

cohen&grigsby[®]

progressive law.

June 6, 2005

NOT ADMISSIBLE FOR ANY PURPOSE

VIA Facsimile (972-3-6025225) and U.S. Certified and Registered Mail (NY Office)

Mr. Eran Liss
Legal Department
Hotbar.com, Inc.
Libn Gvirol Street
P.o.b.-22365
Tel Aviv, 62032, Israel

Re: Javacool Software Response to Request for Additional Detail

Dear Mr. Liss:

We are in receipt of your correspondence dated May 29, 2005. We declined to provide details regarding our investigation earlier because Hotbar had threatened litigation, which threat triggered our response. While we do not believe we owe Hotbar any duty in this case, our client is prepared to provide you with certain additional information on a voluntary basis to aid you in your decision making process. The information provided herein is delivered in contemplation of amicable resolution and may not be used in court or other proceedings without our permission. Nothing in this letter, including the research findings, review, concerns, or overview of our software outlined below, may be used by Hotbar for any purpose other than to have an open dialogue between Hotbar and Javacool Software LLC. This letter is written without prejudice to or waiver of any of Javacool Software's rights or remedies, all of which are expressly reserved.

After receiving your initial letter, Javacool Software LLC reviewed your software. Based on its review of your software (Hotbar), Javacool Software LLC concluded that the Hotbar software does merit inclusion in the SpywareBlaster[®] database of potentially unwanted software. Therefore, we are writing to you to let you know that, at this time, Javacool will not be changing the status of Hotbar or removing Hotbar from its database. Further details appear below.

BELOW IS THE RESULT OF JAVACOOOL SOFTWARE'S RESEARCH EFFORT, AS PROVIDED BY JAVACOOOL SOFTWARE LLC:

Hotbar Review / Outline of Behavior Concerns

We are always willing to provide constructive feedback, when asked, regarding why a particular item is included in our database. We believe you'll find the results of our analysis to be constructive.

Advertising Behavior Overview:

In the helpdesk section of your website (<http://hotbar.com/HelpDesk/Faq/Main.htm>) you state the following:

“1. Hotbar does monitor the websites you visit for the sole purpose of presenting contextually related information; this information is completely anonymous!”

This mantra is repeated many times throughout the website and the program. Yet nowhere (before the non-cancelable installation step detailed below, and with the possible exception of the EULA) is it explicitly stated that “Hotbar displays advertising.” This advertising is displayed in many different ways:

1. In the Internet Explorer interface in the form of buttons or links in the toolbar area.
2. As pop-up/under ads (enabled by default) when you visit websites.
3. In the left-hand “sidebar” in a feature called “ShopperReports”, which doesn’t clearly display to the user that it’s part of Hotbar.

(See Fig. 1A through 1E.)

With the prevalence of pop-up blockers, among other “anti-advertisement” software, we believe it’s fairly easy to see that a significant percentage of computer users do not want advertisements displayed on their computers. The somewhat recent inclusion of a pop-up blocker in Internet Explorer 6 SP2 (in Windows XP SP2), due to user demand, supports this claim. The forms of advertising that Hotbar displays include the pop-up advertisements that many users do not want, as well as other bright, flashing, and potentially intrusive advertisements that users may not want to have displayed on their machines.

Inadequate Disclosure of Advertising Behavior on Homepage / Other Sites:

The Hotbar.com homepage does not mention the fact that advertising is displayed in the above forms, despite touting Hotbar’s other features (emoticons, etc.) in very large type. (Fig. 2A)

Other researchers have come to additional related conclusions regarding possible unwanted and potentially misleading targeting of children: <http://www.benedelman.org/spyware/installations/kidzpage-hotbar/> (Hotbar Installs via Banner Ads at Kids Sites, Benjamin Edelman). We will note that (according to the research detailed on that page) Hotbar again touts its other features (such as emoticons) without mention of its advertising behavior.

Installation:

The Hotbar installer *does* reference two installation options: a “free ad-supported version” or a “paid version”. Prior to this, a user may have clicked past the license agreement without doing much but skimming it, and thus possibly come across his/her first discovery of the fact that Hotbar displays advertising at this stage. Unfortunately, at this stage in the installation process *there is no button that can*

be used to cancel or back out of the installation. The average user is essentially *forced* to make a choice between advertising on their machine or paying money. (Fig. 2B)

Even at this installation screen, however, there is minimal disclosure of the facets of the advertising behavior. The types of advertising and the placement of such advertisements (as noted above), among many other behaviors, are not described.

At this point in the installation, if the "Paid version" option is selected, the user is taken to the "Hotbar Premium" purchase site. (Fig. 2C) If a user then tries to click one of the security/privacy seals at the bottom of the page, the Hotbar toolbar with advertising is still installed/activated (Fig. 2D), despite the fact that the user indicated their preference for the paid version with no ads, and despite the fact that the Hotbar Premium window has not been closed, even though it claims:

"By closing this window you will still be able to enjoy our FREE version."

Also, clicking on the Trust-e seal brings up a webpage (Fig. 2E) that states:

NOT VERIFIED

IS NOT A VALID TRUSTe MEMBER WEB SITE

The unauthorized display of the TRUSTe trustmark is unlawful and violates a TRUSTe trademark. [...]

Monitoring of Websites Viewed / Browsing Behavior:

The Hotbar Terms of Use states:

HOTBAR COLLECTS AND STORES AGGREGATED INFORMATION ABOUT THE WEB SITES ITS USERS VIEW AND THE DATA THEY ENTER IN SEARCH ENGINE SEARCH FIELDS WHILE USING THE SOFTWARE. HOTBAR USES THIS INFORMATION TO DETERMINE WHICH ADS AND BUTTONS TO DISPLAY ON YOUR HOTBAR TOOLBARS AND WHICH ADS TO SHOW YOUR BROWSER.

(Source: <http://hotbar.com/Legal/hotbar/license.htm> - Accessed on May 5th, 2005)

This monitoring of websites (collection of data used for targeted advertising) was confirmed on a fresh installation of Hotbar. For many sites the user would visit, the website address would be sent to another server, presumably to allow "targeted advertising". We also encountered a large number of Hotbar-created pop-up ads on websites that normally have none, or that have pop-up ads that are blocked by the built-in Windows XP SP2 Internet Explorer pop-up blocker.

Uninstallation:

Although there are multiple choices of uninstallers for programs which appear to be related to Hotbar software listed in Add/Remove Programs (whereas there was only one installer executable), the uninstallers do remove most components of the Hotbar package.

However, Hotbar installs a randomly named executable (under the Windows' system directory) that runs on startup and alerts the user when any components of the Hotbar software are missing (possibly having

been removed by “spyware-removal” utilities, or any other programs that perform similar tasks). This behavior is concerning as most software does not install randomly named executables in Windows’ system directories for the purpose of alerting the user when portions of said software have been removed by third-party programs.

SpywareBlaster Information

SpywareBlaster is a preventative solution for spyware *and other potentially unwanted software* (a point that is stressed in multiple places on our website, and others).

We characterize Hotbar in our database as “ActiveX” (Fig 3A), not as “spyware” or “adware”.

Users are in control of the protection our program can potentially provide – we do not block anything by default. Each user can choose to block/exclude only certain items in the database, as well as add their own items. Various program features allow each user to completely decide which items he/she does or does not want installed on his/her machine: including multiple checkboxes to enable only certain parts of the protection, a “permanent ignore list” to permanently remove items from the database on a single PC, etc.

General Summary Points

1. The Hotbar.com main homepage does *not* acknowledge the program’s targeted advertising behavior.
2. Other research has shown that advertisements on the web, at sites targeting children, could be considered misleading as well, as they do not acknowledge the program’s advertising behavior. (<http://www.benedelman.org/spyware/installations/kidzpage-hotbar/>)
3. Hotbar does not overtly or obviously inform the user of its targeted advertising behavior until late in the installation, at which point the user can no longer back out of the installation. (Even at this point, the completeness and the “adequacy” of the notice of advertising behavior can be questioned.)
4. When the user finally sees the “pay version” / “advertising-supported” options, *there is no button that can be used to cancel or back out of the installation*. The average user is essentially *forced* to make a choice between advertising on their machine or paying money. (Note: We believe that a user should *always* be able to back out of the installation of a program, especially before any components of said program, excluding the installer, have been copied to the computer.)
5. The Hotbar toolbar monitors and collects user browsing information (such as the websites users visit).
6. The Hotbar toolbar displays advertising in many forms, and some users may not wish to have software that displays advertising in those forms on their computers. (The “forms” including pop-up/under ads, etc.)
7. Hotbar installs a randomly-named executable in the Windows’ system directory which may impede the removal of Hotbar’s software by third-party utilities.
8. SpywareBlaster gives users the *choice* to prevent the installation of Hotbar (among many other programs). There are many situations where this could be useful: for example, parents

could want to make sure their children don't accidentally install software that displays pop-up advertising, in any form.

9. In regard to SpywareBlaster, it is *always the user's choice what to block*. The user decides what protection they would like to enable, and can even enable or ignore individual items. *SpywareBlaster installs with no protection enabled by default – the user must choose to enable any protection.*
10. Public write-ups on Hotbar also provide additional information (and consensus) on the software's behavior:
 - a. <http://www3.ca.com/securityadvisor/pest/pest.aspx?id=453075474>
 - b. <http://www.howard.edu/technology/hotbar/>
 - c. <http://sarc.com/avcenter/venc/data/adware.hotbar.html>
 - d. <http://www.iamnotageek.com/a/217-p1.php>
 - e. <http://www.benedelman.org/spyware/installations/kidzpage-hotbar/>

We hope this review has answered any questions you had about SpywareBlaster's functionality, as well as satisfied your inquiry.

After a careful review of your program, we do not see a reason to remove Hotbar from SpywareBlaster's database at this time. However we are always willing to review new, public versions of programs in our database, and welcome your future submission of a new, public version of your program for our review.

The above-mentioned behaviors and practices may not be the only criteria for including Hotbar in our database, nor are they a complete description of your software's behavior, but, rather, should be considered an overview of some major concerns we have regarding your software's behavior and practices. We believe the concerns highlighted above, at a minimum, are reasonable justification for including Hotbar's software in our user-selectable database. And we hope that the brief overview of our software clears up any misunderstandings as well.

Very truly yours,

COHEN & GRIGSBY, P.C.



Christopher B. Carson

CBC/bhc

attachments

cc: Javacool Software LLC

Kevin C. Harkins, Esq., Cohen & Grigsby

974588_1