

The Perils of Online Advertising

By Louis J. Levy

As the Internet expands and revenues from online advertising soar, federal and state authorities have been casting a wary eye on the practices of companies that develop online advertising programs and technology (known as “adware”), not to mention the companies who enlist the services of these companies to distribute advertising. In particular, as a result of escalating consumer complaints, state and federal authorities have brought multiple actions against adware providers, imposing stiff penalties for practices deemed to be unfair and deceptive.

In one of the most recent cases, the Federal Trade Commission (“FTC”) reached a settlement with Zango, Inc., formerly 180Solutions, Inc., whereby Zango will have to pay three million dollars and modify its practices to comply with stringent FTC requirements. A review of the complaint and agreement in this case provides online advertisers with a laundry list of practices to avoid.

By way of background, Zango develops and distributes advertising software programs (a.k.a. “adware”), which are delivered to consumers’ computers via the Internet. This software monitors a consumer’s browsing habits, and generates advertisements, primarily in the form of “pop-up” advertisements, which are related to topics queried by the consumer. According to the FTC complaint, Zango’s software has been installed on the computers of U.S. consum-

ers over 70 million times, and has generated over 6.9 billion pop-up advertisements.

Zango distributes its software through a network of affiliates and sub-affiliates, who bundle Zango’s software with supposedly “free” software (a.k.a. “lureware”), including screen savers, emoticons, and entertainment content. Consumers were not fully or adequately informed that Zango’s software had been downloaded on to their computers, nor could they easily view Zango’s terms of use or privacy policies, which were often buried behind a series of inconspicuous hyperlinks, thereby depriving users of an adequate opportunity to review these policies.

The FTC also alleged that Zango made it difficult for consumers to identify, locate and remove its software from their computers through a variety of techniques, including:

- ♦ Failing to identify the name of the adware in the pop-up advertisements;
- ♦ Misleadingly naming adware files or processes and/or saving them to a variety of locations on the user’s computer;
- ♦ Misleadingly listing the name of the adware in the Windows “Add/Remove” utility;
- ♦ Imposing complicated and protracted uninstall procedures on consumers;

(continued on page 5)

This article originally appeared in Business Law, the newsletter of the Maryland State Bar Association Business Law Section, and is reprinted with permission of the Maryland State Bar Association.

Online Advertising . . .

(continued from page 2)

- ♦ Providing uninstall tools that failed to completely remove the adware program; and
- ♦ Installing technology that “silently” reinstalled the adware after the consumer had removed it from his or her computer, often using different, randomly generated file names to thwart detection by anti-spyware programs.

These practices, the FTC alleged, constituted unfair and deceptive practices under the FTC Act.

The Agreement and Consent Order (see <http://www.ftc.gov/os/caselist/0523130/0523130agree061103.pdf>), which was issued on November 3, 2006, forbids Zango from engaging in these practices. In particular, it requires Zango, either directly or indirectly through its affiliates, to obtain a computer user’s affirmative consent prior to downloading its software onto the user’s computer, and to implement a “comprehensive program” that ensures that affiliates obtain the express consent of consumers prior to installing its software.

Zango must also implement a mechanism for receiving and addressing consumer complaints. Consistent with best practices in the online advertising industry, pop-up ads generated by Zango must bear a conspicuous legend identifying the source of the program (i.e., the name of the program generating the program) and instructions for uninstalling the program. Furthermore the uninstall methodology must be clear and straightforward, and *not* require users to download or install any additional software as part of the uninstall process, or to close or deactivate any firewalls, anti-spyware, or anti-virus programs running on the computer.

Zango is also required to pay the FTC three million dollars.

This case has obvious implications for providers of Internet advertising programs. In particular, there is a growing body of law, not to mention a growing consensus within the online community, of acceptable and unacceptable online advertising practices that are reflected in the FTC’s order in *Zango*. Indeed, a growing number of “adware” providers already comply with the requirements mandated by the FTC in this case, i.e., full disclosure prior to installation, easy uninstall procedures, identifying the source of the ads, etc.

Perhaps less obviously, the decision has important implications for the companies that place their ads through adware providers such as Zango. In particular, policy groups such as the Center for Democracy and Technology (“CDT”) have urged advertisers to stop placing advertise-

ments with providers of nuisance adware. Further, as reported by CDT, FTC Commissioner Jonathan Leibowitz has noted that he would urge the FTC to start naming companies whose ads are served by nuisance adware providers if those companies “do not start acting to cut the flow of funds to the makers of nuisance and harmful adware.” See *Following the Money: How Advertising Dollars Encourage Nuisance and Harmful Adware and What Can be Done to Reverse the Trend*, Center for Democracy and Technology, May 2, 2006, at 10 (available at <http://www.cdt.org/privacy/20060320adware.pdf>). Accordingly, advertisers need to exercise vigilance to ensure that the companies they use to place and deliver advertisements via the Internet are complying with industry best practices.

Mr. Levy is a member of the firm Leventhal Senter & Lerman PLLC (www.lsl-law.com), where he specializes in intellectual property, unfair competition, and computer security and privacy issues.