WHO CAN FIX THE SPYWARE PROBLEM?

By Liying Sun

The term "spyware" encompasses a wide range of software that monitors computer usage without a user's knowledge or consent.[1] Some versions of spyware spawn pop-up ads while others track online activity, steal passwords, or even take control of a user's computer.[2] Spyware has grown to be an epidemic on the internet, infecting nearly 60% of household computers and causing an estimated $2.6 billion in damages in 2006.[3] Lawmakers and regulatory agencies confronting the spyware problem face two significant challenges: (1) various intermediaries in the spyware industry dampen accountability for spyware distribution and implementation; and (2) a precise and effective regulatory definition of "spyware" is virtually impossible to create.[4] Despite these difficulties, federal and state legislatures, the Federal Trade Commission (FTC), and private litigants have attempted to either create or enforce several mechanisms to combat the spyware epidemic since 2004. This Note provides a survey of these developments and assesses their overall effectiveness given the two significant challenges regulators face.

Part I of this Note describes the common types of spyware and the tactics they employ. In addition, Part I describes the layers of intermediaries within the industry that make enforcement of anti-spyware laws complex

---

1. FEDERAL TRADE COMMISSION STAFF REPORT, SPYWARE WORKSHOP: MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE 1 (2005), http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf [hereinafter FTC REPORT].

2. *Id.* at 2.

3. Alongside viruses, spam, and phishing, Consumer Reports listed "spyware" among the four major threats on the internet in 2006. It is estimated that spyware caused nearly one million U.S. households to replace their computers in 2006. Cost per incident averaged at $100, and the total damages were $2.6 billion. Consumers Union of U.S., Inc., *Cyber Insecurity: Viruses, Spam, Spyware—You're More Vulnerable Than You Think*, 71 CONSUMER REPORTS 20, No. 9 (2006); *see also*, WEBROOT SOFTWARE, INC., THE STATE OF SPYWARE: 2005 THE YEAR IN REVIEW 30 (2005) [hereinafter WEBROOT REPORT 2005] (identifying 400,000 websites that hosted spyware in 2005); America Online & National Cyber Security Alliance, AOL/NCSA Online Safety Study (2004), http://www.staysafeonline.info/pdf/safety_study_v04.pdf (finding 80% of customers' computers were infected with spyware programs with an average of 93 spyware components).

4. *See* CENTER FOR DEMOCRACY & TECHNOLOGY, FOLLOWING THE MONEY: HOW ADVERTISING DOLLARS ENCOURAGE NUISANCE AND HARMFUL ADWARE AND WHAT CAN BE DONE TO REVERSE THE TREND 5-6 (2006), http://www.cdt.org/privacy/20060320adware.pdf [hereinafter FOLLOWING THE MONEY]; FTC REPORT, *supra* note 1, at 2-5.

and/or less effective. Part II discusses the challenge of creating a regulatory definition of spyware and then analyzes several legislative approaches and existing laws used to combat spyware. Part II also reviews the effectiveness of litigation initiated by individual states, the FTC, and private citizens challenging parties within various sectors of the spyware industry. In Part III, this Note concludes that the encouraging results achieved since 2005 suggest that the multiple legal mechanisms working together are effectively controlling the spyware problem.

I. BACKGROUND

A. Common Types of Spyware

"Spyware" is often classified into four types of software: (1) system monitors, (2) Trojans, (3) adware, and (4) tracking cookies.[5] System monitors pose a serious privacy risk because they can secretly capture and transmit a user's personal information and passwords typed in online transactions.[6] Trojans appear to be legitimate software but they can be used to steal sensitive information, install malicious programs, hijack the computer, or compromise additional computers or networks.[7] Adware tracks users' online activities to deliver targeted pop-up ads.[8] Tracking

5. *See, e.g.*, WEBROOT REPORT 2005, *supra* note 3, at 89.

6. *Id.* at 8,44; FTC REPORT, *supra* note 1, at 9-10.

7. A Trojan is defined as:

> A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

Trojan Definition: TechEncyclopedia from TechWeb, http://www.techweb.com/encyclopedia/defineterm.jhtml?term=Trojan&x=&y= (last visited Jan. 23, 2007); *see also*, FTC REPORT, *supra* note 1, at 35; Kelly Martin, *Viruses, Phishing, and Trojans for Profit*, SECURITYFOCUS, Oct. 24, 2006, http://www.securityfocus.com/columnists/419/1; Joris Evers, *The future of malware: trojan horses*, CNET NEWS.COM, Oct. 13, 2006, http://news.com.com/The+future+of+malware+Trojan+horses/2100-7349_3-6125453.html; Dawn Kawamoto, *Trojan piggybacks on FireFox*, CNET NEWS.COM, July 26, 2006, http://news.com.com/Trojan+piggybacks+on+Firefox/2100-7349_3-6098615.html; United States Computer Emergency Readiness Team (US-CERT), Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks, (July 8, 2005), http://www.us-cert.gov/cas/techalerts/TA05-189A.html.

8. *See* FTC REPORT, *supra* note 1, at 3-4; *see, e.g.*, Benjamin Edelman, Berkman Center for Internet & Society at Harvard Law School, Documentation of Gator Advertising and Targeting (June 7, 2003), http://cyber.law.harvard.edu/people/edelman/ads/gator. *See generally* Peter S. Menell, *Regulating "Spyware": The Limitation of State "Laboratories" and the Case for Federal Preemption of State Unfair Competition Laws*, 20

cookies are small text files downloaded to a user's computer that preserve preferences on specific websites.[9] Many reputable websites use cookies, but third parties like adware developers use cookies for targeted online marketing.[10]

These spyware categories are not mutually exclusive, and different types of spyware often share similar tactics in achieving installation and evading detection and removal. Generally, spyware within these four categories can be installed in one of five ways: (1) without user knowledge or consent, through exploitation of operating system or browser vulnerabilities; (2) with user consent induced by deceptive or misleading pop-up messages; (3) with user consent obtained through inconspicuous, misleading or insufficient disclosure of what the software does or what other software it contains; (4) with user consent and disclosure, but targeting children who may not appreciate the harmful consequences of the installation; or (5) without knowledge or consent, through other spyware already installed on the system.[11]

BERKELEY TECH. L.J. 1363, 1396-97 (2005); Joanna Glasner, *Ads That Know What You Want*, WIRED NEWS, April 28, 2005, http://www.wired.com/news/ebiz/0,1272,67365,00.html.

9. Andrew Kantor, *When Cookies Aren't Monsters and Spyware Isn't Spyware*, USATODAY.COM, Jan. 28, 2005, http://www.usatoday.com/tech/columnist/Andrewkantor/2005-01-28-kantor_x.htm ("That's all cookies do. Sites leave bits of information about you on your own computer, then retrieve the information they left when you return.").

10. FTC REPORT, *supra* note 1, at 27 n.35; Wayne R. Barnes, *Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545, 1550-51 (2006); Stefanie Olsen, *Clueless about cookies or spyware?*, CNET NEWS.COM, Feb 8, 2005, http://news.com.com/Clueless+about+cookies+or+spyware/2100-1029_3-5561063.html; Michael Gowan, *How It Works: Cookies*, PCWORLD.COM, Feb 22, 2000, http://www.pcworld.com/article/id,15352/article.html ("For some, [cookies] promise a more user-friendly Web; for others, they pose a privacy threat.").

11. *See* Benjamin Edelman, Spyware Research, Legislation, and Suits, Spyware Installation Methods (October 16, 2006), http://www.benedelman.org/spyware/installations. One of the more egregious forms of spyware installation is called "drive-by downloads," which exploits a Windows security vulnerability. A user visits a website to view some content, but the webpage contains embedded code that can automatically download and install software without her knowledge or consent. *Id.*; *see also* Benjamin Edelman, Berkman Center for Internet & Society at Harvard Law School, Media Files That Spread Spyware (Jan. 2, 2005), http://www.benedelman.org/news/010205-1.html. In another scenario, a user may choose to install software because he thinks it is required to view content on a website. *Id.*; *see also*, News Release, Federal Trade Commission, FTC Shuts Down Spyware Operation (Nov. 10, 2005), http://www.ftc.gov/opa/2005/11/enternet.htm (discussing shutting down sites that offered "free" music for use on blogs bundled with a program that flashed fraudulent warnings about the security of their com-

Once installed, spyware evades detection and resists removal.[12] Most spyware does not come with uninstall software and many leave components behind after they are uninstalled.[13] Even if uninstalled, some spyware automatically downloads itself again once the computer is restarted.[14] Spyware can also disable users' internet security software or continuously mutate to avoid detection by conventional anti-spyware solutions.[15]

B. The Adware Industry

Although system monitors and Trojans are the most invasive and destructive types of spyware, existing criminal statutes adequately address them.[16] Recent spyware regulation targets the adware industry.[17] The basic adware business model requires only four constituents: advertisers, adware developers, adware distribution affiliates, and consumers.[18] Advertisers supply ad content and pay commissions to developers of adware for targeted advertising to consumers.[19] Adware developers pay distribution affiliates to install their adware on more computers.[20] In this basic model, objectionable installations and operations are easily traced back to the responsible developers or distributors, therefore advertisers and adware de-

---

puter systems). In some cases, even if the user clicks on the "Decline" button, the spyware will install itself anyway. FTC REPORT, *supra* note 1, at 7; *see also* News Release, Federal Trade Commission, FTC Testifies on Spyware (Oct. 5, 2005), http://www.ftc.gov/opa/2005/10/spyware.htm.

12. FTC REPORT, *supra* note 1, at 7-8.

13. *Id.*

14. *Id.*; ANTI-SPYWARE COALITION, ASC RISK MODEL DESCRIPTION, WORKING REPORT 7 (2006), http://www.antispywarecoalition.org/documents/documents/ASCRiskModelDescriptionWorkingReport20060622.pdf. [hereinafter ASC REPORT].

15. Jaikumar Vijayan, *Mutating Malware Evades Detection*, PC ADVISER, Nov. 11, 2006, http://www.pcadvisor.co.uk/news/index.cfm?newsid=7571. Conventional anti-spyware solutions recognize signatures in the spyware code while a new generation of anti-spyware is based on behavior heuristics. *See generally* Sana Security Inc., Sana Security—Delivering Enterprise Threat Protection, http://www.sanasecurity.com/products/technology/activeMDT.php (last visited Mar. 21, 2007) (introducing heuristics-based spyware detection method).

16. *See* Joris Evers, *Computer crime costs $67 billion*, CNET NEWS.COM, Jan. 19, 2006, http://news.com.com/Computer+crime+costs+67+billion+FBI+says/2100-7349_3-6028946.html. For a list of lawsuits involving system monitors and Trojans, see the Federal Spyware Case Summary, Center For Democracy & Technology, http://www.cdt.org/privacy/spyware/20060626spyware-enforcement-federal.php (last visited Feb. 8, 2007).

17. *See infra* Section II.B.

18. *See* FOLLOWING THE MONEY, *supra* note 4, at 2.

19. *Id.* at 3.

20. *Id.*

velopers seeking distribution can refuse to work with those offending players.[21]

But online advertising can be extremely lucrative, fueling not only more complex spyware, but also structure of the adware industry itself by creating numerous layers of intermediaries that reduce accountability to consumers, making it difficult for legislators, agencies, and private litigants to obtain damages.[22] In reality, advertising agencies, advertising affiliate networks ("AANs"), distribution affiliate networks ("DANs"), and their sub-networks form a thicket between advertisers and consumers.[23] Some security experts estimate that spyware generates $500 million to $2 billion a year in revenue for the AANs and DANs.[24] Advertising agencies and bigger AANs direct money (after taking a commission) from advertisers to adware developers or smaller AANs for the click-through traffic they generate.[25] The advertising agencies and AANs shield advertisers from the knowledge and control of how their ads are displayed.[26] Similarly, DANs direct money from adware developers to distribution affiliates by the number of installations they make.[27] Affiliate networks and the layers of sub-affiliate networks enable tens of thousands of individual affili-

21. *Id.*

22. According to the research firm IT-Harvest, spyware rakes in an estimated $2 billion a year in revenue, accounting for about 11% of the internet ad business. Ben Elgin, *The Plot to Hijack Your Computer*, BUSINESSWEEKONLINE, July 17, 2006, http://www.businessweek.com/magazine/content/06_29/b3993001.htm; Matt Hines, *Research: Spyware industry worth billions*, CNET NEWS.COM, May 3, 2005, http://news.com.com/Research+Spyware+industry+worth+billions/2100-1029_3-5693730.html. *See generally* FOLLOWING THE MONEY, *supra* note 4 (discussing the complexities of the real world adware market); Matt Hines, *Malware Money Tough to Trace*, EWEEK.COM, September 18, 2006, http://www.eweek.com/article2/0,1895,2016949,00.asp (commenting on the lack of accountability due to intermediaries in the adware industry).

23. FOLLOWING THE MONEY, *supra* note 4, at 3-6. There are two other kinds of intermediaries: (1) ad-serving platforms and (2) software vendors and websites. These two kinds of intermediaries receive money for serving some passive functions in the adware business model, but do not channel money further downstream. Ad-serving platforms store ads from thousands of advertisers for different adware to retrieve, so adware no longer needs to get ads from advertisers directly. Software developers and websites offer desirable software products and content for adware distributors to buddle with their adware. *Id.* Many of the intermediaries play multiple roles in the adware business model, further complicating the industry structure. *Id.*; Joseph Menn, *Big Firms' Ad Bucks Also Fund Spyware: Fortune 500 Members Are among the Unwitting Backers of Software That Sneaks into Computers*, LA TIMES, May 9, 2005, at C.1.

24. Menn, *supra* note 23.

25. *See* FOLLOWING THE MONEY, *supra* note 4, at 6.

26. *Id.*

27. *Id.* at 5.

ates to participate in the adware business without transparency or accountability.[28] Thus, effective anti-spyware regulation must recognize and address complexities in detection and enforcement created by these intermediaries.

II. REGULATORY APPROACHES AGAINST SPYWARE

A. The Spyware Definition

Spyware eludes a precise and effective regulatory definition.[29] The debate pivots on three issues: (1) the level of user knowledge and consent required for software installation; (2) the types of unacceptable software activities; and (3) the extent of harm that warrants sanction.[30] A narrow definition can easily be circumvented, but too broad a definition will interfere with legitimate business activity and possibly hurt innovation in advertising technology.[31]

It is not controversial to suggest that software distributors should provide disclosure and obtain consent before installation. However, some worry that an overly cumbersome notice and consent requirement will not only be costly to implement, but also counter-productive if users find the terms lengthy and burdensome.[32] Some software that brings risk to privacy and user control[33] can sometimes give consumers added convenience and value. For example, while criminals can use monitoring software to steal information, parents may use the same technology to oversee their children's online activities.[34] Targeted pop-up ads may be intrusive, but also

---

28. *Id.* at 4. Some of the largest advertising networks supporting the 180Solutions ad-delivering software include ValueClick Inc., Commission Junction, BeFree, ClickBank, and LinkShare. *See* Benjamin Edelman, Berkman Center for Internet & Society at Harvard Law School, Intermediaries' Role in the Spyware Mess (May 23, 2005), http://www.benedelman.org/news/052305-1.html.

29. FTC REPORT, *supra* note 1, at 3 (defining spyware as "software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge").

30. *Id.* at 4-5.

31. *Id.* at 15.

32. *Id.* at 5; *cf.* Electronic Privacy Information Center, The Children's Online Privacy Protection Act (Apr. 28, 2003), http://www.epic.org/privacy/kids (identifying some verification methods outlined by the FTC—sending/faxing printed forms, supplement of credit card numbers, calling toll-free numbers, and forwarding digital signatures through e-mail—as prohibitively costly and cumbersome).

33. *See generally* ASC REPORT, *supra* note 14 (showing privacy and control risks associated with various software functions).

34. *See* WEBROOT SOFTWARE INC., STATE OF SPYWARE Q1 2005 59 (2005).

allow consumers to receive relevant shopping information and help advertisers reach a market segment at lower cost.[35] Users with proper knowledge and consent often willingly compromise their privacy and control when there is sufficient reward.[36] A flat ban on any particular technology is not desirable because it can disrupt this market altogether. Individual consumers will tolerate different levels of risk. When defining spyware, some consider that "trespass" on a computer alone is *per se* harmful, while others call for a higher threshold of injury to consumers to justify such classification.[37]

Rather than creating one precise regulatory definition of spyware based on consent, software behavior, or harm, it may be more productive to identify and prohibit deceptive and unfair business practices in the context of spyware.[38] Deceptive and unfair practices can occur both during the software installation and during the operation, and they may encompass all the issues regarding consent, behavior, and harm.[39]

B. Spyware Regulation

The lack of consensus in terms of a regulatory definition of spyware is increasingly apparent when comparing state and federal legislation targeting spyware. By the end of 2006, sixteen states enacted spyware legislation.[40] Several federal bills have been proposed, and two were passed by the House of Representatives.[41] Spyware legislation falls roughly into four

35. *See* Menell, *supra* note 8, at 1396-97; Jean-Philippe Maheu, *2006: The Year of Behavioral Marketing*, BEHAVIORALINSIDER, Dec 16, 2005, http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=37562.

36. A reward may include, for example, free e-mail services or software that provides weather information.

37. *See* FTC REPORT, *supra* note 1, at 3.

38. *Id.* at 4 n.29 ("Panelists expressed broad support for the Consumer Software Working Group's effort to identify and prevent specific activities related to software that are unfair, deceptive, or devious.").

39. *Id.* at 3-4.

40. Twelve states enacted spyware legislation in 2005: Alaska, Arizona, Arkansas, California, Georgia, Indiana, Iowa, New Hampshire, Texas, Utah, Virginia, and Washington. In 2006, Hawaii, Louisiana, Rhode Island, and Tennessee also enacted spyware legislation. *See* National Conference of State Legislatures, 2005 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware05.htm (last visited Mar. 19, 2007); National Conference of State Legislatures, 2006 State Legislation Relating to Internet Spyware or Adware, http://www.ncsl.org/programs/lis/spyware06.htm (last visited Mar. 1, 2007).

41. The Safeguard Against Privacy Invasions Act (SPY-ACT) and the Internet Spyware (I-SPY) Prevention Act have both been passed by the House. H.R. 29, 109th Cong. (2005); H.R. 744, 109th Cong. (2005). Proposed bills include the Software Principles Yielding Better Levels of Consumer Knowledge, the Enhanced Consumer Protec-

categories: (1) bills against adware, (2) bills against deceptive and harmful software installation and operation, (3) bills with enhanced requirements for software notice and disclosure, and (4) bills against fraud and other criminal acts accomplished through spyware.

Utah was the first state to enact state spyware legislation.[42] Utah's Spyware Control Act falls into the first category.[43] Despite objections from many internet companies and adware developers,[44] the Act defines spyware as software that "collects information about an Internet website at the time the Internet website is being viewed" and "uses the information . . . contemporaneously to display pop-up advertising on the computer."[45] The Act bans the display of pop-up ads that are triggered by trademarks or URLs on the websites, which interfere with users' ability to view the content or paid advertising they originally attempted to access.[46] The Act gives the right of private action only to trademark and website owners.[47]

Other states have opted for a more consumer-focused approach, protecting them from deceptive and harmful spyware installation and operation by spyware vendors. Core prohibitions in this category are substantially similar.[48] For example, Washington State outlaws software that

---

tion Against Spyware Act, and the Computer Software Privacy and Control Act. S. 1004, 109th Cong. (2005); S. 687, 109th Cong. (2005); H.R. 4255, 108th Cong. (2004).

42. H.B. 323, 2004 Gen. Sess. (Utah 2004). This act was later amended to accommodate the dormant Commerce Clause. H.B. 104, 2005 Leg., 56th Sess. (Utah 2005).

43. Utah H.B. 104. Alaska and Tennessee have passed bills similar to Utah's amended spyware statute, although the Alaska bill is enforced under existing unfair business practices statute. S.B. 140, 24th Leg., 24th Sess. (Ala. 2005); S.B. 2069, 104th G.A. (Tenn. 2006).

44. Opposition Letter from AOL et al. to John Valentine, Utah State Senator, and Steve Urquhart, Utah House Representative (Mar. 1, 2004) (on file with the author), *available at* http://www.benedelman.org/spyware/utah-mar04/letter-01mar04.pdf. Following the initial enactment of the 2004 Spyware Control Act, an adware company WhenU moved to enjoin the Act for constitutional violations. WhenU won the preliminary injunction, and the Act was subsequently amended and passed again in March 2005. Susan P. Crawford, *First Do No Harm: The Problem of Spyware*, 20 BERKELEY TECH. L.J. 1433, 1440 (2005) (citing WhenU.com, Inc. v. State, No. 040907578 (D. Utah June 22, 2004).

45. *See* Utah H.B. 104 § 13-40-102.

46. Utah H.B. 104 § 13-40-201.

47. Utah H.B. 104 § 13-40-301.

48. This category of spyware laws are from Arkansas, Arizona, California, Georgia, Hawaii, Indiana, Iowa, Louisiana, New Hampshire, Rhode Island, Texas, and Washington. *See* Benjamin Edelman, Spyware Research, Legislation, and Suits, State Spyware Legislation (Apr. 23, 2006), http://www.benedelman.org/spyware/legislation; H.B. 6811, 2006 G.A., Jan. Sess. (R.I. 2006); H.B. 2904, 85th G.A., Reg. Sess. (Ark. 2005); H.B.

"through intentionally deceptive means," (1) modify computer's internet settings, (2) collect "personally identifiable information" through keyloggers or through monitoring "all or substantially all" website visits, (3) prevent "reasonable efforts" to block installation or to remove the software, or (4) disable anti-spyware technology already installed.[49] The law also addresses some of the specific harm that spyware causes: (1) "tak[ing] control of the computer" (a) by using the internet to cause damage to the computer or cause users to incur financial charges, or (b) through incessant display of pop-up advertisements that users "cannot close without turning off the computer or closing the internet browser"; (2) modifying internet settings that affect privacy and computer security.[50] In addition, the Washington statute bans software that installs despite users' express non-consent and that induces users' consent by "intentionally misrepresenting the extent to which installing the software is necessary for security or privacy reasons" or for opening a particular type of content.[51] Most legislation in this second category provides public enforcement by a state attorney general and many provide a private right of action for consumers, trademark owners, or any aggrieved parties.[52] The Washington spyware law gives the right of enforcement to both the attorney general and the affected website or trademark owners.[53]

The third category of legislation also protects consumers by significantly enhancing notice, consent, or disclosure requirements. For example, the Securely Protect Yourself Against Cyber Trespass Act (Spy Act) clearly states requirements for proper notice and consent for "information col-

---

2414, 47th Leg., 1st Reg. Sess. (Ariz. 2005); S.B. 127, 2005-2006 Leg. Sess. (Ga. 2005); H.B. 2256, 23rd Leg., Reg. Sess. (Haw. 2006); S.B 49, 114th G.A., 1st Reg. Sess. (Ind. 2005); H.F. 614, 81st G.A. (Iowa 2005); H.B. 690, 2006 Reg. Sess., (La. 2006); H.B. 47, 2005 Sess. (N.H. 2005); S.B. 327, 79th Leg., Reg. Sess. (Tex. 2005); H.B. 1012, 59th Leg., 2005 Reg. Sess. (Wash. 2005); S.B. 1436, 2003-2004 Sess. (Cal. 2004).

49. Wash. H.B. 1012 § 2.

50. *Id.* § 3.

51. *Id.* § 4.

52. Arkansas only allows public enforcement. Ark. H.B. 2904. Arizona, Texas, and Washington allow both public enforcement and private actions by software vendors, trademark owner, and website owners. Ariz. H.B. 2414; Tex. S.B. 327; Wash. H.B. 1012. California, Georgia, and Hawaii allow both public enforcement and private action by consumers. Cal. S.B. 1436; Ga. S.B. 127; Haw. H.B. 2256. Indiana, Louisiana, New Hampshire, and Rhode Island allow both public enforcement and private actions by any aggrieved parties. Ind. S.B 49; La. H.B. 690; N.H. H.B. 47; R.I. H.B. 6811. Iowa allows only private actions by software vendors and trademark and website owners. Iowa H.F. 614.

53. *See* Wash. H.B. 1012 § 6.

lection programs."[54] The Act prescribes the timing, content, format, and language of the notice and requires disclosure about the type of information collected as well as the purpose for which it is collected.[55] It also mandates that the software contain a disable-function and provide self-identifying information on each pop-up ad it delivers.[56]

The fourth category of spyware legislation combats criminal activity carried out with the use of spyware. For example, the proposed Internet Spyware (I-SPY) Prevention Act of 2005 would amend the Computer Fraud and Abuse Act of 1984 to criminalize unauthorized installation and use of software on a protected computer: (1) in furtherance of another federal crime; (2) to intentionally obtain or transmit personal information with the intent to defraud or injure a person or cause damage to a computer; or (3) to intentionally impair the security protections of the protected computer.[57]

Legislation within each category might prove effective in certain situations, but ineffective in others. For example, the fourth category tackles the most egregious types of spyware based on their criminal purpose, and the other three categories of legislation address spyware based on its offensive operation. In the first category, the Utah Spyware Control Act acknowledges consumers' rights only indirectly by failing to provide consumers with a private cause of action.[58] Nor is enforcement easy for trademark owners. The Act provides a safe haven for defendants who request state of residence information prior to sending pop-up ads.[59] Although it imposes liability for advertisers who purchase ads from adware developers, liability is imposed only if an advertiser ignores specific notices of violations from the trademark or website owners.[60]

---

54. *See* H.R. 29, 109th Cong. § 3. (1st Sess., 2005); *see also* S.B. 1315, 2004 Leg. (Mich. 2004) (as referred to Comm. on Tech. & Energy, June 22, 2004); Crawford, *supra* note 44, at 1445-48.

55. For software that collects user information, notice must be provided and consent be obtained before the software is transmitted, installed or executed. H.R. 29 § 3. Before a user is given the option to consent or decline, disclosure about the types of information collected, the purpose for the information collection and the identity of the software must be disclosed. H.R. 29 § 3(c)

56. H.R. 29 § 3(d)(1)-(2).

57. *See* H.R. 744, 109th Cong. § 2 (1st Sess. 2005).

58. *See* Utah H.B. 104 § 2.

59. The amended Act applies its penalties only to vendors who have installed their spyware on a computer in Utah and exempts from liability those who request residence information prior to sending pop-up ads. *See id*; *see also*, Crawford, *supra* note 44, at 1440.

60. *See* Utah H.B. 104 § 4.

The second category of spyware legislation is more sophisticated than a ban on pop-up ads because it addresses common deployment tactics of spyware developers.[61] Enforcement may also be stronger since both attorneys general and consumers have an incentive to battle spyware.[62] Nonetheless, these laws are weakened by a high threshold of harm to establish unlawful ad dissemination[63] and the requirement that the offending act be "intentionally deceptive."[64] The definition of "intentionally deceptive" fails to address the hidden, confusing or extremely lengthy disclosures that some spyware developers have implemented.[65]

The third category of legislation might address issues of hidden, confusing, or extremely lengthy disclosures by enhancing notice and disclosure requirements, but legislation like the Spy Act allows multiple information collection programs to use a single notice if they are provided in one software bundle.[66] For example, the extremely lengthy disclosure provided by Grokster for its large software bundle will pass the notice requirement unscathed.[67]

C. Spyware Litigation

Existing laws that prohibit unfair and deceptive business practices have also been used to address spyware, including some state business or consumer protection statutes a well as section 5 of the Federal Trade Commission Act ("FTC Act"). Spyware litigation comes in a variety of forms. Suits have been brought pursuant to spyware statutes, state fair business or consumer protection statutes, and common law by both states and by consumers. The FTC has also filed suits under the FTC Act. Although most of the defendants have settled, the way in which the settle-

61. *See e.g.*, H.B. 1012, 59th Leg., 2005 Reg. Sess. §§ 1-4 (Wash. 2005).

62. *See* Benjamin Edelman, Berkman Center for Internet & Society at Harvard Law School, What Hope for Federal Anti-Spyware Legislation? (Jan. 31, 2005) ("State attorneys general face public election which inspires aggressive pro-consumer litigation. Private parties also have clear incentives to sue, since they could seek to recover damages from spyware companies operating in violation of the bill's requirements."), http://www.benedelman.org/news/011905-1.html.

63. *See* Wash. H.B. 1012 § 3(1)(b).

64. "Intentionally deceptive" is (a) an "intentionally and materially" false statement, (b) an intentional and material omission or misrepresentation "in order to deceive", or (c) an intentional and material "failure to provide any notice" regarding the installation or execution of the program. Wash. H.B. 1012 § 1(5).

65. *See* Benjamin Edelman, Berkman Center for Internet & Society at Harvard Law School, California's Toothless Spyware Law (Sept. 29, 2004), http://www.benedelman.org/news/092904-1.html.

66. *See* H.R. 29 § 3(c)(1).

67. *See* Edelman, *supra* note 62.

ment agreements impose duties to control affiliates may have a lasting positive effect on the spyware problem.

1. State and Private Actions

Washington and New York have shown particular interest in fighting spyware through litigation.[68] Actions have been brought under the Washington Spyware Act, Washington Unfair Business Practices-Consumer Protection Act, and New York's General Business Law.[69] While the Washington State Attorney General targeted individual rogue software vendors, the New York Attorney General targeted well-known adware developers and distributors.[70] Both Attorneys General named individual corporate officers as codefendants for their participation in their companies' unlawful practices.[71]

In January 2006, the Washington State Attorney General filed his first spyware action under the Washington Spyware Act and Unfair Business Practices-Consumer Protection Act against Secure Computer LLC, its president, and its marketing affiliates in the U.S. and India.[72] The defen-

68. As of the end of 2006, Washington State Attorney General Rob McKenna has filed three spyware cases and (former) New York State Attorney General Eliot Spitzer has filed two.

69. The Washington Unfair Business Practices-Consumer Protection Act prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." *See* WASH. REV. CODE § 19.86.020 (2005). New York General Business Law prohibits "deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state." N.Y. GEN. BUS. LAW § 349 (1984). It also prohibits "false advertising in the conduct of any business, trade or commerce or in the furnishing of any service in this state[.]" *Id.* § 350 (1963).

70. *See* Verified Petition, New York v. Intermix Media, Inc., No. 401394-2005 (N.Y. Sup. Ct. Apr. 28, 2005); Verified Petition, New York v. DirectRevenue LLC, No. 401325-2006 (N.Y. Sup. Ct. Apr. 4, 2006); Complaint, Washington v. SoftwareOnline.com Inc., No. 06-2-12343-3SEA (Wash. Super. Ct. Apr. 11, 2006); Complaint, Washington v. Secure Computer LLC, No. C06-0126RSL (W.D. Wash. Jan. 24, 2006); Complaint, Washington v. Digital Enters., Inc., No. 06-2-26030-9 (Wash. Super. Ct. Aug. 14, 2006).

71. *See* Verified Petition, New York v. DirectRevenue LLC, No. 401325-2006 (naming Joshua Abram, Alan Murray, Daniel Kaufman, and Rodney Hook, the founders, officers, and owners of DirectRevenue LLC, defendants); Complaint, Washington v. SoftwareOnline.com, Inc., No. 06-2-12343-3SEA (naming David W. Plummer, the Chief Technology Officer of SoftwareOnline, Inc., a defendant); Complaint, Washington v. Secure Computer LLC, No. 06-0126RSL (naming Paul E. Burke, the president of Secure Computer LLC, a defendant); Complaint, Washington v. Digital Enters., Inc., No. 06-2-26030-9 (naming Easton A. Herd, the sole officer of Digital Enterprises, Inc., a defendant).

72. *See* Complaint at 23-32, Washington v. Secure Computer LLC, No. 06-0126RSL. Defendants were also cited for violations of the CAN-SPAM Act and The

dants fraudulently used Microsoft's name in advertisements, claiming that computers had been infected with spyware to induce consumers into purchasing a fake anti-spyware program.[73] The defendants' software also modified computer security settings related to user's access or use of the internet.[74] These acts allegedly violated the Washington Spyware Act, RCW 19.270.040(1) and RCW 19.270.030(2)(b), which prohibit a person from "induc[ing] a computer owner to install a computer software component by intentionally misrepresenting the extent to which installing the software is necessary for security or privacy reasons", and "modify[ing] security settings in order to cause damage to a computer."[75] Defendants' misrepresentation in promoting the software, deceptive tempering of computer settings, false claims of spyware detection and removal, and dissemination of deceptive and misleading pop-up ads allegedly violated the Unfair Business Practices-Consumer Protection Act.[76] Two similar actions have been filed against individual spyware vendors who made false and deceptive claims in promoting and running their products that prevented users from uninstalling their software.[77]

In April 2005, New York Attorney General filed suit against Intermix Media, Inc., a well-known adware distributor.[78] He filed another case in April 2006 against another prominent adware developer and distributor, DirectRevenue LLC.[79] He also named DirectRevenue's founders, owners

---

Commercial Electronic Mail Act for other associated acts. *Id.* at 8-13; *see also* Press Release, Washington State Office of the Attorney General, McKenna, Microsoft Announce Landmark Spyware Lawsuit (Jan. 25, 2006), *available at* http://www.atg.wa.gov/releases/2006/rel_Spyware_Lawsuit_012506.html.

73. *See* Complaint at 7, Washington v. Secure Computer LLC, No. 06-0126RSL.

74. *Id.* at 28-29.

75. *Id.* at 14-32; WASH. REV. CODE §§ 19.270.030(2)(b), 19.270.040(1) (2005).

76. *See* WASH. REV. CODE § 19.86.020.

77. *See* Complaint, Washington v. SoftwareOnline.com, Inc., No. 06-2-12343-3SEA; Complaint, Washington v. Digital Enters., Inc. No. 06-2-26030-9. The case against Digital Enterprises, Inc. is still pending, and the FTC also has sued them for the same conduct. *See* Complaint, FTC v. Digital Enters., Inc., No. CV06-4923CAS (C.D. Cal. Aug. 8, 2006).

78. *See* Verified Petition, New York v. Intermix Media, Inc., No. 401394-2005; *see also*, Press Release, Office of the New York State Attorney General Eliot Spitzer, State Sues Major "Spyware" Distributor: Intermix Media Accused of Vast Pattern of Surreptitious Installations (Apr. 28, 2005), *available at* http://www.oag.state.ny.us/press/2005/apr/apr28a_05.html.

79. *See* Verified Petition, New York v. DirectRevenue LLC, No. 401325-2006; *see also*, Press Release, Office of the New York State Attorney General Eliot Spitzer, State Sues Major "Spyware" Distributor: Direct Revenue Accused of Vast, Elusive Pattern of Spyware Installations (Apr. 4, 2006), *available at* http://www.oag.state.ny.us/press/2006/apr/apr04a_06.html.

and officers as codefendants in the case.[80] Intermix Media operated websites that advertised "free" software downloads.[81] However, Intermix secretly bundled this "free" software with ad-delivery programs, affecting millions of computers in New York and elsewhere.[82] DirectRevenue routinely distributed its programs without proper notice, through either "free" software bundles or "drive-by-downloads."[83] DirectRevenue's software design also hindered detection and removal.[84] New York State has not enacted any spyware statutes, so both actions were brought under the common law trespass to chattels and the New York General Business Law, which prohibits false advertising and deceptive business practices.[85]

Consumer actions also have been filed against big name adware vendors. Since 2005, consumers have filed class actions against adware developers and distributors including DirectRevenue LLC, 180Solutions, Inc., eXact Advertising, LLC, EBates Shopping.com, Inc., and Intermix Media, Inc.[86] *Sotelo v. DirectRevenue LLC* was the first class action suit that has moved past the summary judgment stage.[87] The plaintiff class was able to sustain four claims against Direct Revenue's motion to dismiss: (1) common law trespass to chattels; (2) violation of the Illinois Consumer Fraud Act through deceptive and misleading advertisements; (3) negligent breach of the duty not to harm plaintiffs' computers; and (4) computer

80. Verified Petition, New York v. DirectRevenue LLC, No. 401325-2006.

81. *See* Verified Petition at 4, New York v. Intermix Media, Inc., No. 401394-2005.

82. *Id.* at 3.

83. *See* Verified Petition at 5-13, New York v. DirectRevenue LLC, No. 401325-2006.

84. *Id.* at 14-15.

85. *See* Verified Petition at 8-9, New York v. Intermix Media, Inc. No. 401394-2005; Verified Petition at 17-8, New York v. DirectRevenue LLC, No. 401325-2006; N.Y. GEN. BUS. LAW §§ 349-350. Additional claims were brought against DirectRevenue under the N.Y. PENAL LAW § 156.20 (1999), which prohibits computer tampering. *See* Verified Petition at 19, New York v. DirectRevenue LLC, No. 401325-2006.

86. Civil Minutes for Defendant's Motion to Dismiss, Kerrins v. Intermix Media, Inc., No. CV05-5408-RGK (C.D. Cal. Jan. 10, 2006); Complaint, Consumer Advocates Rights Enforcement Soc'y, Inc. v. 180soultions, Inc., No. CV027141 (Cal. Super. Ct. Oct. 27, 2005); Complaint, Sotelo v. Ebates Shopping.com, Inc., No. 06C-2531 (N.D. Ill. May 5, 2006); Class Action Complaint, Simios v. 180Solutions, Inc., No. 05C5235 (N. D. Ill. Sept. 13, 2005); Memorandum Opinion and Order, Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219 (N.D. Ill. Aug. 31, 2005); Class Action Complaint, Michaeli v. eXact Adver., LLC, No. 05CV8331 (S.D.N.Y. Sept. 27, 2005).

87. *See* Julie Anderson & David Fish, Sotelo v. DirectRevenue, LLC: *Paving the Way for a Spyware-Free Internet*, 22 SANTA CLARA COMP. & HIGH TECH. L.J. 841, 842, 861 (2006).

tampering under Illinois Computer Crime Prevention Law.[88] So far, three of these cases have been filed in Illinois, two in California, and one in New York, all of which involve similar facts and claims.[89]

Although most of these state and private actions have been settled, they have produced some positive results. The settlements in state actions force defendants to disgorge their profits, and the settlements in the consumer actions have created prospective obligations that can disrupt further distribution of spyware. For example, in *Washington v. Secure Computer LLC*, the three U.S. defendants agreed to pay fines, disgorge profits between $2,000 and $84,000, and refrain from future similar practices.[90] The corporation, its officers, and affiliates in *New York v. Intermix Media Inc.* agreed to pay millions in penalties and disgorgement and were banned from future adware distribution.[91] Most consumer cases were either dropped, pending, or were settled without payment to the plaintiffs.[92] De-

88. Memorandum Opinion and Order, Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d at 1229-34, 1235-37.

89. Civil Minutes for Defendant's Motion to Dismiss, Kerrins v. Intermix Media, Inc., No. CV05-5408-RGK; Complaint, Consumer Advocates Rights Enforcement Soc'y, Inc. v. 180soultions, Inc., No. CV027141; Complaint, Sotelo v. Ebates Shopping.com, Inc., No. 06C-2531; Class Action Complaint, Simios v. 180Solutions, Inc., No. 05C5235; Memorandum Opinion and Order, Sotelo v. DirectRevenue, LLC, 384 F. Supp. 2d 1219; Class Action Complaint, Michaeli v. eXact Adver., LLC, No. 05CV8331.

90. *See* Consent Decree as to Seth Traub at 3-5, Washington v. Secure Computer LLC, No. 06-0126RSM (W.D. Wash. June 5, 2006); Consent Degree as to Gary Preston at 3-5, Washington v. Secure Computer LLC., No. C06-0126RSM (W.D. Wash. May 4, 2006); Stipulated Judgment and Order as to Zhijian Chen at 6-8, Washington v. Secure Computer, LLC, No. C06-0126RSM (W.D. Wash. April 14, 2006). In the case against SoftwareOnline.com, the defendants settled with an admission to multiple violations. The defendants agreed to pay $400,000 in civil penalties, with $250,000 suspended on condition of compliance with all terms in the settlement. They must also give refunds to consumers who have filed complaints and pay $40,000 in attorneys' costs and fees. Defendants also agreed to refrain from future similar practices. *See* Stipulated Judgment and Order as to SoftwareOnline.com, Inc. at 8-11, Washington v. SoftwareOnline.com, Inc., No. 06-2-12343-3SEA (Sup. Ct. Wash. Apr. 11, 2006).

91. Under the agreement, Brad Greenspan, the founder and former CEO of Intermix Media, will pay $750,000 in penalties and disgorgement. Assurance of Discontinuance at 3-4, *In re* Brad Greenspan (N.Y. Att'y Gen. Internet Bureau Sept. 28, 2005). Intermix will pay $7.5 million in penalties and disgorgement and accept a ban on the distribution of adware programs in the future. Intermix's affiliate, Acez Software, agreed to pay $35,000 in penalties and disgorgement and to adhere to fair notice and disclosure standards. Consent and Stipulation at 3-5, New York v. Intermix Media, Inc., No. 401394-2005 (N.Y. Sup. Ct. Sept. 28, 2005).

92. Kerrins v. Intermix Media, Inc., No. CV05-5408-RGK (pending); Complaint, Consumer Advocates Rights Enforcement Soc'y, Inc. v. 180soultions, Inc., No. CV027141 (pending); Complaint, Sotelo v. Ebates Shopping.com, No. 06C-2531 (pending); Class Action Complaint, Simios v. 180Solutions, Inc., No. 05C5235 (having been

spite a lack of published case law, these settlement agreements have created some non-pecuniary penalties and prospective responsibilities for defendants.[93] DirectRevenue was required to destroy all personally identifiable information it collected and provide uninstallation support for consumers.[94] Prospectively, DirectRevenue must provide full disclosure and require users to affirmatively consent before installation.[95] It may not distribute software at sites targeting children.[96] Most importantly, the settlement agreement required DirectRevenue to contractually bind its distributors to abide by the policies embodied in the settlement agreement.[97] DirectRevenue carries the duty to closely police its distributors.[98]

2. FTC Enforcement Actions

The FTC has been the most active force against spyware with eight spyware-related enforcement actions in the past two and a half years.[99] Section 5 of the FTC Act allows the FTC to challenge "unfair or deceptive acts or practices in or affecting commerce."[100] This relatively broad language allows the FTC to target ever-changing spyware tactics. So far, the FTC has targeted "deceptive and unfair" practices that include (1) depriving consumers of their right of consent and control in software installation, operation, and removal; (2) making misrepresentation and false statements

---

voluntarily dismissed); Settlement Agreement and Limited Release, Sotelo v. DirectRevenue, LLC, No. 1:05-cv-02562. Civil Minutes for Defendant's Motion to Dismiss, Class Action Complaint, Michaeli v. eXact Adver., LLC, No. 05CV8331 (pending).

93. *See e.g.*, Settlement Agreement and Limited Release 3-7, Sotelo v. DirectRevenue, LLC, No. 1:05-cv-02562.

94. *Id.* at 4-5.

95. *Id.*

96. *Id.* at 6.

97. *Id.* at 5-6.

98. *Id.*

99. Complaint, FTC v. Digital Enters., Inc., No. CV06-4923CAS (C.D. Cal. Aug. 8, 2006); Complaint, FTC v. Enternet Media, Inc. No. CV05-7777 (C.D. Cal. Nov. 10, 2005); Complaint, FTC v. Odysseus Mktg., Inc., No. CV05-00330, 2005 WL 3026853 (D.N.H. Sept. 21, 2005); Complaint, FTC v. TrustSoft, Inc., No. H05-1905, 2005 WL 1555021 (S.D. Tex. May 31, 2005); Complaint, FTC v. MaxTheater, Inc., No. CV-05-69-LRS, 2005 WL 4115954 (E.D. Wash. Mar. 7, 2005); Complaint, FTC v. Seismic Ent. Prods., Inc., No. 04cv00377, 2004 WL 3958666 (D.N.H. Oct. 6, 2004); Complaint, *In re* Zango, Inc., No. 0523130 (F.T.C. Nov. 3, 2006); Complaint, *In re* Advertising.com, Inc., No. C-4147, 2005 WL 2329812 (F.T.C. Sept. 12, 2005).

100. 15 U.S.C. § 45 (2005). In order to establish the "deception" element, the FTC must find that the representations, omissions, or practices likely would mislead consumers, acting reasonably, to their detriment. The "unfair" element is established if the spyware is "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition." *See* 15 U.S.C. § 45(n).

during installation and operation; (3) providing inadequate disclosure for ad-delivering software; (4) interfering with normal computer functions; and (5) failure to provide reasonable uninstall means.

The FTC filed actions against MaxTheater, Inc., TrustSoft, Inc., Seismic Entertainment Productions, Inc., and Advertising.com, Inc.[101] In these cases, defendants utilized affiliate websites, banner ads, pop-up ads, and/or spam to deceptively market fake anti-spyware products.[102] They falsely claimed before and after installation, that computers had been "scanned" and that spyware had been "detected" even though defendants had not performed any scans.[103]

In *In re* Advertising.com, in addition to misrepresentation and false advertising, the action also raised the issue of inadequate notice as a violation of the FTC Act.[104] In this case, the defendant displayed a "security warning" pop-up window and asked the user to install free anti-spyware software called "SpyBlast" which was bundled with other adware products.[105] While the license agreement disclosed that pop-up ads would be delivered based on user's browsing habits, the license was behind a hyperlink and consumers were not required to see it before installing the software.[106] Thus, the FTC alleged that the defendant did not provide sufficient disclosure to the user that third-party adware would be bundled with the SpyBlast.[107] The FTC stated that this insufficient disclosure violated the FTC Act, and ordered respondents to provide clear and conspicuous disclosure when an advertisement would be downloaded.[108]

Interference with normal computer use and control and lack of reasonable means to uninstall software are possibly violations of the FTC Act. In *FTC v. Digital Enterprises Inc.*, an online content provider induced con-

101. *See* Complaint, FTC v. MaxTheater, Inc., 2005 WL 4115954; Complaint, FTC v. TrustSoft, Inc., 2005 WL 1555021; Complaint, FTC v. Seismic Entm't Prods., Inc., 2004 WL 3958666; Complaint, *In re* Advertising.com, Inc., 2005 WL 2329812.

102. *See* Complaint at 3-6, FTC v. MaxTheater, Inc., 2005 WL 4115954; Complaint at 3-5, FTC v. TrustSoft, Inc., 2005 WL 1555021; Complaint at 2-5, 8-9, FTC v. Seismic Entm't Prods., Inc., 2004 WL 3958666; Complaint at 2, *In re* Advertising.com, Inc., 2005 WL 2329812.

103. *See* Complaint at 6-15, FTC v. MaxTheater, Inc., 2005 WL 4115954; Complaint at 5-13, FTC v. TrustSoft, Inc., 2005 WL 1555021; Complaint at 12-13, FTC v. Seismic Entm't Prods., Inc., 2004 WL 3958666; Complaint at 2, *In re* Advertising.com, Inc., 2005 WL 2329812.

104. Complaint 2-3, *In re* Advertising.com, Inc., 2005 WL 2329812.

105. *Id.* at 2.

106. *Id.*

107. *Id.* at 2-3.

108. *See id.* at 3.

sumers to download its software to view content for a "free trial."[109] The software then produced incessant pop-ups and hijacked users' computers, demanding payments.[110] The software provided no uninstall methods and only relinquished control when payments were continuously made.[111] None of the cases have reached a court ruling, and thus, it remains unclear whether this software violates the FTC Act.

In addition to fake anti-spyware vendors, the FTC also targeted various segments of the spyware industry, including adware developers and distributors, individual advertising/distribution affiliates, and intermediate advertising/distribution affiliate networks (AANs and DANs). For example, in *FTC v. Enternet Media, Inc.*, the FTC filed an action against an adware developer/distributor (Enternet Media) and an individual distribution affiliate (Nicholas C. Albert).[112] Albert was an individual distribution affiliate of Enternet Media and created a website with "free" music samples and ring tones, each secretly bundled with the adware code from Enternet Media.[113]

Other examples of defendant advertising/distribution affiliates include the defendants in *FTC v. Odysseus Marketing, Inc.* and *FTC v. Seismic Entertainment Productions, Inc.*[114] Both derived revenues from advertisers for disseminating pop-ups (as advertising affiliates) and from adware developers for installations (as distribution affiliates).[115]

Although adware developers have been able to evade responsibility for the violations of their affiliates, the FTC in *Enternet Media* alleged that providing the means and instrumentalities for the commission of deceptive and unfair acts and practices constituted a violation of section 5(a) of the

109. Complaint at 7, FTC v. Digital Enters., Inc., No. CV06-4923CAS.

110. *Id.* at 8-15.

111. *Id.* at 17-20. The two relevant counts were "unfairly tak[ing] control of consumers' computers to extort payments" and "unfairly instal[ling] software onto consumers' computers that consumers cannot remove." Both acts were unfair practices in violation of 15 U.S.C § 45(a). *Id.* at 21-22.

112. *See* Complaint, FTC v. Enternet Media, Inc., No.CV05-7777; *see also* News Release, Federal Trade Commission, FTC Shuts Down Spyware Operation: Outfit Used Unsuspecting Bloggers to Spread Its Malicious Code (Nov. 10, 2005), http://www.ftc.gov/opa/2005/11/enternet.htm.

113. Complaint at 4-7, 10, FTC v. Enternet Media, Inc., No. CV05-7777.

114. *See* Complaint 2-3, FTC v. Odysseus Mktg., Inc., 2005 WL 3026853; Complaint 2-3, FTC v. Seismic Entm't Prods., Inc., 2004 WL 3958666.

115. *See* Complaint at 9-10, FTC v. Odysseus Mktg., Inc., 2005 WL 3026853; Complaint 9-10, FTC v. Seismic Entm't Prods., Inc., 2004 WL 3958666.

FTC Act.[116] This indicates that adware developers could be held responsible for providing spyware code to their distribution affiliates.

In re Zango Inc. represents a big step toward piercing the layers of intermediaries and holding the top layer advertising and distribution networks responsible for the illegal acts of their third-party affiliates.[117] Defendant Zango (a/k/a 180solutions), is one of the most prominent adware vendors today.[118] Its products—180SearchAssistant, Zango, and others—have been consistently named among the top security threats by the anti-spyware industry.[119] The defendant installed its software on tens of millions of computers through third-party affiliate networks and numerous sub-affiliates.[120] In the past, Zango had been able to hide behind these layers of affiliates.[121] However, the FTC alleged that Zango had violated the FTC Act because it (1) "knew or should have known" that its affiliates had retained numerous third-party sub-affiliates to install its adware; (2) "knew or should have known" that there had been widespread failure by its affiliates and sub-affiliates to provide adequate notice and obtain consumer consent; and (3) had committed, through affiliates and sub-affiliates acting on its behalf and for its benefit, various deceptive and unfair software installations and operations.[122] No specific affiliates were named in the action, and it indicated that adware developers could be held responsible even without direct contact with or specific knowledge of their affiliates or sub-affiliates.[123]

---

116. *See* Complaint at 15, FTC v. Enternet Media, Inc., No.CV05-7777.

117. Complaint, *In re* Zango, Inc., No. 0523130; Agreement Containing Consent Order, *In re* Zango, Inc., No. 0523130 (FTC); News Release, Federal Trade Commission, Zango, Inc. Settles FTC Charges: Will Give Up $3 Million in Ill-Gotten Gains for Unfair and Deceptive Adware Downloads (Nov. 3, 2006), http://www.ftc.gov/opa/2006/11/zango.htm;

118. Complaint at 1-2, *In re* Zango, Inc., No. 0523130.

119. *See, e.g.*, Webroot Report 2005, *supra* note 3, at 34.

120. Complaint at 2, *In re* Zango, Inc., No. 0523130.

121. Letter from Keith Smith, CEO and founder of 180solutions, Inc., to Jerry Berman, the Center for Democracy and Technology (July 8, 2004), *available at* http://www.cdt.org/privacy/spyware/20040708180solutions.pdf ("In this instance, it appears that Aztec Marketing, through their Web site Ilookup.com, exploited a security hole in Microsoft's Internet Explorer to install our software along with others without our knowledge and consent and most importantly, without users' knowledge and consent.").

122. *See* Complaint at 2-5, *In re* Zango, Inc., No. 0523130.

123. *See id.* at 1.

All of the FTC actions have resulted in settlements.[124] Typically, defendants were ordered to disgorge profits ranging from tens of thousands of dollars to several million dollars and were barred from their respective deceptive practices.[125] Zango's settlement is particularly noteworthy because it not only involved a $3 million payment but also imposed some strict guidelines on its future practices.[126] First, Zango had to cease communication with users who downloaded the Zango/180solutions software before January 1, 2006.[127] Nor could it install software on users' computers without first obtaining "express consent" after clear and complete disclosures that are separate from the end-user license agreement (EULA).[128] Most importantly, the settlement makes clear that Zango is responsible for the actions of affiliates acting on its behalf.[129] This settlement sends a message that: (1) companies cannot retain customer bases built on patterns of unfair practices, (2) distributors of unwanted software cannot bury their disclosures in EULAs in hopes that users will simply click through without reading them, and (3) companies can no longer hide behind their affiliates.[130]

III. CONCLUSION

Regulating spyware is a challenge in many respects. This Note has provided a brief overview of the difficulties in defining spyware in the

124. *See* Center for Democracy and Technology, Federal Trade Commission Spyware Case Summary, http://www.cdt.org/privacy/spyware/20060626spyware-enforcement-ftc.php (last visited Mar. 19, 2007).

125. *E.g.*, Stipulated Final Order for Permanent Injunction and Settlement of Claims for Monetary Relief at 17-18, FTC v. Odysseus Mktg., Inc, No. 05CV330-SM, (D.N.H. Oct 24, 2006) (ordering Odysseus Marketing, Inc. to pay $1.75 million and refrain from distributing software that exploits a security vulnerability or installs without user consent); Stipulated Order for Permanent Injunction and Monetary Judgment at 4-12, FTC v. TrustSoft, Inc., No. H05-1905 (S.D. Tex. Jan. 5, 2006) (ordering TrustSoft to pay $1.9 million and refrain from making deceptive claims in the sale, marketing, advertising, or promotion of any goods or services); Stipulated Final Order for Permanent Injunction and Other Equitable Relief at 6-9, FTC v. MaxTheater, Inc., No. 05-CV-0069-LRS (E.D. Wash. Dec. 6, 2005) (ordering MaxTheater, Inc. to pay $76,000 and refrain from installing spyware on consumers' computers or making marketing misrepresentations).

126. Agreement Containing Consent Order at 4-8, *In re* Zango, Inc., No. 0523130 (FTC) (pending Commission's final approval), *available at* http://www.ftc.gov/os/caselist/0523130/0523130agree061103.pdf (last visited Feb 28, 2007).

127. *Id.* at 4.

128. *Id.* at 5, 7.

129. *Id.* at 5-7.

130. *Id.* at 4-7; *see also*, Press Release, Center for Democracy & Technology, CDT Praises FTC Adware Settlement, Urges Continued Enforcement (Nov. 20, 2006), http://www.cdt.org/press/20061120press-zango.php.

face of evolving technology and the complexity of the web advertising industry. However, spyware legislation as well as the existing consumer protection and unfair competition statutes have seemingly addressed the most widespread and egregious spyware problems. State, private, and FTC actions have targeted various segments of the spyware industry and some have been able to extract settlements that require future accountability and reform. Admittedly, enforcing the settlements is a whole other battle, and the online advertising industry needs to find its way to balance the benefits and burdens it creates for society. This Note concludes that the encouraging results achieved since 2005 suggest that the multiple legal mechanisms working simultaneously are effectively controlling the spyware problem.