

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

**In the Matter of Federal Trade Commission Workshop)
Entitled "Monitoring Software on Your PC: Spyware,)
Adware, and Other Software")**

P044509

INITIAL COMMENTS OF CLARIA CORPORATION

Scott G. Eagle

Of Counsel

**D. Reed Freeman, Jr.
Collier Shannon Scott, PLLC
3050 K. Street, N.W.
Suite 400
Washington, DC 20007**

April 16, 2004

Claria Corporation (“Claria”) submits these initial comments in response to the Federal Trade Commission’s (“FTC” or “Commission”) Federal Register Notice dated February 24, 2004, regarding its April 19, 2004, public workshop entitled “Monitoring Software on Your PC: Spyware, Adware and Other Software” (the “Workshop”).

I. Introduction.

Claria Corporation is a pioneer in online behavioral marketing, serving over 43 million consumers, and having had over 900 advertisers, including 85 of the Fortune 1,000. Claria owns and operates the GAIN Network, a desktop advertising network that has been adopted by many of the world’s largest and best-known advertisers, including FTD.com, Inc., Orbitz, Inc., Amerix Mortgage Corporation, ING Direct Securities, Inc., Motorola, Inc., Sprint Corporation, Buy.com, Inc., Shopping.com, American Singles.com, Date.com, Inc., Priceline.com, Inc., Travelocity.com LP, LowerMyBills.com, Inc., RateMyMortgage, Inc., goZing.com, and inPhonic, Inc. GAIN Network ads are up to 40 times more effective than traditional banner ads because Claria’s behavioral marketing technology allows it to bring the right offer to the right consumer at exactly the right time.

More than 43 million consumers actively participate in the GAIN Network because it offers a compelling value proposition – consumers can either receive useful software applications free of charge in exchange for their agreement to receive advertising while they surf the Web (ads that save them money), or they can choose to pay for an ad-free version, generally for \$20 - \$30.

Claria offers its GAIN Network ad-serving software together with its own, free proprietary software applications, such as the Gator E-Wallet (a program that automatically remembers login IDs/passwords and fills in online forms with just one click, and which stores all

personal information on a consumer's hard drive), and with free versions of some of the world's most popular software offered by other publishers, such as DIVx (online video playing software). Software applications such as these, which are provided free of charge in exchange for users' agreement to receive advertising, are appropriately called "adware." Many popular software developers partner with companies like Claria in order to use ad-supporting software, which enables the software developers to offer their applications to consumers free of charge. This allows software developers to focus entirely on what they do best, which is to create software that meets consumers' needs.

Claria serves advertisements based on consumers' Web surfing, and without collecting, storing, using, or disclosing any personally-identifiable information from consumers. Every single consumer who has ever downloaded GAIN-supported software is and always will be anonymous to Claria.

As a leading behavioral marketing company, Claria submits these preliminary comments for three purposes: (1) to help facilitate a better understanding of the differences between illegal "spyware" and legitimate ad-supported software, or "adware"; (2) to describe the consumer benefits of ad-supported software; and (3) to share its core values of providing consumers with notice, choice and control over Claria's adware.

These initial comments are only one way in which Claria is responding to the Commission's request for information on spyware and adware. Claria is also a member of the Consumer Software Working Group ("CSWG"), a diverse community of public interest groups, software companies, Internet service providers, hardware manufacturers, and others brought together by the Center for Democracy and Technology ("CDT") to seek a consensus on responses to the concerns raised by practices that harm consumers. The CSWG plans to release

a document on April 19, 2004, that will describe a series of activities and behaviors that the Group considers to be clearly objectionable in order to help focus technical, self-regulatory, regulatory and law enforcement efforts to protect consumers from inappropriate activities in a more targeted and effective manner, while avoiding unintended negative consequences for good actors and consumers alike. Claria believes that this is an area that is ripe for self-regulatory efforts to craft industry principles to protect consumers and the marketplace.

Claria is also pleased to inform the Commission that it is engaged in a dialog with industry and regulatory groups, such as CDT, as part of Claria's ongoing efforts to continually evolve the behavioral marketing model in a way that most benefits consumers.

Finally, Claria is pleased to announce that Reed Freeman, a leading privacy lawyer and former FTC staff attorney in the Commission's Bureau of Consumer Protection, Division of Marketing Practices, will join Claria next month as Chief Privacy Officer.

II. Illegal Spyware.

Claria believes that the term "spyware" is most appropriately used to identify the behavior listed in the bullets below. This behavior is illegal under existing law – Section 5 of the FTC Act, 15 U.S.C. §45 – as an unfair or deceptive act or practice.

"Spyware":

- Gathers information from a consumer's computer without permission;
- Reports the information to the creator of the software or to one or more third parties;
- Is installed on a consumer's computer without having given adequate notice to consumers;
- Is installed without the consent of the consumer; and
- Provides the consumer with little or no control over removing the software.

This type of nefarious software often is designed to do one or more of the following (and other types of activities described in the CSWG’s forthcoming document):

- Change system settings;
- Install unauthorized dialers;
- Install keystroke loggers;
- Collect and report consumers’ personal information (even sensitive personal information such as credit card numbers or other financial account numbers) to the developer of the software or to one or more third parties;
- Use computer processing capacity without permission; and
- Deliver spam or ads without consumers’ notice and consent.

III. Legitimate Ad-Supported Software (“Adware”).

Claria believes that the use of the terms “spyware” and “adware” are often confused. Simply put, there is no overlap between “spyware” and legitimate “adware.” “Spyware” is illegal. Indeed, the use of the term “spyware” presumes that the software being so described is engaged in disguise, deceit, or deception. In this light, spyware that happens to result in the serving of ads is still spyware, and is still illegal.

“Adware,” on the other hand, should be used to describe software that is (1) supported by advertising, and (2) installed on consumers’ computers within the core principles of notice, consent, and control. If such software is installed without consumers’ notice and consent, or if it is difficult or impossible to remove, it is “spyware,” not legitimate “adware,” even if it is ad-supported.

Claria’s business model is built around three core principles: notice, consent, and control.

A. Notice and Consent.

The consumer's decision to install ad-supported software must be preceded by notice of the relevant aspects of the software and consent to its installation. If adware collects and relies on personally identifying information to serve ads, or if it collects and uses sensitive personal information such as financial account numbers or health-related information, this must be disclosed to consumers clearly, conspicuously, and unavoidably before consumers can choose to download the software.

B. Control.

Consumers should have the right to change their minds. In the context of adware, Claria believes that no decision by a consumer to install its software should be final. Consumers should be able to identify the source of the ads they get from adware they have installed based on a quick look at the text and graphics of the ads themselves. Consumers should also be given a means – also from the ads themselves – to be reminded why they received the ads, and to uninstall the ad-supported software that generates the ads if they so desire. The uninstall procedures of the ad-supported software should be simple, easy to understand, and consistent with the way consumers uninstall software that is not ad-supported generally.

IV. Conclusion.

Claria is pleased to have this opportunity to explain its core principles and to share its views on how the terms “spyware” and “adware” should be defined. Claria hopes that this will help foster legislative, regulatory, and self-regulatory initiatives that focus on putting a halt to clearly illegal conduct while allowing the nascent “adware” industry to compete in the marketplace for downloadable software.