NASCIO Representing Chief Information Officers of the States

Issue Brief

Jan. 2005

The Real Phantom Menace: Spyware and its State Implications

The Low-Down on Spyware: The use of spyware has matured into a major security threat that is transmitted via Internet connections. It can compromise the security of government computer systems and the privacy of personal information, while draining state time and resources in order to properly avert the threat. While California and Utah have enacted legislation addressing spyware and five other states have introduced similar legislation,[1] legislation may not be sufficient to curtail spyware's impact. **States may consider implementing technical anti-spyware solutions and examining whether existing computer trespass and fraud laws would encompass the use of spyware.** While last year's federal anti-spyware legislation did not pass, existing federal laws, such as ECPA (Electronic Communications Privacy Act), CFAA (Computer Fraud and Abuse Act) and the Federal Trade Commission Act, might include spyware threats.

What Is It? Spyware is a generic class of software security threats. It includes key-logger technology, adware, malware, and homepage hijacking and can be installed while a user is connected to the Internet. **The hallmark of spyware is its installation on a user's computer without his or her knowledge, consent or permission.** It has even been known to disguise itself as free anti-spyware software that installs spyware on computers. Spyware is deliberately used for a variety of purposes, including for market research by tracking online behavior and browsing and to steal a user's personal information that can later be used for identity theft and related activities. **The danger of spyware is that it can track a user's online activities, steal a user's personal information from his or her computer, track each and every one of a user's key strokes (including the entry of credit card numbers, Social Security Numbers, and user IDs and passwords), hijack homepages and sometimes substitute them with unacceptable webpages, create an endless stream of pop-up ads, change computer settings, drastically slow infected computers, and result in hard drive corruption.**

Spyware is a real and pervasive threat. Based on a recent study, four out of five surveyed computer users had spyware or adware installed on their computers.[2] It may be a greater threat for broadband connections (as opposed to dial-up) because of its "always on" connection and lack of preventative measures.

What Are The Intended Consequences of Spyware?

It's the Purpose that Counts: Concerns arise from spyware's use for malicious purposes and not from the underlying technology itself.

---

[1] "2004 Legislation Relating to Internet Spyware or Adware," National Conference of State Legislatures (NCSL), <http://www.ncsl.org/programs/lis/spyware04.htm>. Iowa, Michigan, New York, Pennsylvania, and Virginia introduced anti-spyware legislation during 2004.

[2] AOL/National Cyber Security Alliance (NCSA), "Largest In-Home Study of Home Computer Users Shows Major Online Threats, Perception Gap," October 2004, <http://www.staysafeonline.info/news/NCSA-AOLIn-HomeStudyRelease.pdf>.

167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Security Implications: Spyware can be installed on government computer systems in order to gain access to those computer systems. While the installation of spyware can originate from the Internet, it also can be surreptitiously installed by an insider to a government organization to gain unauthorized access to computer systems and information. Finally, spyware can track government computer users' IDs and passwords. Recognizing these and other threats, state CIOs are taking technical and other measures to guard against spyware's security implications.

Privacy Implications: Spyware also can compromise the privacy of a computer user's personal information, such as credit card numbers and Social Security Numbers, by harvesting that information from the user's computer. Key-logger technology that may be embedded within spyware also can track a user's every key stroke, which may include the entry of personal information. Information harvested via spyware applications can later be used to commit identity theft and for a variety of other illegal purposes.

Citizen Trust & Internet Use Implications: As citizens move online only to discover the threats posed by spyware, such as sluggish computer performance, hard drive corruption and even identity theft, citizens are becoming more sensitive to the threats[3] and may choose to move offline. Such an offline migration could result in a decreased user base for e-government applications and could even substantially decrease the benefits of e-government, which can include cost reductions and 24x7 service offerings to citizens.

Business & Cost Implications: Spyware can diminish the productivity of government organizations by slowing the speed of computers, particularly where multiple spyware programs have been installed. Moreover, to protect against spyware and other IT security threats, states have been forced to expend millions of taxpayer dollars that could have been used for other purposes, such as for the delivery of government service programs.

Unintended Consequences for Legitimate Software: An unintended consequence of spyware's proliferation is that it can result in the unfair targeting of beneficial types of legitimate software, such as supportware and certain classes of adware. Supportware can be used to deliver security services or support Internet access, and legitimate types of adware can provide users with free or low-cost software in exchange for the user's agreement to be exposed to advertisements. However, users of those types of adware may be asked to provide personal information to the advertiser as part of the bargain. Such legitimate types of adware can be distinguished from more malevolent classes of adware by the fact that, with legitimate adware, the user consents to the advertising.

Will New Laws Help?

Federal Legislation: During the 108th Congress, Rep. Mary Bono introduced the Spy Act (Securely Protect Yourself Against Cyber Trespass Act) to protect Internet users from the unknowing transmission of their personal information through spyware programs.[4] The bill did not become law, since it was not passed by the Senate. However, on January 4, 2005, Rep. Bono re-introduced an amended version of the bill for consideration during the current 109th Congress. To be effective, federal anti-spyware legislation needs to be broad enough to encompass the different iterations of spyware, while being narrow enough not to penalize legitimate technologies. Finally,

[3] According to a Pew Internet & American Life Project report, 84% of Internet users are concerned about businesses or people they do not know obtaining their or their families' personal information. For more information, see "Trust & Privacy Online: Why Americans Want to Rewrite the Rules," August 2000, <http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf>.

[4] HR 2929, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2929rds.txt.pdf>.

the questionable success of the CAN-SPAM Act's enforcement[5] points out the fact that enforcement of anti-spyware legislation would need to be swift and severe in order to ensure its effectiveness.

State Legislation: California and Utah have enacted anti-spyware legislation. However, such legislation may have a limited impact. For example, a patchwork of state anti-spyware laws may not have the overall effect of deterring and catching spyware users and may be logistically difficult to enforce against the potentially many offenders located outside of a state's borders. There have also been some concerns about whether some anti-spyware laws are so broad that they could apply to supportware or other types of legitimate technologies. Given the amorphous nature of spyware, the legislative or regulatory approach to remedying spyware threats is problematic.

What Are The Potential Solutions?

Technical Solutions: Attack prevention appears to be the current focus of anti-spyware efforts and technical solutions seem to be the most viable way to counter the threat of spyware at the present time. More than a dozen solutions are on the market. However, the effectiveness of technical solutions may be limited to domestic spyware companies and likely will have negligible success in discouraging spyware firms operating in foreign countries. **Nevertheless, states should invest in a technology solution to have an immediate impact against spyware applications. Anti-spyware solutions may be embedded within existing applications, but also are available as stand-alone solutions.** A state should consider which type of solution is the most appropriate for its architectural direction. However, to ensure the consistency of anti-spyware measures across agencies, state CIOs may consider the implementation of enterprise-class solutions with regular automatic definition updates and a high degree of key-logger removal. The cost of anti-spyware solutions can be as high as $39.00 for a single user license but as low as $1.00 per seat for volume installations.

Application of Existing State Laws to Spyware Purveyors: States may consider whether currently existing computer trespass or unauthorized computer access laws that are typically classified as offenses against property might encompass instances of the installation or attempted installation of spyware. For example, Kentucky's computer trespass law would likely cover such instances. It criminalizes the knowing or willful access or attempted access of computer systems, data, networks, programs or software without the owner's consent. If the computer access results in damage in the amount of $300 or more or if the access or attempted access is intended to defraud or obtain money, property (which might include computer hard drive space), or services under false or fraudulent pretenses, then the violation is a felony.[6] The State of Indiana has a similar computer trespass statute.[7] Virginia's Joint Commission on Technology and Science (JCOTS) also is examining how existing state computer crimes laws may be amended to address spyware and other IT security threats.[8] However, such laws may have a limited impact where the user has affirmatively agreed with a click of a mouse to the spyware's terms and conditions.

---

[5] Only 9% of email is compliant with federal anti-spam legislation. See "Commtouch Reports Spam Trends for First Half of 2004: Viagra is King of Spam, 5 Countries are Hosting 99.68% of Spammer Websites, and Nearly 10% of All Spam is CAN-SPAM Compliant," Commtouch Press Release, June 30, 2004, <http://www.commtouch.com/news/english/2004/pr_04063001.shtml>.

[6] Kentucky Revised Statutes, 434.840-860, "Unlawful Access to a Computer," <http://www.lrc.state.ky.us/KRS/434-00/CHAPTER.HTM>

[7] Indiana Code, 35-43-2-3, "Computer Trespass," <http://www.in.gov/legislative/ic/code/title35/ar43/ch2.html>.

[8] For more information about JCOTS, please see its website at <http://jcots.state.va.us/About/about.htm>.

167 West Main St., Suite 600 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrinc.net · http://www.nascio.org

Expanded Awareness & Education: State CIOs need to ensure that state policies inform users as well as citizens of the impact of spyware and how to protect against it. For example, many people may assume that a firewall coupled with anti-virus protection will successfully defend against spyware—and that certainly is not the case. The anti-spyware education process should be similar in nature to CIOs' education efforts regarding other threats, such as spam. CIOs should take a lead position on this issue along with other state officials, such as state attorneys general, in order to inform citizens and raise awareness regarding the spyware issue.

Where Can I Find Additional Resources?

Federal Trade Commission (FTC): http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.htm.

Information Technology Association of America (ITAA):
http://www.itaa.org/news/docs/adwarewp.pdf.

National Conference of State Legislatures (NCSL):
http://www.ncsl.org/programs/lis/spyware04.htm.

Consumer Reports Webpage:
http://www.consumerreports.org/main/detailv4.jsp?CONTENT%3C%3Ecnt_id=461187&FOLDER%3C%3Efolder_id=162693&ASSORTMENT%3C%3East_id=333133.

National Institute of Standards and Technology (NIST), Computer Security Resource Center, Spyware Newsletter, January 2004:
http://sbc.nist.gov/cyber-security-tips/jan04.html.

U.S. Computer Emergency Readiness Team (US-CERT) Homepage:
http://www.cert.org

US-CERT, Cyber Security Alerts, Tips and Reading Room:
http://www.us-cert.gov/nav/res01/ntech/.

US-CERT, "Recognizing and Avoiding Spyware," Cyber Security Tip ST04-016 (2004):
http://www.us-cert.gov/cas/tips/ST04-016.html.

167 West Main St., Suite 600 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrinc.net · http://www.nascio.org