challenges. In order to trigger penalties, the state must prove intent to deceive on the part of the companies installing the spyware. This criteria places a higher burden of proof on plaintiffs. It requires our attorneys to take a different approach with spyware investigations and to consider factors that historically have not been at issue in cases filed exclusively under the Consumer Protection Act.

State's First Spyware Case. The Attorney General's Office filed its first lawsuit under the Spyware Act in January in U.S. District Court in Seattle following a five-month investigation by the office's Consumer Protection High-Tech Unit. *State of Washington v. Secure Computer LLC et al.*, No. 006-0126. (U.S. District Court Western District of Washington). Our suit also alleges violations under the federal Controlling the Assault of Non-Solicited Pornography and Marketing Act a.k.a. "CAN-SPAM," the state Commercial Electronic Mail Act and the state Consumer Protection Act. We announced our case jointly with Microsoft, which has also filed charges against defendants named in our suit.

We accused New York-based Secure Computer LLC and associates of marketing software that falsely claimed computers were infected with spyware, then enticing consumers to pay for a program that claimed to remove it. Secure Computer advertised its Spyware Cleaner program in various ways, including spam and pop-up ads that displayed warnings that a consumer's personal computer "may be infected with harmful spyware" and offered a "free scan" of the computer. If a user elected to have the free scan performed, a software program downloaded, installed, and immediately executed on the user's computer. Our investigation found that this so-called "free scan" always detected spyware on a user's computer, even if none existed. In order to remove this falsely detected spyware, users were instructed to purchase the full software product.

Yet, when tested on a computer that was deliberately infected with spyware, the state's investigation showed Spyware Cleaner detected virtually none of the actual spyware on the computer. The software also erased a computer's Hosts file, which can be used to store Web addresses that a user wants to block.

To date, three defendants have settled. One admitted violating Washington's Computer Spyware Act and Consumer Protection Act as part of a stipulated judgment reached in April. He will pay nearly $84,000 in fines and consumer restitution. A second settled through a consent decree in May and will pay $7,200 in legal costs and attorneys' fees. A third settled through a consent decree in June and will pay $2,000 in legal costs and attorneys' fees. I'm proud of the work of our High-Tech Unit, which is probing other potential spyware targets while continuing to focus its efforts on Secure Computer.

Copyright 2006 Washington Legal Foundation

ISBN 1056 3059