Mr. Jason Lucas
C2 Media Ltd.

London,
United Kingdom

March 12, 2004

Federal Trade Commission
Office Of The Secretary
Room 159-H
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: FTC Public Workshop: "*Monitoring Software On Your PC: Spyware, Adware, And Other Software*"
April 19, 2004

Dear Sirs:

As someone "in the industry," I wish to submit for your review a brief (but necessary) description of the actual difference between 'adware' and 'spyware,' together with an explanation of why that distinction is extremely important in the present controversy that has generated so much public debate.

In order to understand the current situation regarding adware (or advertising software) on the Internet, it is important to realize that the Internet is a medium for communication much like television or radio. Television and radio stations have historically been supported almost entirely through advertising revenue. Thus, the content of the broadcasts on these networks is also almost entirely paid for with advertising dollars.

For the public, television and radio matured over time into indispensable tools for education, communication, and entertainment. Advertising on these communication mediums is not only tolerated by the general public, but accepted and even expected. Over the years, the public has reached the understanding that the television programs, or radio content, they consume, as well as the networks that support them, are funded through advertising dollars. The public has simply accepted this as "the way things are". Advertising generates the benefit of the programs and services which far outweigh the inconvenience of the advertisements that support them.

When it comes to the Internet, however, there seems to be a misconception attached to advertising in general, be it through software (adware), popup ads, banner

ads, text ads, or e-mail advertising. It is as though the Internet is perceived as being free, costing nothing to maintain or expand -- and, therefore a place that advertising is 'invading' rather than supporting. Thus, almost any form of advertising found on the Internet today is considered an annoyance by most people, and to a few it amounts to an actual violation of their personal sovereignty (or at least the sovereignty of their P.C.).

With television or radio, when a consumer is presented with an advertisement, they can choose to watch, listen, or change the channel. The "change the channel" option, however, does not avoid advertisements as the consumer will find that all of the broadcast networks seem to have scheduled their advertisements in equal quantities at the same time!

There is no satisfactory way for the consumer to 'block' advertisements from reaching his or her television or radio receiver. Attempts by such devices as 'TiVo' to grant the consumer the ability to remove commercials automatically from television broadcasts were met with harsh resistance from the communications industry itself and eventually were abandoned. It was the industry's position that advertising revenue was the very back bone of the networks and content developers. The conclusion was also reached that it would be harmful to the communications industry as a whole if mass produced devices were readily available to the public that would allow consumers to remove or bypass the advertising embedded in the broadcasts.

This, however, is strangely not the situation within the Internet communications medium. In fact, it seems quite the opposite. What we see now happening on the Internet is the advertising industry having given birth to an opposing alter ego -- the "anti-advertising industry."

Much of the "evil" things heard about "adware" are over-exaggerations packaged by the "anti-advertising industry" as a "fear sale" pressure tactic. This approach is consistent with the interests of an "anti-adware" company in fostering fear and discontent on the part of the general public regarding advertising software. The more the public fears, the more the "anti-advertising industry" profits.

This, of course, is where the term 'spyware' takes on particular significance. The term 'spy' has a menacing connotation for most people. Even though most 'adware' actually does no spying, the "anti-advertising industry" advises the public that their privacy is at risk from what is mostly a rather benign advertising software package. In my opinion, at least half of all the 'facts' reported by even the most reputable 'anti virus' companies regarding advertising software are either untrue or half-truths. This is because it is obviously in their own financial interest to foster fear on the public mind so that it generates demand for anti-virus software. The fact is if you are in the 'anti advertising' industry, the word 'spyware' sells (and that means money and profits for those so-called "anti-virus" companies).

The truth is 'spyware', or software that secretly spies on an Internet user by logging his or her keystrokes; recording personal information such as credit card numbers and other sensitive data, and sending it back to some unknown party to be used without permission is already illegal under current federal anti-hacking and computer crime laws. Thus, no legitimate advertising company would sell or distribute 'spyware'. That situation, however, does not leave very many programs for the 'anti advertising industry" to put into the "fear sale" spyware category and does little to boost sales.

A leading manufacture, for example, has listed its "own definitions" of adware and spyware -- adopting the presumptuous attitude that it is the arbiter of such definitions and thus validity. That company defines "adware and "spyware" as follows:

ADWARE

> *Programs that secretly gather personal information through the Internet and relay it back to another computer, generally for advertising purposes. This is often accomplished by tracking information related to Internet browser usage or habits.*
>
> *Adware can be downloaded from Web sites (typically in shareware or freeware), e-mail messages, and instant messengers. A user may unknowingly trigger adware by accepting an End User License Agreement ("EULA") from a software program linked to the adware.*

SPYWARE

> *Stand-alone programs that can secretly monitor system activity. These may detect passwords or other confidential information and transmit them to another computer.*
>
> *Spyware can be downloaded from Web sites (typically in shareware or freeware), e-mail messages, and instant messengers. A user may unknowingly trigger spyware by accepting an End User License Agreement from a software program linked to the spyware.*

Any reading of those two definitions reveals the unfair and inaccurate similarity between the two definitions (as in use of the word 'secret' in the same context for both definitions). Of significance is the following line common to both definitions: a user may 'unknowingly trigger' both 'adware' and 'spyware' by ACCEPTING an End User License Agreement. That comment, however, simply makes no sense. Query: how can one "unknowingly" trigger a "secret spy" if he or she previously accepted a written EULA that clearly explained all of the functions of the software before it was even installed?

Common sense dictates that if someone were truly trying to spy on you without your knowledge or consent, the last thing they would do is present you with a legally binding EULA telling you, in writing, exactly what they were going to do.

Thus, contrary to the above-noted inaccurate definition of adware being disseminated by some companies, it is important to recognize the more correct definition of 'Adware':

Adware --

> "Software that, with the user's prior consent and acceptance of an End Users License Agreement ("EULA"), usually in exchange for a free service or software product(s), displays advertisements on the users computer through popup advertisements, banner advertisements or other web browser enhancements (such as toolbars search pages or homepages). Such advertisements may be based on non personally-identifiable browser usage. Adware is installed with the user's consent and has a built in "uninstaller" (available to the user free of charge) that can be activated by the user at any time. The functions of the adware are explained in the EULA before the software is installed. Adware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers."

I believe this to be a more truthful and accurate definition of 'adware' or advertising software. It certainly lacks the scary "fear sale" words (*e.g.,* "secretly' and 'spy'). Clearly, the 'anti advertising' industry should be held equally accountable to fair and truthful advertising standards and should be required to state the truth about the programs they are detecting and removing.

Advertising software companies whose products fall within my proposed definition of 'adware' should not be penalized for creating innovative new technologies that allow advertisers the opportunity to more easily reach targeted consumers. The onslaught of 'anti advertising' software that is now being marketed has had a serious impact on Internet advertising, and that commercial industry is now being forced to create new and innovative methods to deliver their message to consumers.

Advertising software when constructed and distributed in a responsible manner is the very future of Internet advertising. While there should certainly be clear guidelines establishing what is, and is not, acceptable when it comes to this new technology, we should be very careful not to penalize legitimate companies who are willing to follow the rules -- less we unfairly stifle an already weakened industry.

Thank you for your time in reading my comments.

Sincerely,

Jason Lucas