Authors Note: Following the initial publication of this report on March 20, 2006, several of the companies identified as having relationships with adware distributor 180solutions contacted the Center for Democracy & Technology (CDT) to offer more detailed information about their advertising policies and current practices. This version of the report reflects that updated information. For further information, or to obtain earlier versions of the report contact Alissa Cooper (**acooper@cdt.org**).

Following the Money:

How Advertising Dollars Encourage Nuisance and Harmful Adware and What Can be Done to Reverse the Trend

A Report by the Center for Democracy and Technology

May 2 2006 (Update)

Unwanted advertising software or "adware" has evolved from an annoyance into a serious threat to the future of Internet communication. Every day, thousands of Internet users are duped into downloading adware programs they neither want nor need. Once installed, the programs bog down computers' normal functions, deluging users with pop-up advertisements, creating privacy and security risks, and generally diminishing the quality of the online experience. Some users simply give up on the Internet altogether after their computers are rendered useless by the installation of dozens of unwanted programs.

One of the most troubling aspects of this phenomenon is that the companies fueling it are some of the largest, best-known companies in the world. In the following pages, the Center for Democracy & Technology (CDT) details how advertising dollars from major, legitimate companies are fueling the spread of nuisance and harmful adware[1] and how those companies can help to combat the online scourge by adopting and enforcing good advertising placement policies.

Adware's 'Dirty Little Secret'

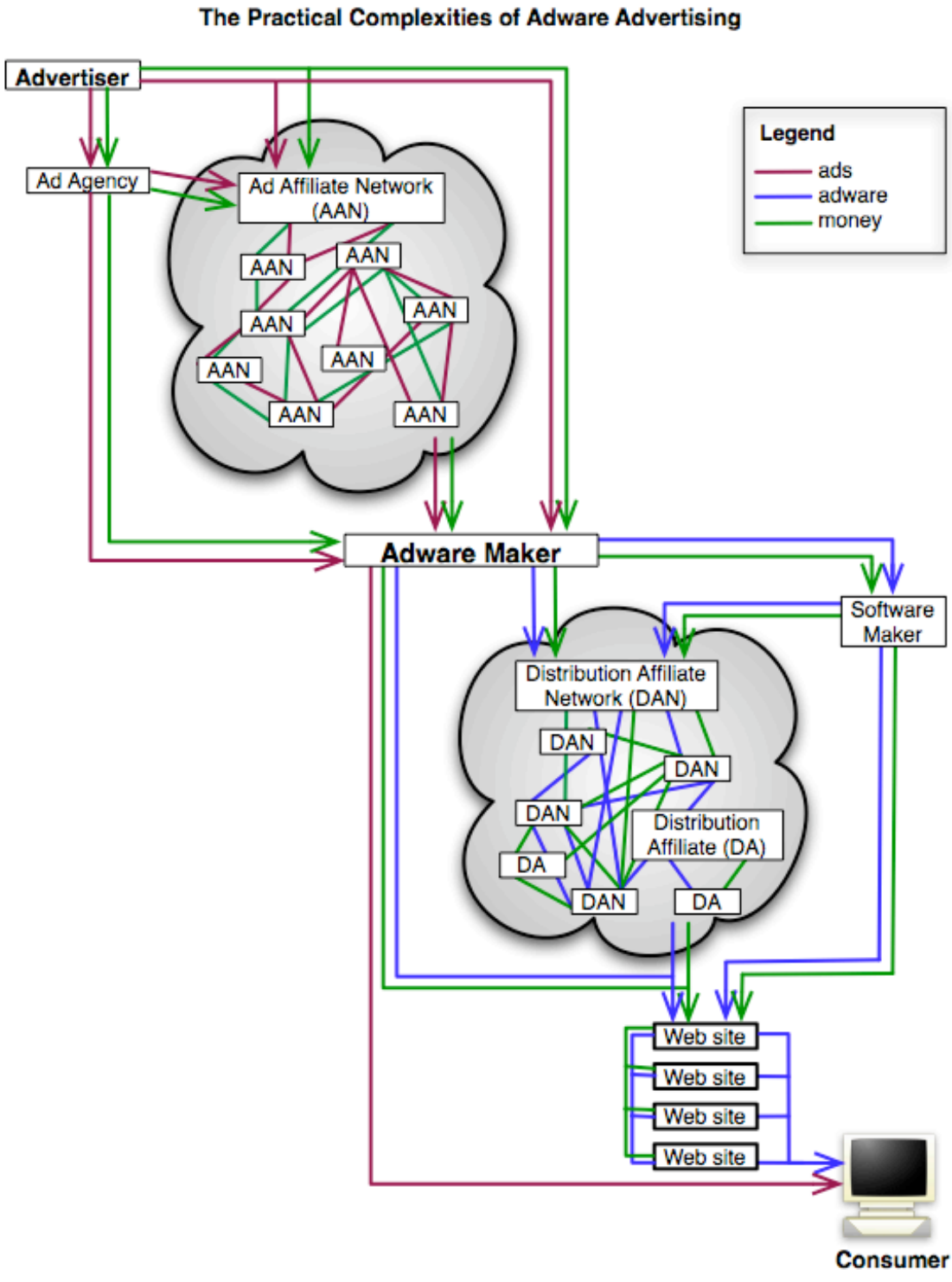
Speaking at the Anti-Spyware Coalition Public Workshop on February 9, 2006, FTC Commissioner Jonathan Leibowitz said that the "dirty little secret" about nuisance and harmful adware is that large, legitimate companies fuel the problem -- knowingly or not --

[1] This report addresses issues associated with nuisance or harmful adware and not with all adware in general. As defined by the Anti-Spyware Coalition (ASC), nuisance or harmful adware is advertising display software that may be a nuisance or impair productivity, display objectionable content, slow a machine down or cause crashes and loss of data, lack adequate removal tools, or may be associated with security risks (*see* http://www.antispywarecoalition.org/documents/definitions.htm). In this report we also consider software to be nuisance or harmful adware if it both meets the ASC definition for "adware" (*see* http://antispywarecoalition.org/documents/glossary.htm) and exhibits high risk factors for installation and distribution, as defined in the ASC Risk Model Description (*see* http://antispywarecoalition.org/documents/RiskModelDescription.htm).

by paying for their ads to be delivered by illegitimate adware programs. To consumers who have experienced the presence of nuisance or harmful adware on their computers, however, this is no secret at all—their browsing experiences are overrun with advertisements for companies that they recognize. Which begs the question: are brand-name companies wittingly delivering their ads via nuisance or harmful adware, or are they truly unaware that this is taking place? On the surface, the adware business model may appear simple, making it seem as though advertisers should have no difficulty monitoring and controlling the placement of their ads. The following diagram illustrates the business model that many adware companies purportedly use:

In theory, an advertiser makes a direct arrangement with an adware company, paying the adware maker each time a user clicks on one of the advertiser's ads. The adware companies in turn make arrangements with software distributors; adware gets bundled with the software, and distributors are paid each time a consumer installs the software-adware bundle. Consumers then view and click on ads while they surf the Web. In this scenario, it should be easy for advertisers to remain vigilant about the placement of their ads. Companies can investigate the adware makers' business practices before striking a deal with them; they can ask for the lists of software distributors that an adware maker uses; and they can monitor those distributors to ensure they follow best practices when distributing adware.

In practice, though, the adware business model is often far more complex than it appears in the diagram above. Although the simple scenario shown above does play out in some instances, there are often a host of other parties involved in the advertising chain, making it difficult to track the journey an advertisement takes from its original source to a user's computer. The following diagram illustrates the complexities of the real adware market:


The Practical Complexities of Adware Advertising
Advertiser
Ad Agency
Ad Affiliate Network (AAN)
AAN
AAN
AAN
AAN
AAN
AAN
AAN
AAN
Legend
ads
adware
money
Adware Maker
Software Maker
Distribution Affiliate Network (DAN)
DAN
DAN
DAN
Distribution Affiliate (DA)
DA
DAN
DA
Web site
Web site
Web site
Web site
Consumer

Many parties may be involved in getting an ad from an advertiser to a consumer. They include:

- **Advertisers**, the companies that pay for the ads. Advertisers may work both with ad agencies and advertising affiliate networks to get their ads placed. Some advertisers place ads directly with adware makers.
- **Ad agencies,** which are paid by advertisers to run marketing campaigns and place ads in multiple mediums. Ad agencies usually work with advertising affiliate networks to place ads online, but they may also work directly with adware makers.
- **Advertising affiliate networks (AANs)**, which charge companies to place their ads in many locations all over the Internet, including in banner ads, alongside search results, and as pop-ups or pop-unders generated by adware. An AAN may work directly with an adware maker, or it might work with other AANs. The latter arrangement can create a long chain of ad networks through which ads are passed. Some AANs also work in a "blind" fashion, such that their clients (advertisers) are not informed about where their ads are placed.[2]
- **Adware makers,** which create and distribute adware. Any party interested in placing ads (i.e., advertisers, ad agencies, or ad networks) can pay adware makers to enter ads into the rotation displayed by the adware programs.
- **Software makers,** which are able to offer their software to consumers free of charge because they get paid by adware makers to include adware as part of the software bundle. These kinds of software makers can distribute their software through the same channels as those available to adware makers: distribution affiliate networks, distribution affiliates, and/or Web sites.
- **Distribution affiliates (DAs)**, which help to distribute adware and other software through Web sites. For example, a Web hosting company might offer free hosting services to Web sites that agree to distribute adware on their hosted sites. DAs may work directly with Web sites or with other DAs for software distribution.
- **Distribution affiliate networks (DANs)**, which get paid by adware and other software makers to find outlets for distributing adware and the software that it is bundled with. DANs may work directly with Web sites or distribution affiliates, or they may work with each other to form chains of distribution networks.
- **Web sites** that distribute adware programs and other software. Consumers who visit these sites can download the programs directly to their computers. A Web site may work with other Web sites to deliver software, thus forming a chain of sites through which software gets distributed.

---

[2] The "advertising affiliate network" category used in this report actually encompasses a broad range of entities that advertisers engage with and that engage with each other to place ads. The category consists of both entities that physically route ads and others that are merely ad brokers; it ranges from networks that use a closed set of ad placement sites to those that operate on a pay-per-performance model. There are also various "levels" of ad networks that serve different functions along the chain. These distinctions were made more clearly in a diagram CDT previously published (*see* http://cdt.org/headlines/776), but are omitted here for the sake of simplicity. We would like to thank David Eastbrook from Hurricane Media and Robert Gratchner from aQuantive for helping us to better understand these networks.

- **Consumers** who visit Web sites that distribute adware or software bundled with adware.

This complicated network of relationships can make it difficult for advertisers to know where their ads are being delivered. A typical scenario looks like this: Company X hires an ad agency to run its advertising campaign. This ad agency then searches for places to show ads online, and it makes a deal with a blind ad network to show a Company X advertisement 1000 times for $5 (the display of an ad is known as an "impression"). The blind ad network already has an arrangement with another ad network for 1000 impressions for $4.50, and that network has a deal with yet another network to show 1000 impressions for $4. The last ad network in the chain has a deal with an adware maker for 1000 impressions for $3.50.

Under this all-too-common scenario, the adware maker has a major incentive to get its software distributed as widely as possible, because the more ads it can display, the more profit it makes. Assume that it pays a distribution affiliate network 40 cents every time a consumer downloads the adware. That distribution network pays another network 20 cents per download, and that network pays a Web site 10 cents every time a user downloads the adware from the site. The Web site owner then sets up its site so that the adware is downloaded onto users' computers without their consent. The Web site can do this without much risk of being caught by the adware maker, even if the adware maker intends to follow best practices for installation, because the chain from the adware maker to the site owner is long, and the adware maker may have dozens of other such relationships to monitor. It is even less likely that the advertiser will catch the Web site owner because the chain between the two is even longer and more complex, and in this example, the advertiser uses a blind network that prevents or discourages it from knowing how and where its ads are actually placed.

Once a consumer has had the adware program placed on his or her computer by the third party Web site, ads begin to appear as he or she browses the Web. The consumer will likely see a Company X ad, and (even if he or she clicks on the ad and lands on the Company X Web site) Company X will have no idea that the consumer was served the ad by a suspiciously-installed adware program because its only contact is with an ad agency that uses a blind ad network. The consumer will have no idea why Company X's ad appears on his or her computer because the Web site owner never gave adequate notice or asked for consent before installing the adware.

In these ways, a legitimate advertiser can unknowingly fuel the distribution of illegitimate adware by paying to place its ads.

In CDT's discussions with participants in the advertising space, it was suggested that many marketing professionals concern themselves more with the effectiveness of their ad campaigns than with the ramifications of where the ads are placed. Adware-delivered ads are likely to be particularly effective because they often appear in unusually intrusive formats (thereby getting consumers' attention and facilitating online purchases), and because they can target competitors' traffic (e.g., a consumer visiting a dating Web site

might be served an ad for a competing dating site). Although some industry members show concern for avoiding certain placement areas, such as pornographic Web sites, for the most part the focus of Internet ad campaigns is on the number of placements and clicks and not on how ad placement may injure the image of the brand in the long run.

As evidenced by the volume of ads being served by nuisance or harmful adware today, these priorities need to be changed. Advertisers must take the initiative by being more vigilant about where their ads end up and working to enforce rules that ensure that every party involved in the advertising chain refuses to work with deceptive and illegitimate affiliates.

Solution: Adoption and Enforcement of Advertising Placement Policies

Dozens of well-known companies are in a position to make an immediate impact on the problem of nuisance or harmful adware by evaporating its funding source. A vital step toward that goal is the adoption and enforcement of advertising placement policies by companies that advertise online.[3]

Several organizations have taken the lead in establishing policies that discourage or prohibit the use of nuisance or harmful adware in serving ads. Others have established strict standards that adware makers must meet. Organizations leading the way in addressing the adware problem include the Interactive Travel Services Association (ITSA), the Direct Marketing Association (DMA)[4], Major League Baseball, Dell, and Verizon.

In 2004, CDT found that travel Web sites were the subject of some of adware maker 180solutions' most numerous and blatant ads. The recently established ITSA policy allows advertising only with adware vendors that follow best practices in installation of adware, labeling of ads, and uninstall capabilities. The policy appears to have already made a significant impact. Since ITSA adopted the policy, 180solutions adware generates far fewer ads for travel sites. By CDT's estimation, 180solutions' software clearly fails to meet the ITSA standards.

Other organizations are working to set parameters for how adware should and should not behave. The recently announced TRUSTe Trusted Download Program[5] has already

---

[3] This report focuses on the role of advertisers in stemming the tide of nuisance and harmful adware, but the role of ad networks is also significant and the remedies are similar for both parties. CDT chose to emphasize advertisers' responsibility because the variety of forms that ad networks take and the complicated ways in which they interconnect make it difficult to address them here. We expect to address their role in a future report.

[4] The DMA recently introduced a new guideline dealing with the use of software in advertising in its Guidelines for Ethical Business Practice (*see Article #40 in* http://www.the-dma.org/guidelines/EthicsGuidelines.pdf). The DMA has also outlined steps that marketers can take to ensure compliance with the guideline (*see* http://multichannelmerchant.com/mag/keeping_tabs_internet_03012006/index.html).

[5] *See* http://truste.org/trusteddownload.php.

issued specific criteria for acceptable adware, and StopBadware.org[6] has begun the process of developing guidelines against which adware may be tested. Both of these sets of criteria, in addition to the policies already in use by the organizations listed above, can serve as models for other companies looking to adopt their own adware advertising policies.

Of course, policies are useless unless they are enforced. Advertisers must insist that ad networks enforce their policies, and advertisers have to be prepared to take their business elsewhere if the complex tangle of ad network relationships makes it impossible to ensure compliance at every level. Monitoring will be necessary in order to identify affiliates that fail to adhere to the policy. The use of blind ad networks may be acceptable only if the blind network can be trusted to enforce the policy without the advertiser having the capability of checking up on the placement of its ads.

Case Study: CDT Engages the Advertisers

On January 23, 2006, CDT filed two complaints with the Federal Trade Commission alleging that 180solutions, one of the world's largest developers of Internet advertising software, had engaged in a pattern of unfair and deceptive trade practices. Following this filing, CDT sought to identify companies that advertise with 180solutions in order to contact them regarding their advertising policies. Our consultant, Ben Edelman, helped to pinpoint 20 companies whose ads are served by 180solutions adware.[7] CDT then contacted 18 of those advertisers[8] (letters were written to the CEOs of those companies with whom we did not have a previously-established contact) to determine whether they had advertising policies addressing nuisance or harmful adware. CDT merely asked whether or not the advertisers had an adware policy that would prevent the placement of their ads through companies that engage in unfair and deceptive practices. We did not demand that the advertisers use a particular policy nor did we stipulate what such a policy should include.

Only seven advertisers responded to CDT. Two of these did not have policies in place; both established them based on our communications. The other five have policies, but the fact that their ads are still being served by nuisance or harmful adware demonstrates that policy enforcement remains an issue. The following 10 companies failed to respond to CDT's request:

- True.com
- PerfectMatch
- Club Med Americas
- uBid
- ProFlowers
- NetZero

[6] *See* http://stopbadware.org/home/reports.
[7] Ben Edelman served as CDT's consultant for a variety of research tasks that contributed to this report.
[8] Two of the companies were not contacted because one was located outside the United States and the other used an ad that seemed to be improperly displayed at the time of our testing.

- Altrec

After the initial publication of this report, several of the companies initially named in the preceding list contacted CDT to discuss their adware relationships. Four of those firms -- Waterfront Media, PeoplePC, LetsTalk.com and GreetingCards.com -- requested that CDT update the report to reflect the current state of their adware policies.

Representatives of Waterfront Media say that the company has suspended its relationship with 180solutions pending further review of that company's business practices. Waterfront Media spends less than one percent of its marketing budget on adware and expects its advertising vendors to obtain explicit user consent before installing software, collect no personal information, allow for easy removal of advertising software and avoid third party advertising distribution, company officials say. Waterfront Media is considering implementing additional standards to insure that its partners and advertising vendors abide by industry best practices.

PeoplePC's parent company, EarthLink, has a clear policy against advertising through nuisance or harmful adware. PeoplePC and Earthlink officials say PeoplePC only briefly advertised through 180solutions and has since ended the relationship. In addition, PeoplePC has reviewed its advertising relationships to ensure that it is in full compliance with the EarthLink policy.

GreetingCards.com informed CDT that it had no record of receiving our original correspondence. The company said it was unaware of 180solutions' history of unfair and deceptive practices, and ended its relationship with 180solutions in February 2006. GreetingCards.com is in the process of defining their advertising placement policy and reviewing their advertising affiliates to ensure that they follow and enforce best practices.

LetsTalk.com informed CDT that it had reduced its spending on nuisance-adware-based advertising to the point that it spends less than 1 percent of its marketing budget on ads served in that manner. The company said it is moving forward with plans to stop advertising through nuisance adware completely. According to the company, "LetsTalk will include in all new and existing affiliate contracts clear language that prohibits adware services, via a third party or via its own internal operations. Adware services are defined as pop-up ads, banner ads, page views or other forms of media based on user behavior, including search queries or visits to specific URLs, which are served based on software downloaded by the user."

It is important to note than the advertisers we contacted may or may not have a direct relationship with 180solutions. Given the nature of the Internet advertising industry, it is possible for companies to have several intermediaries between themselves and adware distributors. However, our testing, which included the use of a packet sniffer to monitor how the ads were loaded, suggested that many of these advertisers did deal directly with 180solutions to place their ads.

Online dating site eHarmony was one company that responded to CDT about their advertising policy. The company explained that it requires all other parties whom they advertise with to adhere to the standard conditions of the Interactive Advertising Bureau (IAB). Unfortunately, the IAB does not have its own guidelines for dealing with nuisance or harmful adware advertising. Instead, the IAB Standard Terms and Conditions document[9] (which the IAB encourages its adherents to use) suggests that advertisers need to include terms in their affiliate agreements to address where and how their ads get placed. Thus, while eHarmony relies on IAB standards, the IAB seems to put the onus back on eHarmony to stipulate adware advertising policies. To CDT's knowledge, eHarmony has not taken this step.

Netflix is one example of a company we contacted that already had an advertising policy in place to address adware. Netflix expressed concern that its ads are appearing via 180solutions software since the Netflix policy explicitly prohibits the display of ads through any adware or spyware program. A Netflix representative investigated the situation and assured CDT that the example found was unique and random, and that the behavior that caused the ad to be served by 180solutions software had ceased. However, within hours of receiving this notification, CDT found three more examples of Netflix ads generated by adware programs. It is important to note that Netflix is one of the largest online advertisers that CDT contacted. To CDT, this illustrates the difficulty that large companies have in enforcing their policies given the current online advertising environment, and the complex web of relationships involved with placing ads. Some companies have instituted detailed auditing processes to address this concern, but more emphasis must be placed throughout the advertising industry on policing advertising networks and dealing only with trustworthy affiliates.

Conclusion

In addition to calling attention to adware's "dirty little secret," Commissioner Leibowitz noted that if advertisers do not start acting to cut the flow of funds to the makers of nuisance and harmful adware, he will urge the Federal Trade Commission to start naming names of companies whose ads are served by this kind of software. CDT supports that intention and we share Commissioner Leibowitz's belief that Internet advertisers will have an incentive to more vigorously police the placement of their ads if light is shed on the business arrangements that make nuisance and harmful adware possible.

At this point, CDT has set a low bar by merely asking a small group of companies to contact us to discuss their advertising policies in the context of nuisance and harmful adware. We are working to increase awareness of the complex business models associated with nuisance and harmful adware, and we are pointing advertisers to policies and criteria that already exist as a step towards creating and enforcing their own policies.

It is also imperative that advertising networks engage in self-regulation in order to aid in this endeavor. Initiatives such as the TRUSTe Trusted Download Program can help to set certification standards and provide public criteria for evaluating adware makers. Advertisers

[9] *See* http://www.iab.net/standards/tandc.asp.

must demand strict compliance from their affiliates and refuse to work with blind networks and other networks that cannot commit to following stringent advertising policies.

Without advertising dollars, there would be no nuisance or harmful adware. CDT is committed to working with advertisers to stem the tide of this nefarious form of software.

For further information, contact:
Ari Schwartz (202) 637-9800 x107
Alissa Cooper (202) 637-9800 x110