Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Advertising.com, Inc., and John Ferber
File No. 042-3196

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order from Advertising.com, Inc. and John Ferber, individually and as an officer of Advertising.com (together "respondents").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement or make final the agreement's proposed order.

Respondents advertised and distributed computer software products, including the SpyBlast computer software product, which was advertised as an Internet security program. This matter concerns the allegation that respondents failed to disclose adequately that SpyBlast included adware that caused consumers to receive pop-up advertisements.

The Commission's complaint alleges that respondents disseminated ads for SpyBlast that represented that because a consumer's computer was broadcasting an Internet IP address, the computer was at risk from hackers. According to the complaint, consumers who clicked on this advertisement were shown an ActiveX "security warning" installation box with a hyperlink describing SpyBlast as "Personal Computer Security and Protection Software from unauthorized users" and telling them "once you agree to the License Terms and Privacy Policy – click YES to continue." If a consumer clicked "Yes," the software was installed, even if the consumer had not clicked on the hyperlink. Only if a consumer clicked on the hyperlink describing SpyBlast as "Personal Computer Security and Protection Software from unauthorized users" before clicking "YES," did SpyBlast's End User Licensing Agreement ("EULA") appear. The EULA contained a statement that consumers agreed to receive marketing messages, including pop-up ads, in exchange for getting SpyBlast.

The complaint further alleges that SpyBlast could also be downloaded directly from the www.SpyBlast.com website. At the very bottom of the www.SpyBlast.com home page, below several hyperlinks to download SpyBlast, a small disclosure stating that "In exchange for usage of the SpyBlast software, user agrees to receive . . . offers on behalf of SpyBlast's marketing partners" appeared.

According to the Commission's complaint, respondents downloaded bundled adware onto the computers of consumers who installed SpyBlast. The adware collected information about SpyBlast users, including URLs of visited pages and the user's IP address, and this information allowed respondents to send users advertisements that they believed might be of interest to them. Consumers received a substantial number of pop-up advertisements as result of respondents' installation of this adware onto their computers.

The complaint alleges that in representing that SpyBlast is an Internet security program, respondents failed to disclose adequately that SpyBlast included adware that caused consumers to receive pop-up advertisements. The complaint further alleges that the presence of the bundled adware would have been material to consumers in their decision whether to install SpyBlast, and, therefore, that the failure to disclose adequately this material fact was a deceptive practice. This allegation regarding the disclosure of bundled adware applies general Commission law on deception, as enunciated in the *Federal Trade Commission Policy Statement on Deception, appended to Cliffdale Assocs*., 103 F.T.C. 110, 174-83 (1984). The application of this law in an online context was illustrated in a 2000 FTC Staff Guidance Document, *Dot Com Disclosures: Information about Online Advertising*, which is available at http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.pdf.

The proposed consent order contains provisions designed to prevent respondents from engaging in similar acts and practices in the future. The proposed order is designed specifically to address the facts of the case at hand. However, the limitation in the proposed order to respondents' software programs whose principal function is to enhance security or privacy should not be read more broadly to suggest that the requirement for clear and prominent disclosure is necessarily limited to those situations. Moreover, the problem here was not the security software that Advertising.com disseminated with its adware. Instead, it was the respondents' practice of downloading software onto users' computers, without adequate notice and consent, that generated repeated pop-up ads as the computer users surfed the Web.

Part I of the proposed order prohibits respondents from making any representation about the performance, benefits, efficacy, or features of SpyBlast or any of respondents' other executable computer software programs whose principal function is to enhance security or privacy, unless respondents disclose clearly and conspicuously that consumers who install the program will receive advertisements, if that is the case.

Parts II through VI require respondents to keep copies of relevant advertisements and materials substantiating claims made in the advertisements; to provide copies of the order to certain of their personnel; to notify the Commission of changes in corporate structure (for the corporate respondents) and changes in employment (for the individual respondent) that might affect compliance obligations under the order; and to file compliance reports with the Commission. Part VII provides that the order will terminate after twenty (20) years under certain circumstances.

The purpose of this analysis is to facilitate public comment on the proposed order, and it is not intended to constitute an official interpretation of the agreement and proposed order or to modify in any way their terms.