Spyware Enforcement

A Report by the Center for Democracy and Technology (CDT)

April 2008 (Updated)

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, http://www.antispywarecoalition.org.

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 chart serves to summarize the spyware and other behaviors that law enforcement officials have targeted in their recent cases. The chart describes charges brought against companies and individuals in cases where one or more of the charged behaviors was (a) consistent with the Anti-Spyware Coalition definition of "Spyware (and Other Potentially Unwanted Technologies)," and (b) alleged to be illegal by federal 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

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
FTC v. Seismic Entertainment Productions, Inc., SmartBot.Net, Inc., and Sanford Wallace Additional defendants: Jared Lansky, John Robert Martinson, OptinTrade, Inc., Mailwiper, Inc., Spy Deleter, Inc. Docket #042-3142	• Installing software onto users' computers that makes substantial modifications to the Internet Explorer Web browser (including the home page and default search engine) without users' knowledge or authorization. • Installing software onto users' computers that in turn creates security holes through which more advertising software and other software is downloaded, all without users' knowledge or authorization. • Inducing users to purchase anti-spyware software products that purport to fix computer problems that the anti-spyware product company itself caused by previously installing software on users' computers without their knowledge or authorization.	Default judgment issued against Wallace and SmartBot.Net:[1] • Ordered to give up over $4 million in ill-gotten gains. • Barred from downloading spyware onto consumers' computers; from downloading any software without consumers' consent; from redirecting consumers' computers to sites other than those the consumers selected to visit; from changing any Web browser's default home page; and from modifying or replacing the search features of any search engine. Settlement reached with Lansky and OptinTrade: • Ordered to give up $227,000 in ill-gotten gains. • Barred from the same practices as Wallace and Smartbot.Net. Seismic Entertainment filed for bankruptcy. Settlement reached with John Robert Martinson and Mailwiper: • Ordered to give up $40,000 in ill-gotten gains with a suspended judgment of $1.86 million. • Barred from the same practices as Wallace and Smartbot.Net http://www.ftc.gov/os/caselist/0423142/0423142.htm

[1] For the settlements listed in the "Status" column of all three charts in this report, defendants admitted no wrongdoing unless otherwise noted.

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
FTC v. MaxTheater, Inc., and Thomas L. Delanoy Docket #042-3213	• Expressly representing or implying that local or remote scans or other examinations of users' computers for spyware had been performed and that spyware had been detected when no such scans or examinations took place and no spyware was detected. • Expressly representing or implying that an anti-spyware product removes all or substantially all spyware on a user's computer when it does not do so.	Settlement reached ordering defendants to give up $76,000 in ill-gotten gains (the full amount of consumer injury). Defendants barred from selling or marketing any anti-spyware product or service in the future; from downloading or installing spyware on consumers' computers, or from assisting others in downloading or installing it; and from making marketing misrepresentations. http://www.ftc.gov/os/caselist/0523059/0523059.htm
FTC v. TrustSoft, Inc. d/b/a Swanksoft and SpyKiller, and Danilo Ladendorf Docket #052-3059	• Expressly representing or implying that remote scans or other examinations of users' computers for spyware had been performed and that spyware had been detected when no such scans or examinations took place and no spyware was detected. • Expressly representing or implying that certain software on a user's computer is spyware (when it is not) after the user downloads and activates an anti-spyware product. • Expressly representing or implying that a spyware removal product removes all, substantially all, or all traces of spyware on a user's computer when it does not do so.	Settlement reached ordering defendants to give up $1.9 million in ill-gotten gains. Settlement bars defendants from making deceptive claims in the sale, marketing, advertising, or promotion of any goods or services and prohibits them from making the specific misrepresentations used in promoting SpyKiller. Defendants barred from using the spyware their "anti-spyware" software supposedly detects and destroys to deliver ads. http://www.ftc.gov/os/caselist/0523059/0523059.htm
In the matter of Advertising.com, Inc. a/d/b/a Teknosurf.com, and John Ferber Docket #042-3196	• Disclosing only within a EULA that software to be downloaded by a user includes adware that collects information about the user (including URLs of visited pages and the user's IP address) and serves a substantial number of pop-up ads to the user.	Final consent order issued prohibiting respondents from making any representations about the performance, benefits, efficacy, or features of its programs promoted as security or privacy software, unless they clearly and conspicuously disclose that consumers who install the program will receive advertisements, if that is the case. http://www.ftc.gov/os/caselist/0423196/0423196.htm

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
FTC v. Odysseus Marketing, Inc, and Walter Rines Docket #042-3205	• Disclosing only within a EULA that software to be downloaded by a user will also cause the installation of additional software that may replace search engine results, collect and transmit information to third parties, deliver pop-up ads, and download more software. • Failing to provide an effective means for users to locate and remove software after it has been downloaded.	Settlement reached ordering defendants to give up $10,000 in ill-gotten gains, with a suspended judgment of $1.75 million. Defendants are also prohibited from producing or distributing software that exploits a security vulnerability, installs without user consent, is overly difficult to uninstall, changes browser settings such as home page, or alters the System32 folder in the Windows operating system. Defendants are further prohibited from gathering personally identifiable information without consumer's consent, selling, or using such information. Finally, defendants are prohibited from making any representation as to the efficacy or performance of software. http://ftc.gov/os/caselist/0423205/0423205.htm
FTC v. Enternet Media, Inc., Conspy & Co., Inc., Lida Rohbani, Nima Hakimi, Baback (Babak) Hakimi, and Nicholas C. Albert Docket #052-3135	• Expressly representing or implying that software functions as an innocuous free program or file (including as a browser upgrade or other security software, or as a music file, song lyric, or ring tone) when the software instead causes a stream of ads to appear on users' computers and/or tracks users' Internet activity. • Providing software that does the following when it is installed[2]: (1) tracks users' Internet activity, (2) changes users' Internet homepage settings, (3) inserts a toolbar onto users' Internet browsers, (4) inserts a large side advertising frame or window onto users' browsers, and (5) displays numerous pop-up ads even when users' browsers are closed. • Furnishing others, including affiliate marketers, with software that substantially interferes with consumers' use	Settlement reached ordering defendants to give up $2.045 million in ill-gotten gains, with a suspended judgment of $8.5 million. Defendants are also enjoined from making false or misleading representations about the nature, performance, features or cost of software code, publishing software that interferes with a consumer's computer use, or helping others to do so. http://www.ftc.gov/os/caselist/0523135/0523135.htm

[2] In CDT's reading of the FTC complaint against Enternet Media, this set of behaviors *on its own* does not constitute an unfair practice. Rather, the unfair practice was marketing the software without telling consumers it behaved in all those ways and without giving consumers choice about them.

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
	of their computers and with marketing media that contains false representations regarding that software. • Failing to disclose that music files users can download and incorporate on their own Web sites contain additional code that delivers ads to users' computers. • Failing to disclose that music files downloaded and incorporated on users' Web sites will display ads that prompt site visitors to download other software represented as browser upgrades or other security software.	
FTC v. Digital Enterprises, Inc, d/b/a Movieland.com; Triumphant Videos, Inc., d/b/a Popcorn.net; Pacificon International, Inc., d/b/a Vitalix; Alchemy Communications, Inc.; AccessMedia Networks, Inc.; Film Web, Inc.; Binary Source, Inc., d/b/a Moviepass.tv; Medicaster, Inc., d/b/a Medicaster.net; CS Hotline, Inc.; Easton Herd; and Andrew Garroni Docket #062-3008	• Expressly representing or implying that the computer owner or user knowingly consented to the installation of software that would repeatedly launch lengthy pop-up payment demands, when neither the owner nor any user consented to the installation. • Expressly representing or implying that the computer owner is responsible to satisfy any contract that any other person entered into while using the computer, when this is not the case. • Causing software to be installed on consumers' computers that repeatedly launches textual and audiovisual pop-up payment windows that: o remain open for 40 seconds and cannot be closed or minimized through reasonable means, o reappear more and more often as time passes, and o demand that consumers pay at least $29.95 to stop the pop-ups from happening. • Causing software to be installed on consumers' computers such that it cannot be located or removed through the use of reasonable efforts. • Causing software to be installed on consumers' computers that makes changes to consumers' computers	Settlement reached requiring defendants to pay over $500,000 in consumer redress. Settlement terms prohibit defendants from: • Offering "anonymous" free trials with a negative option billing feature. • Misrepresenting that consumers have agreed to pop-up payment demands and therefore owe defendants payments. • Downloading software onto consumers' computers without their consent. • Displaying pop-up payment windows more than five times per day, more than once per hour, without a clearly labeled button to close the window and silence associated audio, and without a toll-free phone number and email address consumers can use to contact defendants. • Concealing their software by cloaking files or folders, using random or misleading files names, misrepresenting the purpose of files or folders, or causing files to be automatically reinstalled after the user has removed them.

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
	that actively prevent consumers from using the Windows Control Panel to uninstall the software.	Settlement terms require defendants to: • Provide a mechanism for consumers to uninstall their software. • Post uninstall instruction on all their affiliated web sites. • Stop billing and send uninstall instructions to who have not accessed defendants' content within the past 60 days. http://www.ftc.gov/opa/2007/09/movieland.shtm
In the Matter of Zango, Inc., f/k/a 180solutions, Inc., Keith Smith and Daniel Todd Docket #052-3130	• Using third-party affiliates and sub-affiliates to bundle and install advertising software with other programs without adequately disclosing the existence of the advertising software. • Installing advertising software programs, through affiliates and sub-affiliates, without consumers' knowledge or authorization. • Failing to provide a means for consumers to identify, locate, and remove advertising software.	Proposed settlement reached, ordering respondents to pay $3 million to the FTC. Respondents are forbidden from: • Displaying advertisements to any customer who obtained advertising software prior to January 1, 2006. • Exploiting security vulnerabilities in Internet browsers to install software. • Installing software without obtaining express consent from users. Respondents are obligated to: • Establish and publicize a consumer complaint mechanism that allows consumers to receive timely responses to their complaints about the advertising software. • Maintain a program to ensure that affiliates obtain proper consent from consumers before installing software. • Identify the software program that causes advertisements to be shown to consumers

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
		on the advertisements themselves. • Provide links to the consumer complaint mechanism on the advertisements themselves. • Provide consumers with a reasonable means of uninstalling the advertising software. http://www.ftc.gov/os/caselist/0523130/index.htm
FTC v. ERG Ventures, LLC and d/b/a ERG Ventures, LLC2, Media Motor, Joysticksavers.com, and PrivateinPublic.com; Elliot S. Cameron; Robert A. Davidson, II; Gary E. Hill; Timothy P. Taylor Docket #062-3192	• Representing that software operates as a standalone innocuous free program, such as a screensaver or icon, when that is not the case. • Failing to disclose that software or content being offered contains additional code and files that cause advertisements, track Internet usage and alter browser settings and existing software products. • Proceeding with installation of software packages despite the fact that a user has declined the terms of the software's End User License Agreement. • Installing software on users' computers that changes browser home pages, adds a menu bar to Internet browsers, tracks consumer's Internet usage, generates pop-ups (occasionally pornographic), degrades computer performance and attacks and degrades anti-spyware software.	Settlement reached, ordering defendant to pay $330,000 to the FTC and the IRS. Defendant is required to: • Clearly disclose the name and full functionality of all software prior to installation • Obtain consent from consumers prior to installing software • Maintain records of their business associates, customers, and marketing materials Defendant is forbidden to: • Distribute software which may interfere with consumer computer use http://www.ftc.gov/os/caselist/0623192/index.htm
In the matter of Sony BMG Music Entertainment, a general partnership Docket # 062-3019	• Failing to adequately disclose that audio CDs will install software on consumers' computers that limits the number of possible copies and file formats of the audio files. • Failing to adequately disclose that the bundled media player on an audio CD will transmit the consumer's Internet Protocol (IP) address and an album identifier to remote Internet servers for the purposes of displaying images and promotional messages on the consumer's	Settlement reached. Defendant is required to: • Clearly and prominently disclose on product packaging that: ○ software to limit the number of copies and file formats of audio files will be installed on consumers' computers, and ○ consumers who decline to install

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
	computer. • Causing content protection software which may expose consumers' computers to security risks to be installed on consumers' computers without adequate notification and consent. • Failing to provide a way for consumers to locate and/or remove content protection software through reasonable efforts, and thereby causing consumers to incur substantial costs.	content protection software from an audio CD will not be able to listen to the CD on a computer. • Obtain consent from consumers prior to installing software. • Destroy information collected about consumers through the use of audio CDs within three days of its receipt. • Clearly and prominently disclose on consumers' computer screens that: o information about consumers, their computers, or their use of audio CDs will be transmitted over the Internet, and o consumers who decline to permit transmission of information about them, their computers, or their use of their audio CDs will not be able to listen to the CDs on a computer. • Obtain consent from consumers prior to transmitting information about them, their computers, or their use of audio CDs. • Continue to provide consumer redress and assistance by posting information on the Web, buying advertising to explain the content protection software's security vulnerability, offering software patches, and compensating consumers monetarily and with additional audio CDs or music downloads. Defendant is prohibited from: • Using information collected about consumers through the use of audio CDs for any marketing purposes.

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
		• Installing software that cannot be readily located and removed by a consumer. http://www.ftc.gov/os/caselist/0623019/index.htm
In the matter of DirectRevenue LLC, DirectRevenue Holdings LLC, Joshua Abram, Daniel Kaufman, Alan Murray, and Rodney Hook Docket #052-3131	• Failing to adequately disclose that adware which tracks and stores information regarding consumers' Internet use and displays advertisements based on that information is bundled with other software. • Installing adware, directly or through affiliates, on consumers' computers entirely without notice or authorization. • Failing to provide a reasonable or effective means for consumers to identify, locate, and remove adware from their computers.	Proposed settlement reached, ordering respondents to pay $1.5 million to the FTC. Respondents are forbidden from: • Displaying advertisements to any customer who obtained advertising software prior to October 1, 2005. • Exploiting security vulnerabilities in Internet browsers or other applications to install software. • Installing software without obtaining express consent from users. Respondents are obligated to: • Establish and publicize a consumer complaint mechanism that allows consumers to receive timely responses to their complaints about the advertising software. • Maintain a program to ensure that affiliates obtain proper consent from consumers before installing software. • Identify the software program that causes advertisements to be shown to consumers on the advertisements themselves. • Provide links to the consumer complaint mechanism on the advertisements themselves. • Provide consumers with a reasonable means of uninstalling the advertising software.

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
		http://www.ftc.gov/os/caselist/0523131/index.htm

State Spyware Case Summary

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of New York v. Intermix Media, Inc. http://www.oag.state.ny.us/press/2005/apr/apr28a_05.html	• Deceptively and surreptitiously bundling invasive spyware or adware programs with "free" games, cursors, screensavers, or other small software programs. • Employing deceptive methods to prevent users from detecting and removing installed software, including: not making the software accessible in the "All Programs" or "Programs" list, hiding the software in folders not usually associated with programs, not listing the software in the "Add/Remove Programs" utility, not providing an uninstall utility for the software, and reinstalling the software after a user has deleted it.	New York General Business Law § 349, 350 New York common law prohibiting trespass to chattels	Settlement reached. Defendant agreed to pay $7.5 million in penalties and profit disgorgement, and accepted a ban on adware distribution. Founder and former CEO of Intermix also agreed to pay $750,000 in penalties and profit disgorgement. Acez Software, an affiliate which was downloading Intermix adware with free screensavers, agreed to pay $35,000. http://www.oag.state.ny.us/press/2005/oct/oct20a_05.html
State of Texas v. Sony BMG Music Entertainment http://www.oag.state.tx.us/oagnews/release.php?id=1370	• Failing to disclose on the packaging of an audio CD that software will be installed on the user's computer when the user places the CD in his computer. • Inducing the owner or operator of a computer to install software by ejecting an inserted audio CD unless the computer owner agrees to install the software, even though that software is not necessary for playback of the audio CD. • Surreptitiously installing a file that hides the presence of other files and folders such that the computer owner cannot locate them when performing a search of the file system.	Consumer Protection Against Computer Spyware Act (Texas Business and Commerce Code § 48.001 *et seq*) Texas Deceptive	Settlement reached. Defendant prohibited from releasing audio CDs containing software that employs technology to hide or cloak files or that does not provide an option to decline installation. Defendant required to provide notice on CD packaging of the functions and features of included software. Defendant's software is prohibited from gathering personal identifying information without users' express consent, and must be

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	• Installing files and folders in a location on the computer such that the computer owner may confuse them for essential files needed to run the computer when this is not the case. • Failing to disclose the presence of a software component that hides other files and folders. • Installing software that remains hidden and active even when its associated music player software is not active. • Making it extremely burdensome if not impossible to remove software by not including an uninstall utility and by requiring the computer owner to contact customer service to remove the software. • Secretly installing files on a user's computer before the user has consented to the installation. • Leaving files secretly installed on a user's computer after the user has declined to accept the related software's EULA. • Failing to disclose to the user the presence of secretly installed files even after the user has declined to accept the related software's EULA. • Failing to provide an uninstall utility for files secretly installed before a user has consented to the installation.	Trade Practices-Consumer Protection Act (Texas Business and Commerce Code § 17.47 *et seq*)	easily removed by users. Defendant required to provide consumer redress and assistance by posting information on the Web, buying advertising to explain the content protection software's security vulnerability, and offering software patches. Defendant required to pay restitution to any consumer whose CD-ROM drive was disabled by the software. Defendant also obligated to pay $750,000 to the state of Texas for attorney's fees. http://www.oag.state.tx.us/oagnews/release.php?id=1889
People of the State of California v. Sony BMG Music Entertainment	• Failing to adequately disclose on the outer packaging of a CD or in its EULA that content DRM software would be required to be installed in order to use the CD on a computer. • Failing to adequately disclose that DRM software modifies the Windows operating system in ways unintended by Microsoft. • Failing to adequately disclose that DRM software uses cloaking technology to hide itself on users' computers.	California Penal Code § 502(c) California Business and Professions Code § 17500	Settlement reached. Defendant is enjoined from: • Making false or misleading statements in connection with manufacture, sale or distribution of CDs. • Manufacturing or distributing any CD containing content protection software which hides or cloaks a file or directory.

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	• Failing to adequately disclose that DRM software remains in operation at all times, consuming computer resources. • Failing to adequately disclose that DRM software connects to remote Internet servers. • Failing to adequately disclose that DRM software creates computer security vulnerabilities. • Failing to adequately disclose that DRM software cannot be accessed or removed without extraordinary computer sophistication or outside software. • Causing unauthorized software to be installed on users' computers.		• Manufacturing or distributing any CD containing content protection software which is not readily removable through normal means. • Manufacturing or distributing any CD containing content protection software which tracks, limits or controls transfer or use of music files without disclosure on the outer packaging detailing features and limitations of the use of the CD. • Manufacturing or distributing any CD containing content protection software that tracks or collects personally identifiable information about users and which communicates such information to remote or another entity without express consent. Defendant required to provide consumer redress and assistance by posting information on the Web, buying advertising to explain the content protection software's security vulnerability, and offering software patches. Defendant required to pay restitution to any consumer whose CD-ROM drive was disabled by the software. Defendant also obligated to pay $750,000 to the state of California. http://ag.ca.gov/newsalerts/release.php?id=1400

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of Washington v. Secure Computer LLC, Paul E. Burke, Gary T. Preston, Manoj Kumar, Zhijan Chen, Seth T. Traub http://www.atg.wa.gov/pressrelease.aspx?&id=3770	• Intentionally using deceptive means to alarm the user that his computer may be infected with spyware and thereby inducing the user to download software that claims to be necessary to secure the user's computer. • Inducing the user to run a "free scan" of his computer through false representation and thereby transmitting software to the user's computer that deletes the user's "hosts" file. • Representing that software is an effective spyware removal program when it does not clean the user's computer of virtually any actual spyware. • Labeling something as spyware which is in fact a cookie or harmless registry key, or not installed on the computer at all. • Representing that a removal of infections has been performed when in fact the removed infections were harmless or not present and actual infections were not removed. • Trapping the user in a succession of pop-up warning messages and/or advertisements by simulating buttons on the pop-ups that normally permit the user to close windows or by altering the functionality of standard window-closing buttons. • Engaging in other behaviors including misrepresenting software as a Microsoft product, violations of the CAN-SPAM ACT, and violations of Washington's Commercial Electronic Mail Act.	Computer Spyware Act (Revised Code of Washington 19.270) Consumer Protection Act (Revised Code of Washington 19.86)	Defendant Chen admitted wrongdoing and agreed to pay $84,000 in fines and restitution as part of a settlement. The settlement prohibits Chen from sending Net Send messages for the purpose of advertising and from creating a false sense of urgency, exclusivity or need for products. Prior to advertising anything, Chen must consult with an attorney. Defendant Preston agreed to pay $7,200 in attorneys' fees as part of his settlement. The settlement prohibits him from assisting any person or organization in disguising its identity from the public or law enforcement. Defendant Traub agreed to a settlement in which he will pay $2,000 in attorneys' fees and refrain from illegally using trademarks, making unsubstantiated claims, or otherwise deceiving consumers in a marketing context. Defendant Secure Computer LLC agreed to pay $75,000 as restitution to Washington State purchasers of Spyware Cleaner and Pop-up Padlock, in addition to $925,000 in civil penalties and attorney fees. Settlement also prohibits defendant from engaging in numerous practices dangerous to consumers. http://www.atg.wa.gov/pressrelease.aspx?&id=5926

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status

State of New York
v.
Direct Revenue, LLC, and
Joshua Abram,
Alan Murray,
Daniel Kaufman,
Rodney Hook
 	
http://www.oag.state.ny.us/press/2006/apr/apr04a_06.html
	• Bundling a spyware program with "free" software without giving consumers any notice of the presence of spyware.
	• Bundling a spyware program with "free" software, giving consumers notice of the spyware only by following multiple links (in small print) through lengthy license agreements.
	• Distributing spyware through deceptive "ActiveX" advertisements that bombard consumers with pop-up prompts until they consent to a "free" software download that gives no notice of the presence of spyware.
	• Distributing spyware through deceptive "ActiveX" advertisements that bombard consumers with pop-up prompts until they consent to a "free" software download that gives notice of the presence of spyware only through a linked license agreement.
	• Installing spyware by using malicious code that exploits security vulnerabilities without giving any notice to consumers.
	• Displaying incessant pop-up ads, less than one minute apart, to consumers unwittingly infected with spyware.
	• Displaying deceptive ads which promote "security" and "anti-spyware" programs to consumers unwittingly infected with spyware.
	• Distributing spyware that avoids detection and removal by:
	  ○ failing to inform consumers that the spyware has been installed,
	  ○ obfuscating the presence of the spyware by scattering its files across a user's computer, using randomly-generated file names, and ascribing false modification dates to the files,
	  ○ failing to uninstall the spyware when the
		New York Executive Law § 63(12)
		
		New York General Business Law § 349-350
		
		New York common law
			Litigation pending.

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	software with which it was bundled is uninstalled, o preventing the inclusion of the spyware in the Windows "Add/Remove Programs" utility, and o reinstalling the spyware after consumers manually delete it. • Installing additional spyware and other programs after an initial spyware installation, without notifying consumers. • Installing additional spyware and other programs after an initial spyware installation, giving the spyware distributor permanent remote access to consumers' computers without their consent. • Failing to police contracted distributors, or to establish effective controls ensuring, promoting, or encouraging user notice and consent in third-party spyware distributions.		
State of Washington v. Software Online.com, and David W. Plummer[3]	• Misrepresenting the risk of harm to a user's computer (by falsely finding computers to be at risk and by listing Web sites to which the computer is vulnerable even when the computer blocks access to those sites) in order to induce the user to purchase a security product. • Misrepresenting the functions of standard "buttons" on software advertisements, thereby requiring users to continue to view the advertisements when they try to close them. • Leaving software files on users' computers without their knowledge or consent after they have	Consumer Protection Act (Revised Code of Washington 19.86.020)	Settlement reached in which defendants admit violations of the Consumer Protection Act. Defendants ordered to pay $150,000 in civil penalties and $40,000 in attorneys' fees. Settlement terms prohibit the following: • Inducing computer users to install software by misrepresenting that the user's computer is not secure. • Marketing software by means of a "free scan." • Using "buttons" in advertisements that do not function as the user

[3] An attorney for SoftwareOnline has disputed the inclusion of this case in this table. For more information, see the attorney's letter (http://www.cdt.org/privacy/spyware/20061208softwareonline.com.pdf) and CDT's response (http://www.cdt.org/privacy/spyware/20061222cdt.pdf).

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	uninstalled the associated software program. • Engaging in other behaviors including offering misleading negative-option billing to customers.		would expect. • Installing software that causes pop-up ads when the user tries to close other ads. • Failing to provide a functional uninstall option. • Failing to obtain a consumer's explicit consent to purchase a product or service. http://www.atg.wa.gov/pressrelease.aspx?&id=3878
State of Washington v. Digital Enterprises, Inc., d/b/a Movieland.com; Alchemy Communications, Inc.; AccessMedia Networks, Inc.; Easton A. Herd; and Andrew M. Garroni http://www.atg.wa.gov/pressrelease.aspx?&id=4362	• Taking control of a user's computer by means of pop-up videos that the user cannot close out of and thereby obstructing the user's access to the computer and disabling the functionality of the computer. • Providing a software uninstallation option in the "Add/Remove" section of a user's computer which represents to the user that the software can be removed when in fact it cannot be removed. • Failing to disclose that the two practices listed above will be used to force the user to pay for software when the user's 3-day "Free Trial" of the software ends. • Failing to disclose that software downloaded onto a user's computer for a 3-day "Free Trial" will consume a significant amount of computer memory – at least 27 megabytes of RAM. • Failing to disclose that software will be transmitted to a user's computer surreptitiously and activated with the consumer's knowledge or permission. • Representing that software contains "no spyware" when the software itself constitutes spyware insofar as it places files on the user's computer which send	Unfair Business Practices—Consumer Protection Act (Revised Code of Washington 19.86) Computer Spyware Act (Revised Code of Washington 19.270)	Settlement reached in which defendants agreed to pay $50,000 to resolve the allegations. Settlement terms require that: • Defendants display all material terms of a service offering on the same page of advertisements for the service such that consumers do not need to scroll down to read them. • Defendants obtain consumer consent to a service offering before collecting payment for that service. • Defendants make all service terms accessible to consumers in connection with any software download. • Defendants disclose clearly and prominently prior to software download the nature, frequency, and duration of any pop-up payment window the software may cause to appear on consumers' computers.

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	repeated, harassing notices that interfere with use of the computer; prevents the user from uninstalling the offending files; and leaves parts of the software on the user's computer if he or she manages to uninstall it.		Settlement terms prohibit: • Distributing software without certifying that the computer user owns the computer or is authorized to download software onto it. • Causing any pop-up window to display more than five times in any day or more often than once per hour. • Displaying pop-up windows without a clearly labeled button that causes the window to be invisible and any associated audio to be silenced. • Offering free trial software to Washington residents. • Causing software to appear in the Microsoft add/remove utility unless cliking on such a listing will remove the software. http://www.atg.wa.gov/pressrelease.aspx?&id=14480
State of Washington v. James Lane (QuikShield Security)	• Intentionally and knowingly deceiving consumers by stating that their computers have a malfunctioning security component and thereby inducing consumers to install security software. • Providing an uninstall process that does not work and does not remove the appropriate executable files from consumers' computers. • Misrepresenting that an advertisement for a commercial software product is a Microsoft operating system alert. • Misrepresenting that consumers have malfunctioning security components on their	Consumer Protection Act (Revised Code of Washington 19.86) Computer Spyware Act (Revised Code of Washington 19.270)	Settlement reached in which defendant agreed to pay $10,000 in civil penalties ($5,000 suspended pending compliance) and $6,444 in attorneys' fees. Settlement terms provide restitution to Washington residents and prohibit the following: • Failing to provide an operable install function for any products. • Misrepresenting the source of an advertisement. • Misrepresenting that security or privacy functions on a consumer's

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	computers when no such components exist. • Misrepresenting the ability to close advertisements with "cancel" or "x" buttons when in fact those buttons open a web site associated with the advertisements. • Misrepresenting that a software product is "absolutely free" when in fact only five free uses of the product are available before consumers are forced to pay for further use.		computer are not working properly. • Using the "X" button or other images typically associated with closing a window to perform any other function. • Failing to clearly identify the cost of a product. • Creating a false sense of urgency to purchase a product. http://www.atg.wa.gov/pressrelease.aspx?&id=4118
State of Washington v. High Falls Media, LLC; Roc Telecom, LLC; Mark Libutti; Brian Einhaus; and Thomas A. Tortora (Spyware Slayer)	• Intentionally and knowingly using deceptive means to alarm consumers that their computers may be infected with spyware and thereby inducing consumers to install security software. • Misrepresenting that scanning a consumer's computer for spyware will not load any software onto the computer when in fact a software download is necessary to perform the scan. • Misrepresenting that a "99% chance" that a consumer's computer is infected has been detected when in fact nothing has been done to detect the presence of malicious programs on the consumer's computer. • Misrepresenting that certain registry keys on consumers' computers are "extreme risk" spyware when in fact the keys are harmless. • Failing to address consumers' software complaints. • Providing a disconnected telephone number for consumers to use for customer service. • Other behaviors involving deception and misrepresentation in violation of the Consumer Protection Act.	Consumer Protection Act (Revised Code of Washington 19.86) Computer Spyware Act (Revised Code of Washington 19.270)	Settlement reached in which defendants agreed to pay $300,000 in civil penalties ($275,000 suspended pending compliance) and $30,000 in attorneys' fees. Settlement terms provide restitution to Washington residents and prohibit the following: • Creating a false sense of urgency or need for a product. • Failing to respond to consumers' complaints. http://www.atg.wa.gov/pressrelease.aspx?&id=4950

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of Washington v. SecureLink Networks LLC; NJC Softwares, LLC; Manuel Corona, Jr.; Rudy O. Corella; FixWinReg; and Hoanvinh V. Nguyenphuoc http://www.atg.wa.gov/pressrelease.aspx?&id=12328	• Installing a software bundle on a user's computer after the user has declined to consent to the bundle installation. • Failure to uninstall bundled software components when the program with which they came is uninstalled, or otherwise providing an obvious means of uninstalling bundled components. • Misrepresenting that advertisements for security software are operating system alerts regarding computer security problems. • Representing that critical security errors have been detected on a user's computer when no such errors were detected, with the purpose of inducing the user to purchase security products.	Computer Spyware Act (Revised Code of Washington 19.270) Consumer Protection Act (Revised Code of Washington 19.86)	Defendant HoanVinh Nguyenphoc, owner of WinFixReg, has reached a settlement. Defendants are forbidden from: • Misrepresenting a need for their product or the function of their product • Advertising using simulated system notices, such as security alerts http://www.atg.wa.gov/pressrelease.aspx?&id=18078 Litigation is pending for remaining defendants.

Federal Spyware Case Summary

Case	Behaviors considered illegal by the Department of Justice	Laws invoked	Status
United States v. Jerome T. Heckenkamp http://www.usdoj.gov/criminal/cybercrime/heckenkampPlea.htm	Prosecutors alleged: • Installing on another user's computer an unauthorized computer program that was designed to intercept electronic communications containing usernames and passwords. Defendant pled guilty to: • Engaging in other behaviors including gaining unauthorized access to a computer and recklessly causing damage to it.	18 U.S.C. §§ 2511(1)(a)	Count dismissed on government's motion (defendant convicted on separate, non-spyware counts). http://www.usdoj.gov/criminal/cybercrime/heckenkampSent.htm
United States v. Van T. Dinh	• Knowingly accessing a computer of another person without authorization by installing a series of "keystroke-logging" programs to remotely monitor the keystrokes of the computer user and thereby identify computer accounts and passwords.[4] • Engaging in other behaviors including a scheme to defraud an investor and committing mail and wire fraud.	18 U.S.C. §§ 1030(a)(4)	Defendant sentenced to 13 months in prison, ordered to pay $46,980 in restitution, and fined $3,000. http://www.usdoj.gov/criminal/cybercrime/dinhSent.htm
United States v. Juju Jiang http://www.usdoj.gov/criminal/cybercrime/jiangIndict.htm	• Knowingly accessing a computer of another person without authorization for the purpose of installing keylogging software to surreptitiously record keystroking activity on that computer and thereby collect computer usernames and passwords.[5] • Other behaviors involving trafficking in a counterfeit device and criminal infringement of copyrights.	18 U.S.C. §§ 1030(a)(4)	Defendant sentenced to 27 months in prison and ordered to pay $201,620 in restitution. http://www.usdoj.gov/criminal/cybercrime/jiangSent.htm
United States v.	• Knowingly creating, possessing, and selling a computer program, knowing that the program is primarily useful for the purpose of	18 U.S.C. §§ 2512(1)(b),	Warrant issued for defendant's arrest.

[4] Court documents for this case were unavailable online, thus the exact behaviors considered illegal by the Department of Justice were determined from supporting materials and press releases.
[5] *See* supra note 3.

Case	Behaviors considered illegal by the Department of Justice	Laws invoked	Status
Carlos Enrique Perez-Melara http://www.usdoj.gov/criminal/cybercrime/perezIndict.htm	surreptitious interception of electronic communications and that the program will be transported in interstate or foreign commerce. • Sending in interstate commerce the computer program described above. • Disseminating electronic advertisements for the computer program described above. • Intentionally promoting the use of the computer program described above for the purpose of surreptitious interception of electronic communications. • Knowingly intercepting wire communications using the computer program described above. • Knowingly disclosing to customers the contents of electronic communications obtained by using the computer program described above.	2512(1)(a), 2512(1)(c)(i), 2512(1)(c)(ii), 2511(1)(a), 2511(1)(c)	
United States v. John J. Gannitto (and the related cases of USA v. Powell, USA v. Selway) http://www.usdoj.gov/criminal/cybercrime/perezIndict.htm	Defendants pled guilty to: • Knowingly accessing a computer of another person without authorization by installing a computer program onto it and thereby obtaining information from the computer. Prosecutors also alleged: • Intentionally intercepting or procuring another person to intercept electronic communications of another person.	18 U.S.C. §§ 1030(a)(2)(c), 2511(1)(a)	Gannitto sentenced to 3 years supervised probation with 30 days in halfway house; Powell sentenced to 5 years supervised probation; Selway sentenced to 3 years unsupervised probation. Each defendant sentenced to pay a $500 fine.
United States v. Cheryl Ann Young http://www.usdoj.gov/criminal/cybe	Defendant pled guilty to: • Intentionally intercepting or procuring another person to intercept electronic communications of another person. Prosecutors also alleged: • Knowingly accessing a computer of another person without authorization by installing a computer program onto it and thereby	18 U.S.C. §§ 1030(a)(2)(c), 1030(c)(2)(B)(ii), 2511(1)(a)	Defendant sentenced to 3 years probation and ordered to pay a $500 fine and a $100 special assessment. Defendant ordered to perform 100 hours of community

Case	Behaviors considered illegal by the Department of Justice	Laws invoked	Status
rcrime/perezIndict.htm	obtaining information from the computer via interstate or communication with it.		service and refrain from contact with victim.
United States v. Christopher Maxwell http://www.usdoj.gov/criminal/cybercrime/maxwellIndict.htm	• Creating and using Internet Relay Chat botnets remotely and surreptitiously to install adware or other unauthorized programs on thousands of compromised computers, without the knowledge or consent of the computers' owners, and thereby obtaining thousands of dollars in commission payments from adware companies for those installations. • Conspiring to do the above.	18 U.S.C § 371, 18 U.S.C §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(B)(ii)	Defendant sentenced to 37 months in prison and forced to pay $252,000 in restitution and a $200 special assessment. http://www.usdoj.gov/criminal/cybercrime/maxwellPlea.htm
United States v. Jeanson James Ancheta http://www.usdoj.gov/criminal/cybercrime/anchetaArrest.htm	• Knowingly gaining unauthorized access to thousands of computers with the intent to install adware on those computers without notice to or consent from the users, and thereby obtaining thousands of dollars from the adware companies. • Redirecting infected botnet computers to a server containing a Trojan horse program and thereby causing the surreptitious installation of adware on the infected computers. • Conspiring to do either of the above. • Engaging in other behaviors including conspiring to obtain unauthorized access to thousands of computers and launching denial of service attacks.	18 U.S.C § 371, 18 U.S.C. §§ 1030(a)(5)(A)(i), 1030(a)(5)(B)(v)	Defendant sentenced to 57 months in prison, forced to pay $15,000 in restitution and forfeit the proceeds from his illegal activity. http://www.usdoj.gov/criminal/cybercrime/anchetaSent.htm
United States v. Kenneth Kwak http://www.usdoj.gov/criminal/cybercrime/kwakPlea.htm	• Intentionally installing remote control software on a user's computer (in a United States department or agency) with the intention of observing and gaining unauthorized access to that user's Internet use, electronic mail, and computer files. • Intentionally using remote control software to alter settings and defeat password protections on a user's computer (in a United States department or agency), thus allowing unrestricted access to the user's email by other persons on the user's network.	18 U.S.C. §§ 1030(a)(2)(B), 1030(c)(2)(B)(ii)	Defendant sentenced to 5 months in prison followed by 5 months of house arrest and ordered to pay $40,000 in restitution. http://www.usdoj.gov/criminal/cybercrime/kwakSent.htm
United States	• Surreptitiously installing a keylogger program on public computers	18 U.S.C. §§	Defendant sentenced to 4

Case	Behaviors considered illegal by the Department of Justice	Laws invoked	Status
v. George Nkansah Owusu	to record every keystroke made on those computers and using the collected data to gain unauthorized access to users' online accounts and university management systems.[6]	1030(a)(2)(C), 1030(c)(2)(B)(ii)	years in prison followed by 4 years supervised release and ordered to pay $2,550 in restitution.
United States v. Mario Alberto Simbaqueba Bonilla http://www.justice.gov/criminal/cybercrime/bonillaPlea.htm	• Illegally installing keystroke logging software on computers located in hotel business centers and Internet lounges around the world, and using the collected data to gain access to users' online bank, payroll, brokerage, and other accounts.	18 U.S.C. §§ 371, 1029(a)(2) and 2	Defendant sentenced to 9 years in prison, followed by 3 years supervised release. Ordered to pay $347,000 in restitution. http://www.usdoj.gov/criminal/cybercrime/bonillaSent.pdf
United States v. Hario Tandiwidjojo http://www.justice.gov/criminal/cybercrime/tandiwidjojoPlea.pdf	• Installing malicious software on hotel business computing kiosks that allowed him to intercept data, such as credit card information.	18 U.S.C. §§ 1030(a)(4)	Defendant sentenced to 10 months in prison and ordered to pay $34,000 in restitution.
United States v. John Schiefer	• Gaining unauthorized access to hundreds of thousands of computers in the United States, controlling these computers through servers. • Using compromised computer to search for other vulnerable computers, intercept electronic communication, and engage in identity theft.	18 U.S.C. §§ 1030(a)(4) and (c)(3)(A)	Defendant is awaiting sentencing.

[6] See *supra* note 4.

For further information, contact:
Heather West (202) 637-9800 x315.
Ari Schwartz (202) 637-9800 x107.