

Spyware Update: Revenue Sources, Installations, Litigation, and the Future

1 message

Ben Edelman <edelman@law.harvard.edu>

Mon, Apr 10, 2006 at 3:17 PM

To: kevin@techlawadvisor.com

Greetings, and thanks for requesting updates on my research. Today's newsletter is a four-part piece on spyware -- focusing on revenue sources, installation methods, litigation, and the future of the spyware industry. Details below.

Revenue Sources

Spyware vendors are under attack. Advertisers have learned that spyware is unwanted -- that users hate the extra pop-up ads, and that policy-makers intend to hold advertisers accountable for their advertising decisions. (1, 2) So these days spyware vendors face an uphill battle in selling ads directly to advertisers. Instead, spyware vendors often sell ads to intermediaries -- ad agencies, ad networks, affiliates, banner-farms, and other middle-men -- which in turn build relationships with advertisers. Examples from my files:

- *Syndicated pay-per-click ads.* In the "best" case, a spyware vendor shows a list of pay-per-click ads, and an advertiser pays the PPC search engine if a user clicks that advertiser's ad. But in practice even these "ideal" relationships work out badly: PPC ads are shown in annoying spyware-delivered popups; popups target a merchant with *its own* ads (like "click here to save even more at Dell" when the user is already at the Dell site); PPC ads lack the labeling required by [FTC instructions](#). Many spyware placements of PPC ads are even worse. It's not unusual to see spyware performing click fraud -- faking clicks (and charging advertisers for clicks) that never actually took place. I've also seen spyware unilaterally inserting links into others' sites, and sending such traffic to pay-per-click search engines.

In my analysis Yahoo has the deepest, most frequent, and most convoluted relationships with spyware vendors. But spyware-delivered click fraud is rampant at FindWhat (Miva), Kanoodle, LookSmart, and Marchex. At Google, bad syndication is increasingly frequent. Details: [The Spyware - Click-Fraud Connection -- and Yahoo's Role Revisited, How Yahoo Funds Spyware](#).

- *Affiliates.* "Affiliate programs" are supposed to entail third parties sending merchants bona fide leads -- new customers not already on a merchant's site. But when a spyware vendor sends traffic to an affiliate network, the spyware vendor intends to appear to have delivered a customer to a merchant, when in fact the customer found the merchant *on his own*, without assistance. So this tactic often gives advertisers no real value -- but advertisers can't protect themselves if they don't even realize they're being cheated. Details: [How Affiliate Programs Fund Spyware](#).
- *Other ad syndication and ad networks.* Most online advertising methods turn out to be susceptible to syndication attacks: An advertiser buys an ad from an ad network, but the ad network syndicates that ad to other networks, which place it with their partners and associates ad infinitum. Soon no one knows where or how the advertiser's ad is being shown. The inevitable consequence? The ad appears in spyware-delivered pop-ups. Details: [Intermediaries' Role in the Spyware Mess](#). More to come.

In my view, online advertising need not suffer these problems. Ad networks do require many ads from many advertisers, to be shown on many web sites. But ad networks don't have to allow ad syndication -- where an ad from one network gets copied into another, then another and another in a lengthy and convoluted chain. The better policy, in my view, is a "no syndication" rule -- which improves accountability and simplifies investigations.

Meanwhile, online advertisers are being defrauded by their affiliates and, in many cases, their ad networks. Advertisers contract for one kind of advertising (e.g. ads shown on legitimate web sites), but receive something else (e.g. ads shown in spyware) generally worth far less. On some level this is a problem for advertisers more than consumers: Advertisers, not consumers, directly pay the resulting costs. But when advertisers pay spyware vendors, directly or indirectly, consumers lose out too: These payments let spyware vendors buy and bundle installations to get onto users' computers. That's all the more reason for advertisers to carefully consider where their money goes.

Of course some advertisers still buy ads directly from spyware vendors. I recently reported dozens of [advertisers funding](#)

[180solutions](#) and [Direct Revenue](#). Though some of these ads came through intermediaries (especially Adrevolver, Directtrack, LinkShare, Metareward, Mygeek, and Yfdirect), many of these advertisers bought their ads directly from the spyware vendors.

The online travel industry has long been among the most aggressive buyers of spyware-delivered ads. Last fall I posted [How Expedia Funds Spyware](#), showing Expedia ads appearing through 180solutions, Direct Revenue, and eXact Advertising. To its credit, Expedia subsequently abandoned this advertising channel. But other travel sites are slow to follow. A recent policy from the Interactive Travel Services Association takes an unfortunate step in the wrong direction: ITSA generally endorses advertising software, which it says "provides timely, relevant, and money-saving information." ITSA provides only weak rules for "adware" vendors to satisfy; predictably, ITSA members continue to fund the most notorious spyware. For example, ITSA members Cendant (owner of Howard Johnson and Super 8), Cheap Tickets, and Travelocity all still advertise with Direct Revenue, while Travelocity and Orbitz advertise with Hotbar. Details: [Critiquing ITSA's Pro-Adware Policy](#).

Installation Methods

Spyware vendors know their historic installation methods haven't been good enough. But what *is* good enough? I recently critiqued 180solutions' newest installation methods, as shown at the kids site [Dollidol.com](#). 180 discloses the presence of bundled advertising software in an off-screen footer without scroll bars; fails to disclose that 180's ads are shown in pop-ups; fails to disclose the privacy consequences of installing 180's software; shows a license agreement in an oddly-shaped window that discourages careful review; and uses misleading button labels to encourage installation. A user may ultimately press "Finish," but the user can't reasonably be said to have known what he was (purportedly) accepting.

Details: [180solutions's Misleading Installation Methods - Dollidol.com](#).

And nonconsensual installations continue. For example, I recently documented a distributor that was placing 180solutions' software onto users' computers without their consent -- months after 180 [told](#) the world this was impossible. ("Installation cannot continue until the user gives consent"). Through a security exploit, this installer bombarded users with an incredible mess of spyware: 180solutions, Ad-w-a-r-e, Adservs, Integrated Search Technologies, Internet Optimizer, Media Tickets, [New.net](#), Quicklinks, Surfsidekick, Tagasaurus, Targetsaver, Toolbar888, Ucmore, Webhancer, Web Nexus, WinFixer, and more. Details (including screen-capture video of the installation): [Nonconsensual 180 Installations Continue, Despite 180's "S3" Screen](#).

But run-of-the-mill trickery remains the standard method of infecting users with spyware. As usual Claria leads the pack -- by conveniently [dropping](#) the phrase "pop-ups" from its ActiveX disclosures. I'm also concerned about lousy results at search engines: Search for "screensavers," "smileys," or "wallpaper" (among many other terms), and top results at Google and Yahoo inevitably include lots of software most experts call spyware. Details: [Pushing Spyware through Search](#).

One way to protect consumers from this trickery: Warn them before they install something they'll likely later regret. [SiteAdvisor](#) does the job: Their robots crawl the web looking for downloads; robots install each program they find, then check for spyware. SiteAdvisor's free browser plug-in notifies users before they download a risky program -- and also sends alerts before users take other unwise actions, like registering with sites previously found to bombard SiteAdvisor with excess email. Details: [Deciding Who To Trust](#). Note: I serve on SiteAdvisor's board of advisors.

Litigation

After a multi-year investigation, the New York Attorney General has filed suit against Direct Revenue. In a detailed complaint, the NYAG alleged Direct Revenue surreptitiously installed spyware onto users' computers and made its spyware exceptionally difficult to remove. The suit includes claims under New York's General Business Law (prohibiting false advertising and deceptive business practices), New York's Penal Law (prohibiting computer tampering), and New York's common law prohibitions against trespass. I obtained more than 2,000 pages of exhibits from the NYAG's filings, and I have [organized and summarized these documents](#) on my site. See also my listing of [exceptional documents](#) -- revenues, profits, partners, advertisers, and complaints, as well as threats to critics.

I am aware of ongoing consumer class action litigation against 180solutions, Direct Revenue, eXact Advertising, and Intermix. [Details](#). More to come? There are certainly plenty of other identifiable US-based companies whose unwanted advertising software has been installed without consent, or without informed consent.

The Future of the Spyware Business

Last month Claria [announced](#) its exit from the spyware business. ClickZ [reports](#) that Claria will sell the software tools that previously came bundled with Claria's GAIN pop-up ads -- screensavers, smileys, etc. But it seems Claria intends to shut down the GAIN advertising system and "build its PersonalWeb user base from scratch."

Despite this apparent change of heart, there's still plenty to dislike about Claria. After all, Claria [invented](#) the ActiveX drive-by download. And Claria pioneered covering web sites with their competitors' ads. Nothing to be proud of!

But at this point, shutting down GAIN is the right decision. It's surely the only way to attempt to legitimize Claria's business going forward.

For other spyware vendors, Claria's transition signals increasingly unfavorable economics. Direct Revenue may have boasted a [66% profit margin](#) in 2004, but these days spyware vendors face growing challenges. Savvy advertisers won't buy spyware-delivered ads; security companies are increasingly sophisticated at removing spyware from users' PCs; and regulators are catching on and taking action. Users may sometimes press "yes" in an installation screen, but in practice they "accept" without fully understanding the consequences. With all these challenges, can a spyware company still make money by sneaking onto users' computers, tracking where users go, and covering web sites with competitors' pop-ups? Perhaps not. That's too bad for spyware makers, but it's great news for users.

Future Updates

Let me conclude with an apology. I've updated my site repeatedly in the past 6 months, but I haven't sent a message to this list since September 2005. I always hesitate to send out mass emails; in this era of overflowing inboxes, I hate to add more to the pile. Yet I gather many of you actually want to hear from me more often.

Realistically, I can't promise more frequent email updates. But for fastest notice of additions to my site, consider subscribing to my RSS feed. The RSS sign-up link is [on the front of my site](#), and any standard RSS reader will keep you updated automatically. Need to learn more about RSS? Send me an email for pointers, or check out articles: [c|net introduction](#), [blogspace suggestions](#), [kbcfe reviews](#).

Questions? Puzzles? Suggestions? Just hit reply. I look forward to hearing from you.

Benjamin Edelman
www.benedelman.org

Want to receive no updates, fewer updates, or updates only on particular subjects? Just reply to this email, and I'll adjust your subscription accordingly.
