I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

A Study of Spyware Enforcement Actions in Pursuit of Sound Internet Advertising Policy

RITA M. CAIN*

Abstract: This article focuses on downloaded ad-generating software programs and the legal responses to them. Despite their potentially legitimate advertising role, these downloaded programs cause various problems for users. To determine what kinds of computer problems have prompted legal action and government-enforced remedies, this article studies numerous recent cases brought against purveyors of ad-generating programs. Some of these actions were litigated by state attorneys general under new anti-spyware statutes. The Federal Trade Commission, the State of New York, and private parties have pursued other claims under traditional anti-fraud or computer crime laws. This discussion analyzes actions according to the various types of marketing behavior that the government targeted for enforcement. In a market where disputes abound regarding the problematic nature of "spyware," public policy makers and industry need to understand exactly what kinds of problems in the marketplace have triggered legal responses. This article concludes with recommendations for necessary federal legislation, including the role of the states.

* Professor of Business Law, Bloch School of Business and Public Administration, University of Missouri-Kansas City. Professor Cain gratefully acknowledges funding assistance for this research from the Bloch School Kemper Summer Grant Program.

A STUDY OF SPYWARE ENFORCEMENT ACTIONS IN PURSUIT OF SOUND INTERNET ADVERTISING POLICY

Commentators have noted for some time now that there is no consensus definition for "spyware."[1] Both spyware and "adware" are used to deliver targeted advertisements to individuals surfing the Web. These programs deliver ads in pop-up windows or bars that run across the top or bottom of a screen.[2] Both types of programs are often triggered by the user's particular web activity.[3]

Companies that make programs to run continuously and trigger ads in response to websites that users visit include Claria (formerly Gator), WhenU, and 180Solutions.[4] Others include Secure Computer, Digital Enterprises, and Direct Revenue. These organizations are not international fronts for criminal enterprises.[5] They are domestic companies providing in-demand interactive marketing services. High-profile clients such as Verizon, Merck, FTD, Motorola, and T-

---

[1] Liying Sun, *Who Can Fix the Spyware Problem?*, 22 BERKELEY TECH. L.J. 555 (2007); Martin Boldt & Bengt Carlsson, *Privacy-Invasive Software and Preventive Mechanisms*, IEEE COMPUTER SOCIETY 21 (PROC.OF THE INT'L CONF. ON SYS. AND NETWORKS COMMC'N.) (Oct. 2006), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.5949&rep=rep1&type=pdf; Agenda, Fed. Trade Comm'n Public Workshop, *Monitoring Software on your PC: Spyware, Adware and Other Software* 2 (Apr. 19, 2004).

[2] Some commentators use the term "malware" to describe programs that have nothing but a pernicious purpose, such as delivering viruses or stealing private information from the computer hard drive to facilitate identity theft. *See generally* Webopedia, http://www.webopedia.com/TERM/m/malware.htm (last visited May 30, 2009).

This paper focuses on programs downloaded for advertising purposes. This discussion is not about "malware" although some of the legal actions discussed below may address some of that type of software, as well.

[3] Eric Chien, *Techniques of Adware and Spyware*, SYSTEMS AND NETWORKS COMMUNICATIONS 22 (PROC. OF THE VIRUS BULL. CONF.) (2005), *available at* http://www.symantec.com/avcenter/reference/techniques.of.adware.and.spyware.pdf.

[4] Benjamin Edelman, "Spyware": Research, Testing, Legislation, and Suits, http://www.benedelman.org/spyware/#suits (last visited Apr. 18, 2009).

[5] Ben Elgin, *Guess What– You Asked for those Pop Up Ads*, BUSINESSWEEK ONLINE, June 28, 2004, http://www.businessweek.com/magazine/content/04_26/b3889095_mz063.htm; Annalee Newitz, *Don't Call It Spyware*, WIRED, Dec. 2005, http://www.wired.com/wired/archive/13.12/spyware.html.

Mobile utilize their adware.[6] Even the Anti-Spyware Coalition acknowledges the potential value of various software that it describes as "Spyware and Potentially Unwanted Technology." The group explains that "Advertising Display Software [m]ay be linked to other software that is wanted, subsidizing its cost," and "[m]ay provide advertising that is wanted by the user."[7]

Despite the potential value that ad-generating software can deliver, this marketing method creates many problems. Consumers complain about too many pop-up or banner ads that frustrate their internet browsing. Sometimes these ads cannot be closed and the only way the computer user can reestablish control is by shutting down and restarting.

More problematic are programs that overwhelm computers and necessitate costly clean up and repairs to restore their functionality. In organizations, costs are significant when such problems repeat themselves on multiple workstations. One analysis concluded that spyware cleanup costs a 1,000-person organization $83,000 annually.[8] In 2006, the Radicati Group estimated that cleanup of each workstation costs $265 per spyware infection.[9] Additionally, spyware can expose confidential personal or corporate information. These threats to information create the risk of unwitting regulatory violations under the Sarbanes-Oxley Act for publicly-traded corporations, HIPAA for health care professionals, and the Gramm-Leach-Bliley Act for financial services firms, in addition to the privacy policies of most organizations.[10]

---

[6] Edelman, *supra* note 4.

[7] Anti-Spyware Coalition, Anti-Spyware Coalition's Definitions Document, http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm (last visited Apr. 18, 2009).

[8] Mark Gibbs, *The Cost of Spyware*, NETWORK WORLD, Apr.26, 2004, http://www.networkworld.com/columnists/2004/0426backspin.html.

[9] Is3, Learning Center: The Cost of Spyware to Your Business, http://www.is3.com/learning/CostOfSpywareToYourBusiness.do (last visited Apr. 18, 2009).

[10] Sarah Lysecki, *Spyware Threatens Corporate Integrity, Customer Trust*, COMPUTING CANADA, Apr. 22, 2005, http://www.itbusiness.ca/it/client/en/CDN/DetailNewsPrint.asp?id=17411; Andrea Nixon, *Policy and Legal Implications of Spyware and Data Privacy*, EDUCAUSE Q., Nov. 1, 2006, at 5.

In between the annoying and the costly are various problems that hamper computer productivity. Some programs reset computer settings, such as home pages on Internet Explorer. Some cannot be readily removed, either manually or with anti-spyware programs. Others reinstall under different names when they are "removed." Adding insult to injury are anti-spyware programs that actually behave like spyware themselves.[11]

As a result of these costly problems, producers of ad-generating software are under significant attack through litigation and regulation.[12] Notwithstanding the lack of consensus about which ad-generating software should be characterized as "spyware," fifteen states have already passed anti-spyware legislation.[13] The U.S. Congress has been considering anti-spyware bills for several years without passage.[14]

Not every problem a computer user has with his or her computer because of ad-generating software may justify a legal remedy. To determine what kinds of computer problems have prompted legal action and government-enforced remedies, this article studies numerous recent cases against purveyors of ad-generating programs. State attorneys general litigated some of these actions under new anti-spyware statutes, while the Federal Trade Commission ("FTC"), the State of New York, and private parties have pursued other claims under traditional anti-fraud or computer crime laws. These cases reveal that regulators are undeterred by the lack of any consensus pertaining to the definition of "spyware." In the eyes of federal and state regulators, the behaviors alleged in these cases were actionable under long-held concepts in deceptive advertising law, as well as under new provisions in state spyware statutes. All the actions discussed below include complaints about the classic deceptive practice of making false or misleading statements to a consumer about the nature of the product

---

[11] Chien, *supra* note 3.

[12] *See* Alfred Cheng, *Does Spybot Finally Have Some Allies? An Analysis of Current Spyware Legislation*, 58 SMU L. REV. 1497 (2005).

[13] *See* National Conference of State Legislatures, State Spyware Laws, http://www.ncsl.org/programs/lis/privacy/spywarelaws.htm (last visited Apr. 18, 2009).

[14] Brian Krebs, *Spy vs. I-Spy: A Tale of Dueling Anti-Spyware Bills*, WASHINGTONPOST.COM, May 29, 2007, http://blog.washingtonpost.com/securityfix/2007/05/spy_vs_ispy_a_tale_of_dueling.html.

that the consumer is acquiring. Most of the actions discussed below also include some deception that is unique to computing and software.

On his website, Benjamin Edelman chronicles enforcement actions according to the particular vendor that is sued.[15] Conversely, the following discussion analyzes actions according to the various types of marketing behavior that the government targeted for enforcement. The article discusses whether existing consumer protection laws sufficiently remedy alleged harms from problem programs, or whether a different regulatory approach is needed to address the harms typical of ad-generating programs. These actions, which the parties settled, reveal legal issues that could be problematic for law enforcement if taken all the way through a trial and appeal. This study of pending and concluded actions suggests what is needed in spyware-specific federal legislation, including meaningful recommendations about federal preemption of state spyware regulation.

First, this article explains the marketing uses of these computer programs, and whether they are called adware or spyware.

I. MARKETING VIA DOWNLOADED PROGRAMS

The marketing model that employs ad-generating programs begins like the sale of many other forms of advertising. Legitimate companies looking for ways to advertise their goods or services hire ad agencies to place their advertising content on the Internet. Alternatively, advertisers may contact Internet ad purveyors themselves. The advertiser or ad agency will purchase ad space from adware vendors like Claria and others mentioned above.

Adware vendors employ a variety of vehicles to get clients' ads into end users' computers, including gaming software, peer-to-peer file sharing programs, toolbars for Internet browsers, cursors, clip art, or screen savers.[16] When computer users download these applications, they also get ad-generating modules that run concurrently with the application.[17] Programmers use a variety of techniques to trigger

---

[15] Edelman, *supra* note 4.

[16] Andrew Conry-Murray & Vincent Weafer, *The Symantec Guide to Home Internet Security* 68 (2005), *available at* www.informit.com/content/images/0321356411/samplechapter/Conry_ch05.pdf.

[17] Dan Tynan & Tom Spring, *The Hidden Money Trail*, PC WORLD, Oct. 3, 2005, http://www.pcworld.com/printable/article/id,122495/printable.html.

The existence of the advertising component may be disclosed in an end user licensing agreement ("EULA"). These ad-generating programs may avoid the label of spyware based

downloading, storage, and execution of interactive advertising programs on end users' computers.[18]

A survey of media directors of interactive advertising agencies found that a majority believes "click-through" is the best measure of online advertising effectiveness.[19] In other words, if the computer user responds to a pop-up ad or banner by clicking on it and being directed to the advertiser's website, then the ad has provided the advertising client real value. Such an ad-generating program targets users by tracking the content of the user's Internet browsing to trigger pop-ups that this particular user might be interested in following to learn more about this advertiser's product.

Despite the expected value of good targeting to increase "click through" rates, the foregoing study also found that only 33% of the respondents employed a click-through pricing model.[20] More than 90% of the respondents frequently used a "cost per thousand" to price banner ads, a metric that is used to price advertising in other mass media as well.[21]

Adding to this paradoxical pricing strategy is the presence of numerous "affiliates" that ad agencies use to distribute online advertising. These third parties are usually paid per "impression," the

---

on these disclosures regardless of whether customers have read or understood the entire EULA to realize all that they are downloading. *See infra* notes 109–13 and accompanying text. Others contend, however, that the notices in adware are inadequate to fully inform users that their Internet activity is being monitored to trigger the ads. Such commentators characterize all such programs as spyware. *See* Daniel B. Garrie, et al., *The Legal Status of Spyware*, 59 FED. COMM. L.J. 157, 161 (2006); Chien, *supra* note 3; Cade Metz, *Spy Stoppers*, PC MAGAZINE, Mar. 2, 2004, http://www.pcmag.com/article2/0,1895,1524249,00.asp. Researchers are studying the best way to alert consumers to the nature of what they are downloading. *See* Jordan M. Blanke, *"Robust Notice" and "Informed Consent:" The Keys to Successful Spyware Legislation*, 7 COLUM. SCI. & TECH. L. REV. 1, 2 (2006), *available at* http://www.stlr.org/html/volume7/blanke.pdf; Nathaniel Good et al., *User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware*, 2 ISJLP 283 (2006). This article will only discuss those issues in the context of legal mandates for customer notices.

[18] Chien, *supra* note 3.

[19] Fuyuan Shen, *Banner Advertisement Pricing, Measurement, and Pretesting Practices: Perspectives from Interactive Agencies*, 31 J. ADVERTISING 59, 62 (2002).

[20] *Id.*

[21] *Id.* at 62–65.

simple appearance of an ad on a user's screen.[22] This payment system motivates these distributors to load ads and ad-generating software all over the Internet, without regard to whether particular viewers would be interested in that ad or that advertiser's product. Other affiliates are software programmers who are motivated to get their programs distributed as widely as possible in exchange for bundling ad-generating programs into their freeware.[23] In other words, the more distributors who participate in the process, most with financial incentives unrelated to directing traffic back to advertisers' website, the less targeting is done.

Current common law of agency and contracts seldom imposes liability on vendors when their independent contractors improperly distribute a product through deceptive advertising practices like those discussed in the cases below.[24] Further, no existing state spyware law expressly requires that adware vendors monitor their affiliate distributors. A few states impose liability for "conscious avoidance" of knowledge about prohibited downloads.[25] This is the closest the law currently comes to binding an adware vendor for acts within their affiliate distribution channel. Unfortunately, this "conscious avoidance" standard requires proof that the vendor turned a blind eye to the unlawful acts of an affiliate, which may be difficult to prove if the distribution channel is vast and any individual programmer is remote from the adware vendor. Accordingly, as the cases below reveal, the role of these affiliates, and adware vendors' control of them, will be critical to a proper legislative response.

Some contend that targeting ads to accomplish click-through should not be the standard for measuring online advertising effectiveness.[26] These researchers contend that brand enhancement is a valuable function of Internet advertising and results from exposure

---

[22] CTR. FOR DEM. AND TECH., FOLLOWING THE MONEY: HOW ADVERTISING DOLLARS ENCOURAGE NUISANCE AND HARMFUL ADWARE AND WHAT CAN BE DONE TO REVERSE THE TREND 1, 6 (2006), http://www.cdt.org/privacy/20060320adware.pdf.

[23] *Id.*

[24] John Murphy & Harry Street, STREET ON TORTS 597 (12th ed. 2007).

[25] *See, e.g.*, S.B. 1436, Cal. State Leg., 2003–2004 Sess. (Cal. 2004).

[26] Rex Briggs & Nigel Hollis *Advertising on the Web: Is There Response Before Click-Through?* 37 J. ADVERTISING RES. 33, 33–34 (1997); Gerard Broussard, *How Advertising Frequency Can Work to Build Online Advertising Effectiveness*, 42 INT'L J. OF MARKET RES. 439 (2000); Xavier Drèze & François-Xavier Hussherr, *Internet Advertising: Is Anybody Watching?* 17 J. INTERACTIVE MARKETING 8, 8–9 (2003).

frequency, not unlike advertising in other mass media such as magazines and TV.[27] Under this theory, presenting computer users with multiple banner and pop-up ads about an advertiser's product accomplishes the legitimate marketing interests of the advertiser regardless of the number of direct responses to the ad.[28] Under this theory, paying affiliates for the volume of ad appearances triggered by the downloaded software is a logical pricing model (although one study concluded that gains in awareness diminish after seven exposures).[29]

While online ad frequency may be building brand enhancement for advertisers, the programs that deliver those ads are often overwhelming computers and frustrating computer users. These users complain to government officials, who respond with legal action.[30] These consumer problems and the legal responses they have spawned are discussed in the following section.

II. SPYWARE ACTIONS BASED ON EXPRESS MISSTATEMENTS AND NONDISCLOSURE FRAUD

Federal and state law expressly prohibits false, misleading or deceptive advertising.[31] As the following cases reflect, the FTC and state attorneys general do not need specific spyware legislation, or even an accepted definition of spyware, to prosecute vendors of ad-generating software for fraud.

Federal Trade Commission v. Enternet Media.[32] is the seminal case and is the closest spyware example to traditional fraudulent misrepresentation. A seller represented a product to be of one type or quality, but what the consumer actually got was something completely

---

[27] *Id.*

[28] Chun-Yao Huang & Chen-Shun Lin, *Modeling the Audience's Banner Ad Exposure for Internet Advertising Planning*, 35 J. ADVERTISING 123, 124 (2006).

[29] Broussard, *supra* note 26.

[30] *See supra* notes 8–11.

[31] *See generally* Jon Mize, *Fencing Off the Path of Least Resistance: Re-Examining the Role of Little FTC Act Actions in the Law of False Advertising*, 72 TENN. L. REV. 653 (2005).

[32] Complaint for Injunctive and other Equitable Relief at 2, Fed. Trade Comm'n v. Enternet Media, No. CV-05-7777 (C.D. Ca. Nov. 1, 2005), *available at* http://www.ftc.gov/os/caselist/0523135/051110compo523135.pdf.

different. The FTC alleged that the defendants duped consumers into downloading and installing exploitative software code by disguising it as innocuous freeware such as Internet browser upgrades, music files, cell phone ring tones, and song lyrics.[33] Most of the downloaded programs were not the promised freeware at all. Instead, they were programs that tracked Internet activity, changed homepage settings and displayed pop-up ads.[34]

Fraud can be proved by express misstatements and also by failure to disclose material information to the buyer about the promised good or service. One affiliate in *Enternet Media* operated a website that offered free music files to bloggers and others to play as background music on their websites. In this instance, although the user received the promised free music, the downloads also included unwanted, undisclosed code.[35] Once the music was copied and pasted into blogs or other websites, the undisclosed program captured the sites and used them to distribute the exploitative code even further.[36]

In this case, the vendors' express misstatements about allegedly free software and failure to disclose the presence of "exploitative" programs allegedly constituted deceptive acts and practices under the FTC Act.[37] The FTC and Enternet Media (along with various individual defendants) entered into a settlement agreement in August, 2006. The final order permanently enjoins Enternet Media and its affiliates from all of the offending Internet advertising practices the FTC alleged.[38] The FTC fined the defendants over $8.5 million, but suspended $6.5 million.[39] The defendants were placed on eight-year "probation" during which the FTC will monitor them. Additionally, the defendants were imposed with multiple monitoring and reporting obligations regarding the Internet advertising activities of all "their officers, agents, directors, employees, salespersons, independent

---

[33] *Id.* at 6.

[34] *Id.* at 7.

[35] *Id.* at 6.

[36] *Id.* at 6–7.

[37] 45 U.S.C. § 45(a) (2007).

[38] Stipulated Final Order for Permanent Injunction and Monetary Judgment at 5, Fed. Trade Comm'n v. Enternet Media, No. CV-05-7777 (C.D. Cal. August 22, 2006), *available at* http://www.ftc.gov/os/caselist/0523135/060823enternetmediastlmnt.pdf.

[39] *Id.* at 8.

contractors, subsidiaries, affiliates, successors, assigns, and all other persons in active concert or participation with any of them . . . ."[40]

Similarly, in *State of New York v. Intermix Media,* the New York Attorney General accused the defendants of deceptively and surreptitiously bundling invasive ad-generating programs with "free" games, cursors, screensavers, or other software programs.[41] To support its complaint, the state relied on the general business code, which prohibits false advertising and deceptive business practices, as well as the common law claim of trespass to chattels.[42] The state alleged more than three million downloads of the offending software to New York computers.[43]

In 2005, Intermix Media agreed to pay $7.5 million in penalties and profit disgorgement, and accepted a ban on adware distribution.[44] Brad Greenspan, the founder and former CEO of Intermix, agreed to pay $750,000 in penalties and profit disgorgement.[45] Acez Software, an affiliate that was downloading Intermix adware with free screensavers, agreed to pay $35,000.[46]

A similar action is pending in New York against Direct Revenue and several of its individual officers.[47] In this case, the lack of an agreed-upon definition of spyware could be fatal to one of the state's

---

[40] *Id.* at 15.

[41] Verified Petition at 3, People of the State of New York v. Intermix Media, Inc., No. 401394-05 (N.Y.S. Apr. 28, 2005) [hereinafter Intermix Media Petition], *available at* http://www.oag.state.ny.us/media_center/2005/apr/Verified_Petition.pdf.

[42] N.Y. GEN. BUS. LAW §§ 349–350 (2007).

[43] Intermix Media Petition, *supra* note 41, at 3.

[44] Consent and Stipulation at 4, New York v. Intermix Media, Inc., No. 401394-05 (N.Y.S. Sept. 28, 2005), *available at* http://www.oag.state.ny.us/media_center/2005/oct/Intermix%20COJ.pdf.

[45] Att'y Gen. of the State of N.Y.: Internet Bureau, Assurance of Discontinuance at 3, In the Matter of Brad Greenspan (Sept. 28, 2005), *available at* http://www.oag.state.ny.us/media_center/2005/oct/Greenspan%20AOD.pdf.

[46] *See* Press Release, Office of the N.Y. State Att'y Gen., Internet Exec Held Accountable for Adware, Spyware (Oct. 20, 2005), *available at* http://www.oag.state.ny.us/press/2005/oct/oct20a_05.html.

[47] Verified Petition at 7, New York v. Direct Revenue, No. 401325-06 (N.Y.S. Apr. 4, 2006) [hereinafter New York v. Direct Revenue Petition], *available at* http://www.oag.state.ny.us/media_center/2006/apr/Direct Revenue Verified Petition.pdf.

allegations of express misstatement. New York asserts that Direct Revenue offered a free program on a website that falsely stated that the program was "100% Spyware Free."[48] This vendor, like most adware vendors, differentiates its ad-generating software from "spyware" based on an End User License Agreement ("EULA") associated with the products that disclosed the presence of the ad-generating code.[49] New York has no spyware-specific legislation that provides any definition of spyware. Plaintiffs and prosecutors will have difficulty proving *intentional* falsity by adware vendors about whether their products are spyware without an accepted standard of what is, or is not, spyware.[50] New York's case against Direct Revenue appears strong– with only one allegation that could fail without a statutory definition of "spyware." Accordingly, the alleged express misrepresentation claim will hinge on a conclusion that "100% Spyware Free" was a known falsity.

A consumer class action against Direct Revenue in Illinois federal court asserted many of the same complaints as the New York case.[51] The case survived the defendants' motion to dismiss and the parties agreed to injunctive relief.[52] Ultimately, the defendants agreed to pay $300,000 in attorneys' fees and expenses.[53]

Defendants deny any wrongdoing when they enter the settlements like those in *Enternet Media* and *Intermix Media*. Thus, such cases do not reflect any legal conclusion by a court about the alleged wrongdoing. Nevertheless, these cases challenge whether any special legislation targeting ad-generating software is necessary to address classic fraudulent misstatements or nondisclosure about the nature of the product the vendor is providing. The FTC and New York pursued

---

[48] *Id.*

[49] *See infra* notes 120–23 and accompanying text.

[50] The Direct Revenue complaint includes a violation of New York criminal law for computer tampering, which prohibits any intentional altering or destroying of another person's computer programs or data. *See* New York v. Direct Revenue Petition, *supra* note 47.

[51] Mem. Op. and Order at 1, Soleto v. Direct Revenue, No. 05 C 2562 (N.D. Ill. Aug. 29, 2005), *available at* http://www.sunbelt-software.com/ihs/alex/drruling.pdf.

[52] *Id.* at 28.

[53] Settlement Agreement and Limited Release at 4, 13, Soleto v. Direct Revenue, No. 05 C 2562 (N.D. Ill. Mar. 9, 2006), *available at* http://www.spywarewarrior.com/mvp/DirectRevenue-SA.pdf.

and settled these cases under long-held authority to regulate false and misleading advertising. New York also relied on a common law tort for the protection of personal property. All states grant similar authority to their state attorneys general to regulate in-state actions for false and misleading advertising. The tort of trespass to chattels has been widely discussed as a remedy to assaults on computers from unwanted ad-generating programs.[54]

Like the foregoing cases prosecuted under existing anti-fraud authority, most of the actions discussed next also include some claim of false statement or nondisclosure about the nature of the program(s) the computer user is actually downloading. The following cases are distinguishable, however, because they also include complaints about programming tactics that are employed by the ad-generating software. Do unique computing and software tactics suggest that new or special authority is necessary? These next cases address that question.

III. SPYWARE ACTIONS BASED ON DRIVE-BY DOWNLOADS AND UNINSTALL/REINSTALL TACTICS

The FTC maintains a basic enforcement premise that a computer user's hardware is his or her own property that cannot be disrupted or violated simply because a software distributor can access it.[55] Many current federal and state statutory and common laws that protect personal property are based on this same principle. The following cases reflect issues beyond misstating or failing to disclose the exact nature of downloaded software. These cases include programming tactics that actually alter the computer users' existing software and computer settings.

The FTC's first spyware case was *Federal Trade Commission v. Seismic Entertainment*, in which the Commission alleged that defendants exploited a known vulnerability in Internet Explorer to download spyware to users' computers without their knowledge.[56]

---

[54] *See* Blanke, *supra* note 17; but *see* Alan F. Blakley et al., *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 25 DUKE L. & TECH. REV. ¶¶ 7–9 (2005), http://www.law.duke.edu/journals/dltr/articles/2005dltr0025.html.

[55] DEBORAH PLATT MAJORAS, FINDING SOLUTIONS TO FIGHT SPYWARE: THE FTC'S THREE ENFORCEMENT PRINCIPLES 5 (Feb. 9, 2006), http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf.

[56] Compl. for Inj. and Other Equitable Relief, Fed. Trade Comm'n v. Seismic Entm't, Inc., No. 04-377-JD (D.N.H. Oct. 6, 2004) [hereinafter Seismic Entm't Complaint].

This is referred to as a "drive-by" tactic.[57] According to the complaint, the offending software hijacked consumers' home pages, caused an incessant stream of pop-up ads, and allowed secret installation of additional software programs that generated more ads and tracked users' Internet activity.[58] These unannounced programs caused computers to severely slow down or crash.[59]

A federal district court temporarily enjoined the defendants from using this method to distribute their software.[60] A default judgment was entered against two defendants who never answered, which included injunctions and a penalty over $1.8 million.[61]

The pending action of the New York Attorney General against Direct Revenue also includes a complaint of drive-by downloads: "In such instances, simply visiting a given website infected the user's computer with spyware programs."[62]

In *Federal Trade Commission v. Odysseus Marketing,* defendants offered a free software program that purported to make users anonymous when using peer-to-peer file-sharing programs.[63] Along with this "anonymizer" program, defendants' software also installed other harmful, unwanted programs.[64] These facts reflect the same nondisclosure deception discussed above in *Enternet Media* and *Intermix.* Additionally, in this case consumers could not remove the unwanted ad-generating software by any reasonable means.[65] The

---

[57] *Id.*

[58] *Id.* at 10.

[59] *Id.*

[60] Fed. Trade Comm'n v. Seismic Entm't, No. 04-377-JD, 2006 U.S. Dist. LEXIS 75206, at *15 (D. N.H. July 14, 2006).

[61] Order of Default J., Permanent Inj. and Other Equitable Relief Against Sanford Wallace and Smartbot.net, Inc. at 16, Fed. Trade Comm'n v. Seismic Entm't, Inc., No. 04-377-JD (D.N.H. Mar. 22, 2006), *available at* http://www.ftc.gov/os/caselist/0423142/WallaceFinalJudgment.pdf.

[62] *See* New York v. Direct Revenue Petition, *supra* note 47, at 12.

[63] Compl. for Inj. and Other Equitable Relief at 4, Fed. Trade Comm'n v. Odysseus Mktg., Inc., No. 05-CV-330-SM (D.N.H. Sept. 21, 2005), *available at* http://www.ftc.gov/os/caselist/0423205/050929comp0423205.pdf.

[64] *Id.* at 2.

[65] *Id.* at 3.

"Add/Remove" function in the Microsoft Windows operating system was disabled in the code.[66] The instructions that defendants provided for uninstalling the program were extremely difficult for consumers to find, and did not work once a user located them.[67] The FTC alleged that failure to provide users with a reasonable means to locate and remove the program was an unfair act or practice in violation of Section 5 of the FTC Act.[68] Ultimately, the defendants agreed to a permanent injunction and a suspended penalty of $1.75 million.[69]

Programming revisions to Microsoft's Internet Explorer, such as upgrades and security patches, have helped prevent additional "drive-by" cases. Unfortunately, motivated marketers seem to find new programming tactics to which Microsoft and others are always reacting. For example, in 2008, the FTC moved to hold the *Odysseus Marketing* defendants in contempt based on violations of their injunction.[70] Allegedly, defendants have been diverting users of MySpace.com by downloading computer code onto their computers without their consent when the users navigate to the MySpace site.[71] Once diverted to different web sites, ads barraged the users, simply to earn advertising commissions.[72] This alleged contempt for the consent decree order suggests that the FTC's traditional anti-fraud enforcement and penalties may be insufficient to deter determined adware vendors.

A 2007 FTC case against ERG Ventures for distribution of its "Media Motor Application"[73] has many allegations of express

---

[66] *Id.* at 9.

[67] *Id.*

[68] *Id.* at 12.

[69] Stipulated Final Order for Permanent Inj. and Settlement of Claims for Monetary Relief at 8, Fed. Trade Comm'n v. Seismic Entm't, Inc., No. 04-377-JD (D.N.H. Oct. 20, 2006), *available at* http://www.ftc.gov/os/caselist/0423205/061121odysseusstipfinal.pdf.

[70] Pl.'s Mot. for an Order Holding Walter Rines, Online Turbo Merch., Inc., and Sanford Wallace in Civil Contempt for their Violations of this Ct.'s Permanent Inj., Fed. Trade Comm'n v. Odysseus Mktg. Inc., No. 05-CV-330-SM at 2 (D.N.H. filed Jan. 23, 2008), *available at* http://www.ftc.gov/os/caselist/0423205/080131motion.pdf.

[71] *Id.*

[72] *Id.*

[73] Compl. for Inj. and Other Equitable Relief, Fed. Trade Comm'n vs. ERG Ventures, LLC, No. 3:06-CV-00578-LRH-VPC (D. Nev. filed Oct. 30, 2006), *available at* http://www.ftc.gov/os/caselist/0623192/061030ergventurescmplt.pdf.

misstatements and deceptive nondisclosures similar to the complaints against *Enternet Media* and *Intermix*. Unlike those cases, however, the ERG complaint includes an allegation that the ad-generating software programs actually disabled at least two popular anti-spyware software programs: Lavasoft's Ad-Aware SE ("Ad-Aware") and Microsoft's Windows Defender.[74] In the case of Ad-Aware, the user's computer would shut down prior to completing the Ad-Aware scan. As a result, the Ad-Aware scan never fully ran and never removed any of ERG's ad-generating programs on the computer.[75] When the user would run Microsoft's Windows Defender, ERG's ad-generating software programs were added to the "Allow" list. As a result, Windows Defender would ignore those files in its scan and users would never be advised to remove them.[76]

These drive-by downloads and uninstall/reinstall tactics reflect issues beyond misstating or failing to disclose the exact nature of downloaded software. These cases include programming tactics that actually alter the computer users' existing software and computer settings. These tactics violate the FTC's basic enforcement tenet that a computer user's hardware is his or her own property that cannot be disrupted or violated simply because a software distributor can.[77] As mentioned above, the common law tort of trespass to chattels is one example of existing law that could address these tactics.[78] The basic claim of "unfair" business practices that the FTC and all state attorneys general can litigate also would seemingly be appropriate to combat these programming tactics that alter a computer user's existing software and computer settings. Notwithstanding applicable legal authority, however, the alleged contempt by the *Odysseus Marketing* defendants suggests that existing remedies against adware vendors may not suffice. New legislative strategies may need to include harsher penalties and cover more participants in the adware distribution channel to offset the financial incentives that keep these marketing tactics thriving.[79]

---

[74] *Id.* at 38.

[75] *Id.* at 39.

[76] *Id.* at 40.

[77] *See* Seismic Entm't Complaint, *supra* note 56.

[78] *See* Blanke, *supra* note 17, at 29 and accompanying text; Blakley, *supra* note 54, at 6.

[79] *See infra* notes 120–129 and accompanying text.

Finally, in New York's fraud case against *Intermix Media*, the state also alleged that the defendants' programs did not make the ad-generating software accessible in the "All Programs" or "Programs" list.[80] The programs were hidden in folders not usually associated with programs, were not listed in the "Add/Remove Programs" utility, nor was there any alternative uninstall utility for the software.[81] These allegations are programming choices that make the program inconvenient to access. Arguably, they do not affirmatively affect the individual's computer or program settings as the previous examples reflected. These programming inconveniences would not seem to rise to the level of deception.[82]

Presumably, if lawmakers believe consumers require legal protection against programmers who make it hard to uninstall their ad-generating code, a legislative response will be required. Current state spyware laws only prohibit *intentional deception* regarding installation and removal instructions.[83] Reasonable minds might differ on whether the inconvenience in finding a program to uninstall it would rise to the level of intentional deception. Proposed federal law would mandate uninstall instructions for all downloaded ad-generating software.[84] This proposed federal approach avoids any conclusion about whether the installation process was intentionally deceptive and simply makes removal instructions part of mandated notices. Ad-generating code that does not include such an instruction or that does not uninstall pursuant to the instructions would properly be deemed "spyware" without any proof of the defendants' intent.

IV. SPYWARE ACTIONS BASED ON AD-GENERATING SOFTWARE THAT POSES AS ANTI-SPYWARE PROTECTION

Nothing would seem to be more flagrantly deceptive than infecting a computer with spyware under the guise of an offer to detect and

---

[80] Intermix Media Petition, *supra* note 41, at 24.

[81] *Id.* at 27.

[82] The claims against Intermix Media ultimately fall into the "*Uninstall/Reinstall*" category, because the program also reinstalled the ad-generating code after a user deleted it. *Id.* at 28.

[83] Edelman, *supra* note 4.

[84] H.R. 964, 110th Cong. § 2(a)(5) (2007).

eliminate spyware. Yet, that is the scenario in several cases brought by the FTC and state regulators.

In 2006, the FTC settled two suits against vendors of spyware detection programs for their deceptive claims that consumers' computers had been remotely scanned and spyware had been detected.[85] Consumers received pop-up and e-mail messages about the risks to their computers, as well as fake warnings purportedly generated by Internet Explorer or the Windows operating system.[86] Ultimately, consumers purchased products such as Spykiller and Spyware Assassin that generally failed to detect most spyware on infected computers.[87]

The vendors of Spykiller entered a settlement requiring payments of more than $900,000, as well as forfeiture of several luxury vehicles.[88] MaxTheater, the vendor of Spyware Assassin, agreed to pay $76,000 and is prohibited from all future marketing and sales of any anti-spyware software.[89]

In its first case under Washington's spyware-specific legislation, the state attorney general accused Secure Computer and three affiliate advertisers of marketing a product called Spyware Cleaner that falsely claimed computers were infected with spyware, and also accused Secure Computer and its affiliates of selling those consumers a program that claimed to remove it.[90] The program not only failed to

---

[85] Compl. for Inj. and Other Equitable Relief, Fed. Trade Comm'n v. Trustsoft, No. H 05 1905, (S.D. Tex. filed May 31, 2005) [hereinafter Fed. Trade Comm'n v. Trustsoft Complaint], *available at* http://www.ftc.gov/os/caselist/0523059/050623comp0523059.pdf; Compl. for Inj. and Other Equitable Relief, Fed. Trade Comm'n v. MaxTheater, No. 2:05-cv-00069-LRS (E.D. Wash. filed Mar. 11, 2005) [hereinafter Fed. Trade Comm'n v. MaxTheater Complaint], *available at* http://www.ftc.gov/os/caselist/0423213/050311comp0423213.pdf.

[86] Fed. Trade Comm'n v. Trustsoft Complaint, *supra* note 85, at 12–13; Fed. Trade Comm'n v. MaxTheater Complaint, *supra* note 85, at 9.

[87] Fed. Trade Comm'n v. Trustsoft Complaint, *supra* note 85, at 40; Fed. Trade Comm'n v. MaxTheater Complaint, *supra* note 85, at 21.

[88] Final Stipulated Order for Permanent Inj. and Monetary J., Fed. Trade Comm'n v. Trustsoft, No. H 05 1905 at 7, 11–12 (S.D. Tex. Jan. 5, 2006), *available at* http://www.ftc.gov/os/caselist/0523059/060104trustsoftfinalorder.pdf.

[89] Stipulated Final Order for Permanent Inj. and Other Equitable Relief. Fed. Trade Comm'n v. MaxTheater, No. 2:05-cv-00069-LRS at 6–8 (E.D. Wash. Dec. 6, 2005), *available at* http://www.ftc.gov/os/caselist/0423213/051206maxtheaterfinalorder.pdf.

[90] Compl. for Inj. and Additional Relief, State of Washington v. Secure Computer LLC, No. C06-0126 at 8.11 (W.D. Wa. filed Jan. 24, 2006) [hereinafter State of Washington v. Secure

detect most spyware programs, but also rendered computers more susceptible to attacks by tampering with the user's security settings.[91]

The Washington spyware statute specifically prohibits installing software on a computer by intentionally misrepresenting to the computer owner that the software is necessary for security.[92] The complaint included alleged violations of the federal CAN-SPAM Act, the Washington Unsolicited E-mail Act, and Washington's Computer Spyware Act.[93] The state entered consent decrees with most of the defendants and imposed fines totaling $1 million dollars.[94]

Washington settled similar complaints against QuickShield and Spyware Slayer for much smaller amounts.[95] A 2007 case is still pending against several defendants for products marketed as Registry Sweeper Pro, Registry Rinse, Registry Doc, Registry Cleaner, and Registry Cleaner Pro.[96]

Of these cases against vendors of spyware-detection programs, only the *Secure Computer* case in Washington includes a claim that the downloaded product interacted with users' computers in a detrimental manner. The rest of the cases against vendors of spyware-detection programs reflect classic deceptive advertising claims, such as telling consumers they need a product when they do not. Those allegedly deceptive ads were not triggered by downloaded software that took up processor or hard drive space and/or were difficult to remove. Instead, the deceptive ads were embedded in certain

---

Computer LLC Complaint], *available at* http://www.atg.wa.gov/uploadedFiles/Another/News/Press_Releases/2006/Complaint.pdf.

[91] *Id.* at 8.18.

[92] WASH. REV. CODE § 19.207.040(1) (2007).

[93] State of Washington v. Secure Computer LLC Complaint, *supra* note 90, at 6.5, 6.9, 6.13, 6.17, 6.21, 6.22, 6.26, 6.27, 7.3, 7.6, 8.8, 8.13, 8.21, 9.3, 9.6, 9.9, 9.12, 9.15, 9.18, 9.24, 9.28.

[94] Consent Decree as to Defs. Secure Computer LLC and Paul Burke, State of Washington v. Secure Computer LLC, No. 07-2-04987-8SEA at 1 (W.D. Wa. Nov. 30, 2006), *available at* http://www.atg.wa.gov/uploadedFiles/Home/News/Press_Releases/2007/SecureLinkComplaint020707.pdf.

[95] Edelman, *supra* note 4.

[96] Compl. for Inj. and Additional Relief, State of Washington v. SecureLink Networks LLC, No. 07-2-04987-8SEA (King County Super. Ct. filed Feb. 7, 2007), *available at* http://www.atg.wa.gov/uploadedFiles/Home/News/Press_Releases/2007/SecureLinkComplaint020707.pdf.

websites. The transactions included downloaded software, but that is the only similarity to the other regulatory "spyware" cases. These cases of ad-generating software that pose as anti-spyware protection programs reflect nothing new or different in deceptive advertising law and require no new legislative response.

V. MOVIELAND.COM ACTIONS

The recent federal and state cases against Movieland.com are further examples of express misstatements and nondisclosure. The facts are unique, however, in that the ad-generating software itself made the misstatements about consumers' supposed contractual obligations to the defendants.

Washington and the FTC pursued actions against multiple defendants regarding a movie download service promoted through websites such as movieland.com, moviepass.tv, and popcorn.net.[97] The FTC acted under its traditional authority against deceptive and unfair trade practices.[98] Washington sued under its spyware-specific legislation.[99]

The defendants' putative business is an Internet download subscription service that provides access to news, sports, games, and adult content.[100] Their websites offered consumers a free three-day trial of the services. Consumers who accepted the free trial downloaded a "download manager" that would provide access to the content. Unbeknownst to computer users, however, billing software was also downloaded onto their computers. After the trial period, the defendants could remotely activate the billing software, causing a pop-up window to appear that stated the trial period had expired. A

---

[97] *See infra* footnotes 98–99.

[98] Compl. for Permanent Inj. and Other Equitable Relief, Fed. Trade Comm'n v. Digital Enters., No. CV-06-4923 at 47 (C.D. Ca. filed Aug. 8, 2006) [hereinafter Fed. Trade Comm'n v. Digital Enters. Complaint], *available at* http://www.ftc.gov/os/caselist/0623008/060808movielandcmplt.pdf.

[99] Compl. for Inj. Relief, State of Washington v. Digital Enters., No. 06-2-26030-9SEA at 6.1–12.1 (King County Super. Ct. filed Aug. 4, 2006) [hereinafter State of Washington v. Digital Enters. Complaint], *available at* http://www.atg.wa.gov/uploadedFiles/Another/News/Press_Releases/2006/MovielandComplaint8-14-06.pdf.

[100] *See* Movieland, http://www.movieland.com (last visited Feb. 2, 2009).

"Continue" link on the pop-up led consumers to a forty-second video that recurred hourly.[101]

The statements in the video constituted the alleged misstatements in both the federal and state complaints.[102] Consumers were told they were legally obligated to purchase a subscription. A separate statement on the company's website also asserted that failure to pay "may result in an escalation of collection proceedings that could have an adverse effect on your credit status."[103] The FTC characterized the marketing tactic as an anonymous free trial with a negative option feature.[104]

Contrary to the defendants' statements, consumers had no legal obligation after the free trial ended. The defendants had no ability to carry out the stated threats about collection proceedings and credit ratings because they had no personal information identifying the consumers at that point. However, the defendants' downloaded software had the ability to harass the computer user in a way that traditional debt collectors could only dream about! Because the software was so difficult to remove, many frustrated consumers ultimately paid between $19.95 and $80 for the movie subscription service just to stop the threatening pop-up videos.[105]

In this case, the Washington attorney general relied on prohibitions in Washington's Computer Spyware Act against installing software on a computer without a user's consent, taking control of a user's computer, and interfering with the user's ability to identify and remove that software.[106] As in all the foregoing examples, the FTC

---

[101] *See* Fed. Trade Comm'n v. Digital Enters. Complaint, *supra* note 98, at 25–30; State of Washington v. Digital Enters. Complaint, *supra* note 99, at 6.3–6.7.

[102] Fed. Trade Comm'n v. Digital Enters. Complaint, *supra* note 98, at 48–50; State of Washington v. Digital Enters. Complaint, *supra* note 99, at 9.2.2.

[103] Fed. Trade Comm'n v. Digital Enters. Complaint, *supra* note 98, at 30.

[104] The paradox in this characterization is that negative option marketing is based on a *subscriber relationship* between a book club or CD club, for example, that sends its subscribers periodic notices of the item they will receive if they do not decline it. Anonymity defies the underlying premise of negative option marketing: the customer can be sent the product and billed for it because they agreed to such a transaction in the original subscription. Mark Huffman, *Negative Option: When No Means Yes,* CONSUMERAFFAIRS.COM, Nov. 7, 2005, http://www.consumeraffairs.com/news04/2005/negative_option.html.

[105] Fed. Trade Comm'n v. Digital Enters. Complaint, *supra* note 98, at 37.

[106] WASH. REV. CODE §§ 19.270.020(4), 19.270.040(1) (2007).

relied on its general authority against unfair and deceptive trade practices.

Washington settled its case against the defendants for $50,000,[107] and the FTC settled its case for just over $500,000.[108] In both orders, the defendants agreed to discontinue *anonymous* free trials but can continue to offer and collect payment for the subscription service with downloaded software.[109] Both orders require proper disclosure of all software to be downloaded in conjunction with future contracts for the service,[110] as well as proper consent from the computer owner.[111] Many of the particulars regarding disclosures and other future software practices are identical in the federal and state orders.[112] Both orders require proper control of affiliates to ensure compliance with the consent decrees.[113]

Of course, the major difference is that the FTC has the power to enforce its order throughout the United States, while the Washington Attorney General is confined to his state. Accordingly, the FTC ordered the defendants to terminate any recurring billing of consumers who had enrolled after a free trial but were not continuing to use the service.[114] Presumably, this order was intended to protect

---

[107] Stipulated Agreement and Order, State of Washington v. Digital Enters., No. 06-2-26030-9SEA at 1.3 (King County Super. Ct. Apr. 19, 2007) [hereinafter Digital Enterprise Stipulated Agreement], *available at* http://www.atg.wa.gov/uploadedFiles/Home/News/Press_Releases/2007/MovielandStipulatedAgreementOrder041907.pdf.

[108] Settlement Agreement and Stipulated Final Order, Fed. Trade Comm'n v. Digital Enters., No. CV-06-4923 at 13 (C.D. Ca. Sept. 11, 2007) [hereinafter Digital Enterprise Settlement], *available at* http://www.ftc.gov/os/caselist/0623008/070905digitalenterprisesstipfnl.pdf.

[109] *See* Digital Enterprise Stipulated Agreement, *supra* note 107, at 3.3; *See also* Digital Enterprise Settlement, *supra* note 108, at 5.

[110] *See* Digital Enterprise Stipulated Agreement, *supra* note 107, at 3.5; *See also* Digital Enterprise Settlement, *supra* note 108, at 6–7.

[111] *See* Digital Enterprise Stipulated Agreement, *supra* note 107, at 3.6; *See also* Digital Enterprise Settlement, *supra* note 108, at 8.

[112] *See, e.g.*, Digital Enterprise Stipulated Agreement, *supra* note 107, ¶ 3.7; *See also* Digital Enterprise Settlement, *supra* note 108, at 9–11.

[113] *See* Digital Enterprise Stipulated Agreement, *supra* note 107, at 3.8–3.10; *See also* Digital Enterprise Settlement, *supra* note 108, at 11–12.

[114] *See* Digital Enterprise Settlement, *supra* note 108, at 14.

individuals who had ordered the service just to break the cycle of pop-up ads rather than actually using the service. The FTC also ordered the defendants to post instructions on its various websites for removing any of its software from a user's computer.[115] The same instructions must also be e-mailed to customers who paid for the service.[116] Such an order under the Washington law could only apply to Washington residents.

The Washington settlement money will be distributed to Washington citizens who are eligible for a refund.[117] The federal settlement is for "consumer redress,"[118] and thus the defendants must provide the FTC with the names and contact information of consumers who are eligible for a refund.

As noted above, these settlement agreements do not reflect any legal conclusions by a court about the alleged wrongdoing and the exact violations of law they reflect. Washington's Attorney General is proud that his state is "leading the battle against online fraud."[119] Nevertheless, the Movieland.com case does not suggest that special spyware-specific legislation is necessary to address fraudulent misstatements or nondisclosure simply because the fraud is perpetrated using programming tactics. The FTC and Washington asserted claims against the same defendants based on identical behavior. Both regulators alleged that the software-generated statements falsely represented consumers' actual obligations. The FTC settled its case under long-held authority to regulate false and misleading advertising, a power every state attorney general also holds. Accordingly, the unique programming tactics and the fraud perpetrated by these defendants using software did not require any new or special authority to regulate.

---

[115] *Id.* at 16.

[116] *Id.*

[117] Press Release, Attorney General McKenna Settles with Movieland.com and Associates Concerning Pop-Up Payment Demands (Apr. 19, 2007), *available at* http://www.atg.wa.gov/pressrelease.aspx?&id=14480.

[118] *See* Digital Enterprise Settlement, *supra* note 108, at 13.

[119] Press Release, McKenna Announces Fifth Computer Spyware Case; Washington Sues Three Internet Affiliate Advertisers (Feb. 7, 2007), *available at* http://www.atg.wa.gov/pressrelease.aspx?id=12328.

VI. LEGISLATIVE RECOMMENDATIONS

Clearly, the Washington Attorney General feels empowered by his state's spyware statute. However, ten other states have spyware-specific legislation and they are not showing the same activism as Washington. Nothing in these case studies suggests that Washington's spyware-specific legislation has made prosecution of the cases easier or resulted in better consumer protection than traditional anti-fraud prosecutions by the FTC or by New York.

A consent decree, however, is not the same as a trial verdict or an appellate decision. What the current federal and state law could impose on an unwilling defendant may be somewhat different. If the types of cases discussed herein were pursued all the way through to a decision by an appellate court, the regulators may encounter two separate legal roadblocks under existing law. The first is the EULA.

The *Odysseus Advertising*, *Direct Revenue*, and *ERG* cases discussed above all included complaints that notices to computer users were not readily available or clear enough to adequately disclose the existence of ad-generating software to be downloaded.[120] In some cases, the consumer had to link to a separate website to find any information about the true nature of what was being downloaded. In other cases, a notice was buried deep in lengthy legalese. The reader was not required to navigate to the relevant information about the ad-generating code in order to download the sought-after product. Regulators alleged that these notices amounted to unfair and deceptive trade practices.

Traditional contract law may deem a contract unconscionable and unenforceable based on factors such as unfair surprise, lack of notice, and disparity of bargaining power.[121] Such concepts could apply to notices buried in lengthy online agreements or linked through many websites. Accordingly, existing common law and regulatory authority could suffice to protect consumers against overly-dense or circuitous EULAs that regulators characterize as unfair trade practices.

On the other hand, courts have held that "click through" web agreements are binding on consumers.[122] These results cast doubt on

---

[120] *See supra* notes 63–84 and accompanying text.

[121] Dawn Davidson, *Click and Commit: What Terms are Consumers Bound to When They Enter Web Sites*, 26 WM. MITCHELL L. REV. 1171, 1196 (2000).

[122] Lydia J. Wilhelmi, *Ensuring Enforceability: How Online Businesses Can Best Protect Themselves from Consumer Litigation*, 86 MARQ. L. REV. 181, 197 (2002).

whether the FTC and state regulators could get judgments in cases where the alleged deception was a lengthy EULA that did not prominently disclose to consumers that ad-generating software was being downloaded.

Further, current state spyware-specific statutes do not address the issue of inadequate disclosure or appropriate notice.[123] Accordingly, this is one area in which new federal legislation would be appropriate. Federal law could mandate national online disclosure protocols. States could remain empowered to enforce that law along with provisions of their own state spyware laws that do not conflict with such a federal notice law.

The next stumbling block in existing law that could impede legal control of spyware is control of the "affiliate" ad distribution network. As discussed above, the Internet advertising model is facilitated by a vast web of parties who distribute the ad-generating software by programming it into many downloadable products. These affiliates are usually paid "per impression," so they are motivated to load the ad-generating code in a vast number of locations online.[124] Most of the consent decrees in the foregoing cases call for the defendants to control these affiliates to insure compliance with the consent decrees.

Current common law of agency and contracts usually does not impose liability on vendors when their independent contractors deceptively distribute a product like those discussed above. Further, as explained above, only a few existing state spyware laws impose liability for "conscious avoidance" of knowledge about prohibited downloads.[125] This is the closest that current law comes to binding an adware vendor for acts within their affiliate distribution channel. Unfortunately, this "conscious avoidance" standard requires proof that the vendor turned a blind eye to the unlawful acts of an affiliate, which may be difficult to prove in many far-flung adware distribution networks.

A better legislative approach would be to impose an affirmative duty on adware vendors to control the distribution of their software. This approach could actually reign in mass online distribution of unwanted ad-generating software. Federal law should create this

---

[123] Benjamin Edelman, *California's Toothless Spyware Law*, Sept. 29, 2004, http://www.benedelman.org/news/092904-1.html.

[124] *See supra* notes 17–29 and accompanying text.

[125] *See, e.g.*, Consumer Prot. Against Computer Spyware Act, S.B. 1436, 2003–2004 Sess. § 2(32)(22947.2)–(22947.3) (Ca. 2004), *available at* http://pub.bna.com/eclr/sb1436.htm.

duty, similar to what defendants have agreed to in the foregoing consent decrees. State attorneys general should be empowered to enforce this federal standard, along with the FTC.

A similar duty could be imposed on all advertisers for the harm caused by the deceptive distribution of their ads on the Internet. In 2007, the state of New York entered into consent decrees with Cingular Wireless (now AT&T), Travelocity, and Priceline for their ads that were delivered through adware distributed by Direct Revenue. The New York attorney general accused these advertisers of deception because they had "turned a blind" eye to the deceptive practices of their adware vendor.[126] This was the first enforcement action against buyers of Internet advertising. All defendants agreed to a series of controls over future Internet advertising such as full disclosure of the presence of ad-code, meaningful consent, practicable removal, and prominent branding.[127] The settlement imposes due diligence of the advertising over future Internet advertising contracts to investigate and control how their advertising is delivered.[128] Defendants Cingular and Priceline agreed to pay $35,000 and Travelocity agreed to pay $30,000.[129]

Finally, the most dramatic step would be to impose strict liability on all advertisers and adware vendors for deceptive distribution of ad-generating software, regardless of due diligence. This would be comparable to strict products liability imposed on all sellers in the chain of distribution for defective products that cause personal injury. This step should be the last legal resort if the deceptive spyware distribution problem is not curtailed by other legal strategies discussed above. Further, before such strict liability could be imposed, a standard beyond "deceptive" or "unfair" would need to be established for what programming behaviors triggered the liability. Such a standard would have to include the disclosure mandates and other notice mandates discussed above.

---

[126] Office of the Att'y Gen., *Groundbreaking Settlements Hold Advertisers Responsible for Displaying Ads Through Deceptively Installed "Adware" Programs*, Jan. 29, 2007, http://www.oag.state.ny.us/media_center/2007/jan/jan29b_07.html.

[127] *Id.*

[128] *Id.*

[129] *Id.*

CONCLUSION

Numerous cases have been litigated between adware vendors and makers of anti-spyware scanning programs for alleged defamation by including "legitimate" adware in a spyware scan. [130] Securities regulation cases hinge on whether adware vendors have misled investors when they did not discuss in company disclosures the possible implication of pending "spyware" legislation. [131] Federal legislation needs to end this confusion and dictate once and for all what products are categorized as offending "spyware." A bright line needs to be drawn between legitimate ad-generating software that keeps the price of sought-after online content down (or free) and products that frustrate computer users and make them wish they had never encountered the vendor's products.

That line should be based on new federal notice requirements discussed above that any ad-generating program either meets or does not. Research on the best notice protocols should drive that federal legislation and rulemaking. [132] This bright defining line in a new federal law should also rely on trends in current state spyware-specific laws against changing computer settings and uninstall capabilities. Code that does not provide and respond to clear and easy removal instructions would be labeled spyware. The FTC should be empowered to continually update and revise these definitions as technology evolves.

By contrast, "spyware" is not the appropriate characterization for any and all examples of online false advertising regarding downloaded software. The definition of spyware should not include cases of purchased software that do not perform as promised, including spyware removal programs, *unless* the programs include damaging code that denies the computer user control over the machine. Traditional false advertising and warranty law should be left to handle cases of buyers' remorse for products that do not perform as promised. Computer users must accept that online purchases of downloaded content require the same scrutiny as any other products that buyers might introduce into their homes or offices.

---

[130] Benjamin Edelman, *Threats against Spyware Detectors, Removers, and Critics*, http://www.benedelman.org/spyware/threats (last updated Sept. 20, 2007).

[131] In re Miva, Inc., Sec. Litig., 511 F. Supp. 2d. 1242 (M.D. Fla. 2007); In re Navarre Corp. Sec. Litig., 2006 U.S. Dist. LEXIS 92604 (D. Minn. 2006).

[132] *See, e.g.*, Blanke, *supra* note 17; Good et al., *supra* note 17.

Nothing in future federal spyware legislation should prevent state enforcement. In *Pike v. Bruce Church,* the U.S. Supreme Court established a two-part test to determine if a state law imposes an undue burden on interstate commerce.[133] First, the state must assert a legitimate state interest for its regulation. The problems with spyware discussed above easily satisfy this requirement.[134] Then the state statutory burden on interstate commerce is weighed against the local benefit derived from the state law.[135] The Washington and New York prosecutions reveal enforcement that is nearly identical to the FTC's. Accordingly, compliance with existing or new state spyware legislation does not impose the kind of undue burden on interstate commerce that would justify preemption of state spyware laws.

Nothing about the problems with spyware distribution are insurmountable. Existing federal and state authority needs to be bolstered with federal legislation to clarify the offending behaviors and impose duties on those at the top of the ad distribution channel.

---

[133] Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).

[134] *See supra* notes 8–11 and accompanying text.

[135] *Pike*, 397 U.S. at 142.