

Testimony of
Ari Schwartz, Deputy Director
Center for Democracy and Technology
before
The House Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection
on
“Combating Spyware: H.R. 964, the Spy Act”

March 15, 2007

Chairman Rush and Ranking Member Stearns, thank you for holding this hearing on spyware, which continues to be a major problem for consumers and businesses alike. CDT is honored to have the opportunity to participate in the Committee's hearing on this important topic.

CDT is a non-profit public interest organization dedicated to preserving and promoting privacy, civil liberties and other democratic values on the Internet. CDT has been a widely recognized leader in the policy debate about the issues raised by spyware.¹ Since CDT last testified before the Committee about spyware, in January 2005, the Federal Trade Commission has completed 11 spyware enforcement actions, three of which were based at least in part on petitions submitted by CDT. Over the past two years, CDT has also convened the Anti-Spyware Coalition (ASC), a group dedicated to building consensus about definitions and best practices in the debate surrounding spyware. The ASC's work to create uniform language and guidelines that can be used across the software industry has been beneficial for both consumers and software makers.

As an organization dedicated both to protecting consumer privacy and to preserving openness and innovation online, CDT has sought to promote responses to the spyware epidemic that provide meaningful protection for users while avoiding unintended consequences that could harm the open, decentralized Internet. We've worked with this committee now for several years, and during that time we've been consistently impressed with its open, deliberative approach to this complex issue.

¹ For example, CDT leads the Anti-Spyware Coalition (ASC), a group of anti-spyware software companies, academics, and public interest groups dedicated to defeating spyware; In 2006, CDT Deputy Director Ari Schwartz won the RSA Award for Excellence in Public Policy for his work in building the ASC and other efforts against spyware. See also "Eye Spyware," *The Christian Science Monitor*, Apr. 21, 2004 ["Some computer-focused organizations, like the Center for Democracy and Technology, are working to increase public awareness of spyware and its risks."]; "The Spies in Your Computer," *The New York Times*, Feb. 18, 2004 ["Congress will miss the point (in spyware legislation) if it regulates specific varieties of spyware, only to watch the programs mutate into forms that evade narrowly tailored law. A better solution, as proposed recently by the Center for Democracy and Technology, is to develop privacy standards that protect computer users from all programs that covertly collect information that rightfully belongs to the user."]; John Borland, "Spyware and its discontents," *CNET News.com*, Feb. 12, 2004 ["In the past few months, Ari Schwartz and the Washington, D.C.-based Center for Democracy and Technology have leapt into the front ranks of the Net's spyware-fighters."].

Summary

Although we have seen advances in the fight against spyware, millions of consumers are still losing money, time and peace of mind to this online scourge. CDT believes that the necessary framework for combating spyware involves a combination of law enforcement, anti-spyware technology, industry self-regulation and consumer education, legislation, and increased responsibility on the part of advertisers.

On the law enforcement front, the number of spyware actions at the federal level has increased dramatically since this Committee reported spyware legislation during the 109th Congress. The FTC has had a successful run in pursuing spyware cases, but the Commission needs increased civil penalty authority in order to be comprehensively effective. H.R. 964 provides such authority.

Spyware enforcement has also been developing at the state level, with 10 cases across four states thus far. Although H.R. 964 safeguards state-level enforcement under consumer protection statutes, it does not explicitly preserve the ability for state attorneys general to bring civil actions under statutory provisions specific to spyware. With all of the enforcement work going on at the state level, we feel it is important to safeguard the role of state attorneys general by empowering them to help enforce federal law.

We remain firmly committed to the idea that a long-term solution to spyware and other similar issues requires baseline privacy legislation. General privacy legislation would provide businesses with guidance as they deploy new technologies and business models that involve the collection of information. At the same time, a baseline law would give consumers some measure of confidence that their privacy is protected as companies roll out new ventures.

There are now 13 major companies that have joined with consumer groups in support of baseline privacy legislation.² If we do not begin to address privacy issues more comprehensively, the same players will be back in front of this Committee in a few months to address the next emerging threat to online privacy. We hope that we can address these issues in a way that obviates the need to enact new legislation each time a new privacy threat arises.

I. Understanding and Combating the Spyware Problem

When CDT last testified before this Committee about spyware, little data existed to quantify the size and impact of the spyware problem. Research conducted over the past two years, however, has produced some alarming results. Consumer Reports estimates that spyware cost consumers \$2.6 billion last year and affected 1 in 8 Internet users.³ An

² See *Consumer Privacy Legislative Forum Statement of Support in Principle for Comprehensive Consumer Privacy Legislation*, June 2006, <http://www.cdt.org/privacy/20060620cplstatement.pdf>. General Electric announced its support after the statement was issued.

³ "State of the net 2006," *ConsumerReports.org*, Sept. 2006,

AOL/National Cyber Security Alliance study conducted in 354 homes found that 61% of users had spyware installed on their computers.⁴ And the Pew Internet & American Life Project reported that nine out of ten Internet users say they have altered their behavior online due to fear of malicious software.⁵ All of these figures indicate that while we have seen advances in the fight against spyware, it continues to be a problem for many consumers.

CDT has long endorsed a multi-faceted approach to the spyware problem. We believe that the appropriate framework incorporates the following components:

- *Anti-spyware technology* – Anti-spyware software is a consumer's first defense against spyware infections. The collaboration fostered amongst technology vendors and public interest groups by the Anti-Spyware Coalition has helped to increase the usefulness of these technologies, which, in turn, creates a safer Internet experience for consumers.
- *Industry self-regulation and consumer education* – Helping industry and consumers understand the threat that spyware poses is an essential component of this framework. CDT has been active in the TRUSTe Trusted Download Program and the StopBadware campaign coordinated by Harvard's Berkman Center. Both of these have helped consumers and companies better understand the spyware issue.
- *Responsible advertising* – Large, well-respected companies help to fund the spread of unwanted and harmful adware by paying for advertisements generated by those unwanted programs. The New York attorney general's recent action against three high-profile advertisers,⁶ along with public pressure from the FTC,⁷ CDT,⁸ and others has begun to increase advertiser awareness and accountability.

http://www.consumerreports.org:80/cro/electronics-computers/online-protection-9-06/state-of-the-net/0609_online-prot_state.htm.

⁴ AOL/NCSA Online Safety Study, America Online and the National Cyber Security Alliance, Dec. 2005, http://www.staysafeonline.info/pdf/safety_study_2005.pdf.

⁵ Susannah Fox, *Spyware: The threat of unwanted software programs is changing the way people use the internet*, Pew Internet & American Life Project, July 6, 2005, http://www.pewinternet.org/PPF/r/160/report_display.asp.

⁶ See *In the Matter of Priceline.com Incorporated* (filed Oct. 23, 2006); *In the Matter of Travelocity.com LP* (filed Dec. 18, 2006); and *In the Matter of Cingular Wireless LLC* (filed Jan. 29, 2007), all available at <http://www.oag.state.ny.us/press/2007/jan/adware-scannedAODs.pdf>.

⁷ See, e.g., Cindy Skrzycki, "Stopping Spyware at the Source," *The Washington Post*, Mar. 6, 2007 [“We need to stop the demand side of spyware,’ said Jon Leibowitz, one of the five [FTC] commission members and a Democrat. ‘We will send letters to major corporations and entities that place the majority of these ads. This is a wake-up call to put them on notice. That would be a good way to choke off the money.’”].

⁸ See *Following the Money: How Advertising Dollars Encourage Nuisance or Harmful Adware and What Can be Done to Reverse the Trend*, Center for Democracy & Technology, May 2, 2006, <http://www.cdt.org/privacy/20060320adware.pdf>; and *Following the Money II: The Role of Intermediaries in Adware Advertising*, Center for Democracy & Technology, Aug. 2006, <http://www.cdt.org/privacy/20060809adware.pdf>.

- *Law enforcement* – The enforcement landscape has seen many changes over the past two years. The implications of these changes are discussed in section II below.
- *Legislation* – Legislative approaches to fighting spyware at the federal level fall into two broad categories – attempts to narrowly address the issues raised by spyware, and attempts to deal with the underlying privacy issues in a coherent, long-term fashion. H.R. 964, which we address in sections II and III below, is an example of the first approach. CDT has appreciated the opportunity to work with the Committee on this bill and is generally supportive of this effort, particularly because of the increased civil penalty authority it grants to the FTC for use in prosecuting spyware cases. At the same time, we remain firmly committed to the idea that a long-term solution to spyware and other similar issues requires baseline privacy legislation, as discussed in section IV below.

II. Spyware Enforcement and H.R. 964

The spyware enforcement landscape looks vastly different than it did two years ago when CDT last expressed concern to the Committee about the lack of enforcement activity. When the Spy Act passed out of the House in 2005, the FTC had issued complaints against two spyware distributors and one state attorney general had sued one spyware company. As of this writing, the FTC has completed 11 spyware enforcement cases and four states have conducted a total of 10 spyware lawsuits.⁹ The following sections explain the implications of FTC and state spyware enforcement for H.R. 964.

FTC Spyware Enforcement

The FTC filed the nation's first spyware lawsuit in 2004 against a network of deceptive adware distributors and their affiliates.¹⁰ The scammers involved were secretly installing software that left consumers' computers vulnerable to hackers, and then duping those same users into purchasing fake security software to help repair their systems. Not only did the FTC succeed in the case – obtaining a \$4 million order against the primary defendant and over \$300,000 in disgorgement from the other defendants – but the investigations in the case opened up several additional leads that contributed to the FTC's pursuit of other malicious software distributors. In the more than two years since launching this first suit, the FTC has used its broad authority under Title 5 of the FTC Act to pursue cases that cover a wide range of malicious software behaviors, all of which have ended with settlements or court orders that benefit consumers.

The FTC's enforcement efforts have also played an integral role in establishing standards for the software industry as a whole. In two of its most recent enforcement efforts, the FTC reached settlement agreements with major adware distributors Zango Inc. and

⁹ See Appendix A for a summary of all FTC, state, and Department of Justice spyware enforcement actions.

¹⁰ *FTC v. Seismic Entertainment, Inc., et al.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

DirectRevenue LLC that required the distributors to clearly and conspicuously disclose material terms about their adware programs *outside of any End User License Agreement (EULA)*.¹¹ With these requirements the FTC has set a disclosure guideline that can be applied across the software industry, for the benefit of consumers. Not only were the adware distributors themselves forced to abandon the practice of offering deceptive or nonexistent disclosures, but software vendors throughout the industry were also put on notice about what constitutes legitimate behavior. The FTC's leadership in this respect has helped to curb uncertainty in the software industry while creating a better online experience for consumers.

While these settlements set important precedents, the monetary relief obtained by the Commission was not commensurate with the harms perpetrated on consumers. Zango, a company that used deceptive tactics to earn over \$50 million in revenue in 2004 alone,¹² settled for a mere \$3 million with the FTC.¹³ The founders of DirectRevenue have pocketed a combined \$23 million,¹⁴ yet the FTC's proposed settlement requires only a \$1.5 million payment.¹⁵ As FTC Commissioner Jon Leibowitz noted in his dissenting statement in the DirectRevenue case, these numbers are disappointing because they leave the owners of the adware companies "lining their pockets . . . from a business model based on deceit."¹⁶

The increased civil penalty authority granted by H.R. 964 provides the FTC with the means to obtain more appropriate monetary relief. By giving the FTC explicit authority to seek large civil penalties for spyware infractions, the Commission will be much less encumbered and much more willing to obtain monetary relief commensurate with the harms committed. Both CDT and officials at the FTC have long been supportive of increased penalties, and we are pleased to see them included in H.R. 964.

State Spyware Enforcement

Several state attorneys general have become active in challenging spyware purveyors under state consumer protection, trespass, business practices, and spyware laws. In some of these cases the state attorneys general have taken the lead in nabbing high-profile offenders. For example, Texas took swift action against Sony BMG after it was discovered that the company had distributed millions of audio CDs containing spyware, and New York launched the nation's first investigation into DirectRevenue, nearly a year

¹¹ See *In the Matter of Zango, Inc., formerly known as 180solutions, Inc., Keith Smith, and Daniel Todd*, FTC File No. 052 3130 (filed Nov. 3, 2006), available at <http://www.ftc.gov/os/caselist/0523130/index.htm>; *In the Matter of DirectRevenue LLC, DirectRevenue Holdings LLC, Joshua Abram, Daniel Kaufman, Alan Murray, and Rodney Hook*, FTC File No. 052 3131 (filed Feb. 16, 2007), available at <http://ftc.gov/os/caselist/0523131/index.htm>.

¹² "Inc. Magazine Reveals America's 500 Fastest Growing Private Companies," Zango Inc., Nov. 1, 2005, <http://www.zango.com/Destination/Corporate/ReadArticle.aspx?id=36>.

¹³ See *supra* note 11.

¹⁴ Ben Elgin and Brian Grow, "The Plot to Hijack Your Computer," *BusinessWeek*, July 17, 2006, http://www.businessweek.com/magazine/content/06_29/b3993001.htm.

¹⁵ See *supra* note 11.

¹⁶ *Dissenting Statement of Commissioner Jon Leibowitz In Re DirectRevenue LLC, et al., File No. 052 3131*, Feb. 16, 2007, <http://www.ftc.gov/os/caselist/0523131/0523131directrevenueleibowitzstmt.pdf>.

before the FTC announced its settlement with the company. That litigation is still pending.

This growth in spyware enforcement at the state level in particular has several implications for H.R. 964. All of the state spyware cases have invoked state consumer protection laws, and thus we are pleased that Section 6(a)(2)(B) safeguards the authority of state attorneys general to challenge spyware practices under consumer protection statutes. What H.R. 964 does not safeguard, however, is the ability for state attorneys general to bring civil actions under statutory provisions specific to spyware. H.R. 964 preempts state spyware statutes without giving state attorneys general explicit authority to bring civil actions under the new federal law.

Six out of the 10 state spyware cases have invoked state spyware laws. If these state-level laws were to be replaced with a single federal standard, we feel it would be important to preserve the role of state attorneys general by empowering them to help enforce federal law. We understand that adding authority for state attorneys general raises jurisdictional issues, but we feel that this vital component of spyware enforcement must be addressed.

III. Comments on Specific H.R. 964 Language

CDT has minor suggestions on two specific parts of the bill.

First, CDT believes that Section 4(b) of H.R. 964, which gives the FTC explicit authority to seek civil penalties for pattern or practice violations of the Spy Act, will effectively increase the deterrent effect of spyware enforcement. However, it is important for the statute to be clear about what constitutes a “single action or conduct” in violation of the Act, because each single action or conduct carries either the \$3 million or \$1 million penalty as described in Section 4(b)(1). For example, DirectRevenue is a company that distributed similar software under a handful of different names and through dozens of different distribution channels and schemes. Had the FTC been able to bring its case against DirectRevenue under the Spy Act, we would hope that each of the different software distributions would be considered a “single action or conduct,” and thus the civil penalty sought by the FTC could be commensurate with the harm caused. We believe this clarification – that software provided by a single entity using multiple versions, configurations, or distributions can cause multiple violations – may be appropriately addressed in the Committee Report for H.R. 964.

Second, the definition of “personally identifiable information” provided in Section 11(13)(A) includes a list of different types of information that may be used to identify a living individual. An email address is one piece of information in this list, but in some cases email addresses cannot be used to determine the “real world” identity of particular individuals. Thus, some interpretations of this language could exempt email addresses from the definition of personally identifiable information. We believe that this would be a mistake, and we suggest that in Section 11(13)(A) the phrase “allows a living individual to be identified” should be replaced with “allows a living individual to be identified *or contacted*.” This will ensure that email addresses are considered as part of PII, since a

person can generally be contacted via email even if the email address does not identify the person.

IV. General Privacy Legislation and H.R. 964

Since our first testimony on this issue, we have urged the Committee to consider how some provisions of the Spy Act may be better addressed in baseline consumer privacy legislation. In light of the growing momentum behind this effort and the numerous other consumer and government privacy issues facing this Congress, we hope that the Committee will revisit these issues. For example, Section 3(c)(1)(B) of H.R. 964 prescribes specific notice language for software. Given the influence that H.R. 964 may have on the broader privacy debate, we have misgivings about a notice approach that specifies disclosure language in statute. Addressing notice at this level of detail in this bill could risk conflicting with or establishing difficult precedents for more general notice provisions in a broader privacy law.

A comprehensive privacy law may also address behaviors that have been omitted by the specificity of H.R. 964. For example, Section 3(b)(1)(B) includes in the definition of “information collection program” computer software that collects information about Web pages accessed on the computer and uses such information to display advertising on the computer. The statute does not, however, cover computer software which is used to collect information about Web pages accessed where that information is later disclosed to a third party but not directly used for advertising purposes. A broader privacy bill could help plug such gaps in H.R. 964.

V. Conclusion

CDT would like to thank the Committee for its hard work and openness throughout the spyware legislation process. While we believe H.R. 964 provides valuable increases to FTC civil penalty authority, we have several concerns with the bill. These include the bill’s pre-emption of state-level enforcement in an area where states are proving effective and interstate commerce has not been negatively affected, and the bill’s potential impact on the process of crafting and implementing general privacy legislation. We look forward to continuing to work with the Committee in addressing these issues and developing the strongest possible framework to protect consumer privacy in the digital age.

Appendix A: Summary of FTC, State, and Department of Justice Spyware Enforcement Actions

FTC 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	<ul style="list-style-type: none"> 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. <p>Additional defendants: Jared Lansky, John Robert Martinson, OptinTrade, Inc., Mailwiper, Inc., Spy Deleter, Inc.</p> <p>Docket #042-3142</p>	<p>Default judgment issued against Wallace and SmartBot.Net.¹⁷</p> <ul style="list-style-type: none"> 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. <p>Settlement reached with Lansky and OptinTrade:</p> <ul style="list-style-type: none"> Ordered to give up \$227,000 in ill-gotten gains. Barred from the same practices as Wallace and Smartbot.Net. <p>Seismic Entertainment filed for bankruptcy.</p> <p>Settlement reached with John Robert Martinson and Mailwiper:</p> <ul style="list-style-type: none"> Ordered to give up \$40,000 in ill-gotten

¹⁷ For the settlements listed in the "Status" column of all three charts in this Appendix, defendants admitted no wrongdoing unless otherwise noted.

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
		<p>gains with a suspended judgment of \$1.86 million.</p> <ul style="list-style-type: none"> • Barred from the same practices as Wallace and Smartbot.Net <p>http://www.ftc.gov/os/caselist/0423142/0423142.htm</p>
<p>FTC v. MaxTheater, Inc., and Thomas L. Delanoy Docket #042-3213</p>	<ul style="list-style-type: none"> • 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. 	<p>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</p> <p>http://www.ftc.gov/os/caselist/0523059/0523059.htm</p>
<p>FTC v. TrustSoft, Inc. d/b/a Swanksoft and SpyKiller, and Danilo Ladendorf Docket #052-3059</p>	<ul style="list-style-type: none"> • 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. 	<p>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.</p> <p>http://www.ftc.gov/os/caselist/0523059/0523059.htm</p>

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
In the matter of Advertising.com, Inc. a/d/b/a Teknousurf.com, and John Ferber Docket #042-3196	<ul style="list-style-type: none"> • 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. http://www.ftc.gov/os/caselist/0423196/0423196.htm	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.
FTC v. Odysseus Marketing, Inc., and Walter Rines Docket #042-3205	<ul style="list-style-type: none"> • 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.

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
<p>FTC v. Enternet Media, Inc., Conspy & Co., Inc., Lida Rohbani, Nima Hakimi, Baback (Babak) Hakimi, and Nicholas C. Albert</p> <p>Docket #052-3135</p>	<ul style="list-style-type: none"> • 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 installed¹⁸: (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 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. 	<p>Settlement reached with Defendant Albert ordering him to give up \$3,300 in ill-gotten gains. Defendant is enjoined from distributing software that interferes with consumers' computer use and from making false or misleading representations. Defendant is required to do substantial due diligence if he is to participate in any affiliate program.</p> <p>Settlement reached ordering remaining 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.</p> <p>http://www.ftc.gov/os/caselist/0523135/0523135.htm</p>

¹⁸ 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
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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ remain open for 40 seconds and cannot be closed or minimized through reasonable means, ○ reappear more and more often as time passes, and ○ 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 that actively prevent consumers from using the Windows Control Panel to uninstall the software. 	<p>Stipulated interim agreements reached.</p> <p>Defendants are:</p> <ul style="list-style-type: none"> • Prohibited from making representations that computer owners or users are required to pay for software when that is not the case. • Required to clearly and prominently disclose the nature, frequency, and duration of pop-up payment windows prior to obtaining consent from computer owners or users to download software that will cause the pop-ups. • Required to obtain consent from computer owners or users prior to installing software. • Prohibited from displaying pop-up windows more than five times in one day. • Prohibited from displaying pop-up ads that cannot easily be closed or whose audio is not easily silenced. • Prohibited from displaying pop-up ads that only appear when all other windows are closed. <p>Defendants Alchemy Communications, Inc. and AccessMedia Network, Inc. are additionally required to provide clear and prominent links on their pop-ups and home pages to a customer service Web site with a toll-free customer service telephone number and email utility. Other defendants are prohibited from interfering with the efforts of Alchemy Communications, Inc. and AccessMedia Networks, Inc. in complying with their stipulated interim agreement.</p> <p>http://www.ftc.gov/os/caselist/0623008/index.htm</p>

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
In the Matter of Zango, Inc., f/k/a 180solutions, Inc., Keith Smith and Daniel Todd Docket #052-3130	<ul style="list-style-type: none"> • 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. 	<p>Settlement reached, ordering respondents to pay \$3 million to the FTC.</p> <p>Respondents are forbidden from:</p> <ul style="list-style-type: none"> • 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. <p>Respondents are obligated to:</p> <ul style="list-style-type: none"> • 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	
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	<ul style="list-style-type: none"> • 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. 	<p>Defendants are also prohibited from making and distributing software that:</p> <ul style="list-style-type: none"> • Tracks consumers' Internet activity. • Changes browser settings, including security settings or home pages. • Generates numerous pop-up advertisements, even while browsers are closed. • Tampers with, disables or otherwise alters the performance of other programs, including anti-spyware or anti-virus programs. 	<p>Defendants' assets are also frozen.</p> <p>http://www.ftc.gov/os/caselist/05223130/index.htm</p>
In the matter of Sony BMG Music Entertainment, a general partnership Docket # 062-3019	<ul style="list-style-type: none"> • 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 	<p>Proposed settlement reached. Defendant is required to:</p> <ul style="list-style-type: none"> • Clearly and prominently disclose on product packaging that: <ul style="list-style-type: none"> ○ software to limit the number of copies and file formats of audio files will be installed on consumers' computers, and 	<p>http://www.ftc.gov/os/caselist/0623192/index.htm</p>

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
	<p>computer.</p> <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> ○ consumers who decline to install 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: <ul style="list-style-type: none"> ○ information about consumers, their computers, or their use of audio CDs will be transmitted over the Internet, and ○ 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 and with additional audio CDs or music

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
	<p>In the matter of DirectRevenue LLC, DirectRevenue Holdings LLC, Joshua Abram, Daniel Kaufman, Alan Murray, and Rodney Hook Docket #052-3131</p> <ul style="list-style-type: none"> • 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. <p>http://www.ftc.gov/os/caselist/06223019/index.htm</p>	<p>Defendant is prohibited from:</p> <ul style="list-style-type: none"> • Using information collected about consumers through the use of audio CDs for any marketing purposes. • Installing software that cannot be readily located and removed by a consumer. <p>Proposed settlement reached, ordering respondents to pay \$1.5 million to the FTC.</p> <p>Respondents are forbidden from:</p> <ul style="list-style-type: none"> • 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. <p>Respondents are obligated to:</p> <ul style="list-style-type: none"> • 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

Case	Company behaviors deemed unfair and/or deceptive by the FTC	Status
	<p>consumers before installing software.</p> <ul style="list-style-type: none"> • 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. 	<p><u>http://www.ftc.gov/os/caselist/0523131/index.htm</u></p>

State Spyware Case Summary

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of New York v. Itermix Media, Inc. http://www.oag.state.ny.us/press/2005/apr/apr28a_05.html	<ul style="list-style-type: none"> 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 Itermix also agreed to pay \$750,000 in penalties and profit disgorgement. Acez Software, an affiliate which was downloading Itermix adware with free screensavers, agreed to pay \$35,000. http://www.oag.state.ny.us/press/2005/oct/oc_t20a_05.html
State of Texas v. Sony BMG Music Entertainment http://www.oag.state.tx.us/oagnews/release.php?id=1370	<ul style="list-style-type: none"> 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. Installing files and folders in a location on the 	Consumer Protection Against Computer Spyware Act (Texas Business and Commerce Code § 48.001 <i>et seq</i>) Texas Deceptive Trade	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 easily removed by users.

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	<p>computer such that the computer owner may confuse them for essential files needed to run the computer when this is not the case.</p> <ul style="list-style-type: none"> • 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. 	<p>Practices-Consumer Protection Act (Texas Business and Commerce Code § 17.47 <i>et seq</i>)</p> <p>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.</p> <p>http://www.oag.state.tx.us/oagnews/release.php?id=1889</p>	
People of the State of California v. Sony BMG Music Entertainment	<ul style="list-style-type: none"> • 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. 	<p>California Penal Code § 502(c)</p> <p>California Business and Professions</p>	<p>Settlement reached. Defendant is enjoined from:</p> <ul style="list-style-type: none"> • Making false or misleading statements in connection with manufacture, sale or distribution of CDs. • Manufacturing or distributing any

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	<ul style="list-style-type: none"> • Failing to adequately disclose that DRM software uses cloaking technology to hide itself on users' computers. • 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. 	<p>Code § 17500</p> <ul style="list-style-type: none"> • CD containing content protection software which hides or cloaks a file or directory. • 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. 	<p>CD containing content protection software which hides or cloaks a file or directory.</p> <p>CD containing content protection software which is not readily removable through normal means.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Defendant required to pay restitution to any consumer whose CD-ROM drive was</p>

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, Zhiyan Chen, Seth T. Traub	<ul style="list-style-type: none"> 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. 	<p>Computer Spyware Act (Revised Code of Washington 19.270)</p> <p>Consumer Protection Act (Revised Code of Washington 19.86)</p>	<p>disabled by the software. Defendant also obligated to pay \$750,000 to the state of California.</p> <p>http://ag.ca.gov/newsalerts/release.php?id=1400</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Defendant Secure Computer LLC agreed to pay \$75,000 as restitution to Washington</p>

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
	<ul style="list-style-type: none"> 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. 	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	
State of New York v. Direct Revenue, LLC, and Joshua Abram, Alan Murray, Daniel Kaufman, Rodney Hook	<ul style="list-style-type: none"> 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 	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
	<p>spyware.</p> <ul style="list-style-type: none"> • Displaying deceptive ads which promote “security” and “anti-spyware” programs to consumers unwittingly infected with spyware. • Distributing spyware that avoids detection and removal by: <ul style="list-style-type: none"> ◦ 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 software with which it was bundled is uninstalled, ◦ preventing the inclusion of the spyware in the Windows “Add/Remove Programs” utility, and ◦ 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. <ul style="list-style-type: none"> • Failing to police contracted distributors, or to establish effective controls ensuring, promoting, or encouraging user notice and consent in third-party 		

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of Washington v. Software Online.com, and David W. Plummer ¹⁹	<ul style="list-style-type: none"> 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 uninstalled the associated software program. Engaging in other behaviors including offering misleading negative-option billing to customers. 	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: <ul style="list-style-type: none"> 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 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

¹⁹ 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
<p>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</p> <p>http://www.atg.wa.gov/pressrelease.aspx?id=4362</p> <ul style="list-style-type: none"> • 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. • 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 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. 	<p>Unfair Business Practices—Consumer Protection Act (Revised Code of Washington 19.86)</p> <p>Computer Spyware Act (Revised Code of Washington 19.270)</p>	<p>Litigation pending.</p>	

Case	Company behaviors considered illegal by state Attorneys General	Laws invoked	Status
State of Washington v. James Lane (QuikShield Security)	<ul style="list-style-type: none"> • 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 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. 	<p>Consumer Protection Act (Revised Code of Washington 19.86)</p> <p>Computer Spyware Act (Revised Code of Washington 19.270)</p>	<p>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:</p> <ul style="list-style-type: none"> • 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 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. <p>http://www.atg.wa.gov/pressrelease.aspx?&id=4118</p>

Case	Company behaviors considered illegal by state Attorneys General		Laws invoked	Status
State of Washington v. High Falls Media, LLC; Roc Telecom, LLC; Mark Libutti; Brian Einhaus; and Thomas A. Tortora (Spyware Slayer)	<ul style="list-style-type: none"> • 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. 		<p>Consumer Protection Act (Revised Code of Washington 19.86)</p> <p>Computer Spyware Act (Revised Code of Washington 19.270)</p>	<p>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:</p> <ul style="list-style-type: none"> • Creating a false sense of urgency or need for a product. • Failing to respond to consumers' complaints. <p>http://www.atg.wa.gov/pressrelease.aspx?&id=4950</p>

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	<ul style="list-style-type: none"> • 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. <p><u>http://www.atg.wa.gov/pressrelease.aspx?id=12328</u></p>	Computer Spyware Act (Revised Code of Washington 19.270)	Litigation pending.

Department of Justice 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	<p>Prosecutors alleged:</p> <ul style="list-style-type: none"> • Installing on another user's computer an unauthorized computer program that was designed to intercept electronic communications containing usernames and passwords. <p>Defendant pled guilty to:</p> <ul style="list-style-type: none"> • Engaging in other behaviors including gaining unauthorized access to a computer and recklessly causing damage to it. 	18 U.S.C. §§ 2511(1)(a)	Court 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 http://www.usdoj.gov/criminal/cybercrime/dinhIndict.htm	<ul style="list-style-type: none"> • 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.²⁰ • 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	<ul style="list-style-type: none"> • 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.²¹ • 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

²⁰ 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.

²¹ See supra note 19.

Case	Behaviors considered illegal by the Department of Justice	Laws invoked	Status
United States v. Carlos Enrique Perez-Melara http://www.usdoj.gov/criminal/cybercrime/perez/Indict.htm	<ul style="list-style-type: none"> • Knowingly creating, possessing, and selling a computer program, knowing that the program is primarily useful for the purpose of 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. 	18 U.S.C. §§ 2512(1)(b), 2512(1)(a), 2512(1)(c)(i), 2512(1)(c)(ii), 2511(1)(a), 2511(1)(c)	Warrant issued for defendant's arrest.
United States v. John J. Gannitto (and the related cases of USA v. Powell, USA v. Selway) http://www.usdoj.gov/criminal/cybercrime	<p>Defendants pled guilty to:</p> <ul style="list-style-type: none"> • Knowingly accessing a computer of another person without authorization by installing a computer program onto it and thereby obtaining information from the computer. <p>Prosecutors also alleged:</p> <ul style="list-style-type: none"> • 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

Case ime/perezIndict.htm	Behaviors considered illegal by the Department of Justice	Laws invoked	Status
United States v. Cheryl Ann Young http://www.usdoj.g ov/criminal/cybercr ime/perezIndict.htm	<p>Defendant pled guilty to:</p> <ul style="list-style-type: none"> • Intentionally intercepting or procuring another person to intercept electronic communications of another person. <p>Prosecutors also alleged:</p> <ul style="list-style-type: none"> • Knowingly accessing a computer of another person without authorization by installing a computer program onto it and thereby obtaining information from the computer via interstate or communication with it. 	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 service and refrain from contact with victim. http://www.usdoj.gov/crimina l/cybercrime/maxwellPlea.htm
United States v. Christopher Maxwell http://www.usdoj.g ov/criminal/cybercr ime/maxwellIndict.htm	<ul style="list-style-type: none"> • 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/crimina l/cybercrime/maxwellPlea.htm
United States v. Jenson James Ancheta http://www.usdoj.g ov/criminal/cybercr ime/anchetaArrest.htm	<ul style="list-style-type: none"> • 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. 	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/crimina l/cybercrime/anchetaArrest.htm

Case <u>htm</u>	Behaviors considered illegal by the Department of Justice	Laws invoked	Status http://www.usdoj.gov/criminal/cybercrime/anchetaSent.htm
	<ul style="list-style-type: none"> • 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. 		
<p>United States v. Kenneth Kwak http://www.usdoj.gov/criminal/cybercrime/kwakPlea.htm</p>	<ul style="list-style-type: none"> • 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 v. George Nkansah Owusu	<ul style="list-style-type: none"> • Surreptitiously installing a keylogger program on public computers 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.²² 	18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(ii)	Defendant sentenced to 4 years in prison followed by 4 years supervised release and ordered to pay \$2,550 in restitution.

²² See *supra* note 20.