Spyware Enforcement

April 29, 2008
Tags: Array

Supporting Documents

By now most computer users have become familiar with the term "spyware," largely because they or someone they know have experienced it first-hand. Computer users are increasingly finding programs on their computers that they did not know were installed and that they cannot uninstall, that create privacy problems and open security holes, that can hurt the performance and stability of their systems and that can lead them to mistakenly believe that these problems are the fault of their hardware or Internet provider. One vital component of the response to this menace has been the use of new and existing laws to prosecute spyware distributors.

In March 2004, CDT President Jerry Berman testified about spyware before the Senate Commerce Committee, highlighting the fact that several existing federal laws - Section 5 of the Federal Trade Commission Act, the Electronic Communications Privacy Act (ECPA), and the Computer Fraud and Abuse Act (CFAA) - could be used to target the tactics of malicious spyware distributors. He urged the Congress to provide law enforcement officials with the necessary resources to use these laws in prosecuting spyware offenses. He also noted that many states had long-standing fraud statutes that could be brought to bear on spyware distributors, and that neither the federal nor the state laws had yet been used to take action in the spyware space.

Since then, law enforcement officials have increasingly applied statutes - some long-standing, some relatively new - to spyware cases. Leading the charge has been the FTC, which to date has brought 11 cases under its unfair and deceptive practices authority. The Department of Justice has actively pursued spyware purveyors under the CFAA and the Wiretap Act, with 11 cases to date. And several attorneys general at the state level have filed spyware lawsuits under state fraud and consumer protection laws, with a few cases initiated under new state spyware statutes.

The states are in a unique position to make a great impact in the broader spyware fight. With a relatively small investment in consumer outreach and technical training, states can contribute towards broadening and diversifying the pool of law enforcement officials who are actively combating the spyware problem. CDT encourages more states to join in by taking the following steps:

1. Establish consumer complaint Web sites where computer users can submit complaints about suspected spyware.
2. Establish or support computer forensic capabilities so that consumer protection enforcement agencies can investigate and verify complaints of spyware and trace responsibility.
3. Train investigators and prosecutors in identifying the attributes of spyware that violate existing laws.

Law enforcement is one important tool that can be used to pursue spyware purveyors, but for consumers seeking quick relief from spyware infections, anti-spyware technology is their most essential resource. Consumers can use anti-spyware programs to block software that they do not want, whether or not that software is considered illegal under today's standards. More information on anti-spyware technologies can be found at the Anti-Spyware Coalition Web site [1].

Because spyware is a moving target, it requires attention from a multitude of sectors, from litigators and legislators to technologists and consumer advocates. The following charts serve to summarize

the spyware behaviors that law enforcement officials have targeted in their recent cases. The charts describe companies and individuals whose behaviors are or once were (a) consistent with the Anti-Spyware Coalition definition of "Spyware (and Other Potentially Unwanted Technologies)," [2] and (b) alleged to be illegal by law enforcement. By highlighting specific practices that have already been determined to be illegal, CDT hopes to provide a tool for future spyware prosecutors, consumer protection agencies, and legislators, as well as for software developers looking to avoid behaviors that could cause their software to be classified as spyware.

- Federal Trade Commission Spyware Case Summary [3]
- State Spyware Case Summary [4]
- Federal Spyware Case Summary [5]

For further information

Contact:

- Alissa Cooper (202) 637-9800 x110.
- Ari Schwartz (202) 637-9800 x107.

-
- spyware
- FTC
- asc
- anti-spyware coalition

Links:
[1] http://www.antispywarecoalition.org
[2] http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm
[3] http://cdt.org/privacy/spyware/ftc-enforcement.php
[4] http://cdt.org/privacy/spyware/state-enforcement.php
[5] http://cdt.org/privacy/spyware/federal-enforcement.php