

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

NORMAN J. BLEARS (95600)
HELLER EHRMAN LLP
275 Middlefield Road
Menlo Park, CA 94025-3506
Telephone: (650) 324-7000
Facsimile: (650) 324-0638

MICHAEL P.A. COHEN
SHARI A. ROSE (235870)
HELLER EHRMAN LLP
1717 Rhode Island Ave., NW
Washington, D.C. 20036
Telephone: (202) 912-2000
Facsimile: (202) 912-2020

Attorneys for Plaintiff
SYMANTEC CORPORATION

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

SYMANTEC CORPORATION,

Plaintiff,

v.

HOTBAR.COM, INC.,

Defendant.

E-filing

ADR



JUN 07 2005

NOV 11 2005

05 02309

Case No.:

COMPLAINT FOR
DECLARATORY JUDGMENT

RS

Plaintiff Symantec Corporation ("Symantec") brings this Complaint for Declaratory Judgment against Defendant Hotbar.com, Inc. ("Hotbar") and states as follows:

PARTIES TO THE ACTION

1. Plaintiff Symantec is a company incorporated under the laws of Delaware with its principal place of business located at 20330 Stevens Creek Boulevard, Cupertino,

1 California.

2 2. Upon information and belief, Defendant Hotbar is a company incorporated
3 under the laws of Delaware with its principal place of business located at 226 West 37th
4 Street, New York, New York.

5 **JURISDICTION AND VENUE**

6 3. Plaintiff brings this action under the Declaratory Judgment Act, 28 U.S.C.
7 §2201. The Court has federal question subject matter jurisdiction based upon 28 U.S.C.
8 §1331 in that this action seeks declaratory judgment under the laws of the United States.
9 The Court has supplemental jurisdiction over the portion of this action seeking declaratory
10 judgment under related state laws pursuant to 28 U.S.C. § 1367.

11 4. Venue is proper in this district pursuant to 28 U.S.C. §1391, because a
12 substantial part of the events giving rise to the claim occurred in this district.

13 **FACTS**

14 5. Symantec is the world leader for computer, network and Internet security
15 technology. With approximately 6,000 employees and operations in more than thirty-five
16 countries, Symantec provides content and network security software and appliance solutions
17 to individuals, enterprises and service providers. The company is the leading provider of
18 client, gateway and server security for virus protection, intrusion detection, firewalls and
19 Internet content and e-mail filtering, among other computer security services. Its popular
20 Norton AntiVirus software has more than 100 million computer users throughout the world.

21 6. To identify programs or files that present computer security risks in a twenty-
22 four hour, seven days a week environment, Symantec has a Security Response team of
23 experts, security engineers, virus hunters and technical support personnel located in
24 Australia, Canada, Ireland, Japan and the United States. Symantec Security Response
25 provides security alerts, advisories and content including dynamic, rapid security protection
26 through, among other services, emergency anti-virus definitions, intrusion detection
27 signatures and policies updated and distributed through automated processes.

28 7. Symantec detects, names and classifies potentially unwanted technologies

1 according to the detected program or file's method of operation and potential level of risk.
2 Customers who install Symantec's software applications can receive information about
3 these programs and files, including their risk assessment and instructions on how to remove
4 them from a system or network. These customers also receive regular updates to their
5 installed software when Symantec detects programs or files that are new or reclassified.

6 8. Symantec's Internet website, located at www.symantec.com, provides
7 computer users with detailed descriptions about the programs and files it identifies. The
8 website also provides users with definitions of the terms that Symantec uses to describe
9 various detected programs and files, for example: "viruses," "worms," "Trojan horses,"
10 "adware," and "spyware."

11 9. Symantec defines adware as follows: "Programs that facilitate delivery of
12 advertising content to the user through their own window, or by utilizing another program's
13 interface. In some cases, these programs may gather information from the user's computer,
14 including information related to Internet browser usage or other computing habits, and relay
15 this information back to a remote computer or other location in cyber-space. Adware can be
16 downloaded from Web sites (typically in shareware or freeware), email messages, and
17 instant messengers. Additionally, a user may unknowingly receive and/or trigger adware by
18 accepting an End User License Agreement from a software program linked to the adware or
19 from visiting a website that downloads the adware with or without an End User License
20 Agreement." *See Exhibit A.*

21 10. Symantec's definition of adware is consistent with the academic and computer
22 science communities. For example, WhatIs.TechTarget.com, an Internet-based information
23 technology encyclopedia, defines adware as "any software application in which advertising
24 banners are displayed while the program is running." *See Exhibit B.* Indiana State
25 University's Office of Information Technology states: "Adware is software which is free to
26 the user or available at a reduced cost because it displays advertisements either in the
27 software window itself or in separate pop-up windows. By itself adware is merely irritating
28 as the user must contend with unwanted pop-up windows while running the ad-supported

1 software." *See* Exhibit C. Princeton University states that "[a]dware refers to programs
2 which gather information about you for marketing purposes in order to target your computer
3 with advertisements." *See* Exhibit D.

4 11. Wikipedia.org, an Internet encyclopedia written collaboratively by volunteers,
5 includes this definition of adware: "Adware or advertising-supported software is any
6 software application in which advertisements are displayed while the program is running.
7 These applications include additional code that displays the ads in pop-up windows or
8 through a bar that appears on a computer screen. . . . Some adware programs have been
9 criticized for occasionally including code that tracks a user's personal information and
10 passes it on to third parties, without the user's authorization or knowledge. This practice has
11 been dubbed spyware and has prompted an outcry from computer security and privacy
12 advocates." *See* Exhibit E.

13 12. As the Wikipedia definition of adware illustrates, from a technical and
14 academic perspective, adware can also be spyware.

15 13. Webopedia, an online dictionary dedicated to computer technology also
16 explains the relationship between spyware and adware: "Unfortunately, some freeware
17 applications which contain adware do track your surfing habits in order to serve ads related
18 to you. When the adware becomes intrusive like this, then we move it in the spyware
19 category and it then becomes something you should avoid for privacy and security reasons.
20 Due to its invasive nature, spyware has really given adware a bad name as many people do
21 not know the differences between the two, or use the terms interchangeably." *See* Exhibit
22 F.

23 14. The United States Department of Homeland Security has also recognized the
24 overlap between adware and spyware. In its Cyber Security Tip ST04-016, the Department
25 of Homeland Security states, "In fact, spyware is also known as 'adware.' It refers to a
26 category of software that, when installed on your computer, may send you pop-up ads,
27 redirect your browser to certain web sites, or monitor the web sites that you visit. Some
28 extreme, invasive versions of spyware may track exactly what keys you type. Because of

1 the extra processing, spyware may cause your computer to become slow or sluggish. There
2 are also privacy implications: What information is being gathered? Who is receiving it?
3 How is it being used?" See Exhibit G.

4 15. When classifying programs and files, Symantec separately defines adware and
5 spyware, based on the program or file's method of operation and potential security risk. By
6 so doing, Symantec helps its users become more knowledgeable about the programs and
7 files on their computers and enables them to make informed choices about the software they
8 choose to keep or remove from their computers.

9 16. Symantec defines spyware as follows: "Programs that have the ability to scan
10 systems or monitor activity and relay information to other computers or locations in cyber-
11 space. Among the information that may be actively or passively gathered and disseminated
12 by Spyware: passwords, log-in details, account numbers, personal information, individual
13 files or other personal documents. Spyware may also gather and distribute information
14 related to the user's computer, applications running on the computer, Internet browser usage
15 or other computing habits. Spyware frequently attempts to remain unnoticed, either by
16 actively hiding or by simply not making its presence on a system known to the user.
17 Spyware can be downloaded from Web sites (typically in shareware or freeware), email
18 messages, and instant messengers. Additionally, a user may unknowingly receive and/or
19 trigger spyware by accepting an End User License Agreement from a software program
20 linked to the spyware or from visiting a website that downloads the spyware with or without
21 an End User License Agreement." See Exhibit A.

22 17. Symantec's definition of spyware is also consistent with academic and
23 computer science definitions of spyware. Indiana State University, for example, provides
24 the following definition of spyware: "Spyware is any software which utilizes the bandwidth
25 of the machine on which it is installed to communicate with the parent company. Statistics
26 about one's browsing habits, installed software and other information are collected by these
27 companies and then either sold as market research or used by the company itself to target
28 ads at the user. Together (often a program works as both adware and spyware) [adware and

1 spyware] represent a serious invasion of the user's privacy and could use up considerable
2 bandwidth and processor resources communicating with the developer and downloading ad
3 content." *See* Exhibit C; *see also* Princeton University, Exhibit D ("Spyware is the generic
4 term for computer software that gathers information about you and your Internet surfing
5 habits for marketing purposes.").

6 18. From a computer security standpoint, any executable file that accesses a
7 remote third party is capable of giving that third party, and potentially others, access to the
8 computer and the computer network. For this reason, the government, network
9 administrators, business customers and individual computer users are interested in
10 identifying any "open door" to a computer system, whether it be adware, spyware or
11 otherwise.

12 19. This type of "open door" is itself a security vulnerability, independent of the
13 specific behavior of a particular file or program. In 2004, a graduate student and two
14 professors from the University of Washington's Department of Computer Science and
15 Engineering made this point, in a study that examines this very type of security risk. *See*
16 Exhibit H. At the time, the study found that two Internet applications, Gator and eZula,
17 "suffered from a simple vulnerability in how they install data file updates." *Id.* The authors
18 describe how they were able to exploit this security vulnerability: "We implemented and
19 successfully mounted an attack by sending spoofed DNS responses to *gator.com* and
20 *ezula.com* DNS requests coming from the [computers with Gator and eZula installed]. Our
21 spoofed responses trick[ed] the spyware programs into downloading and installing updates
22 that we supply from a local Web server, instead of downloading updates from the intended
23 servers." *Id.* The University of Washington study concluded: "We verified that we could
24 insert arbitrary executables in our updates, leaving open the possibility of running malicious
25 code or installing backdoors." *Id.*

26 20. It is precisely this type of security risk, along with others, that lead
27 governments, businesses and individual computer users to want to understand not just what
28 files are on a computer, but *how* those files operate. From a computer security standpoint,

1 how a computer file or application serves Internet advertisements, for example, is just as
2 important as the fact that advertisements are served.

3 21. Hotbar is a company that distributes a computer program which adds
4 graphical skins and toolbars to Microsoft Internet Explorer, Microsoft Outlook and Outlook
5 Express. The Hotbar program also contains computer files that facilitate the delivery and
6 display of Internet advertisements, including "pop-up" advertisements. The program can be
7 downloaded from Hotbar's Internet website, located at www.hotbar.com. Hotbar's program
8 is distributed through numerous other Internet websites as well.

9 22. Hotbar's adware program has created a good deal of controversy. Numerous
10 Internet websites have posted comments or issued warnings relating to Hotbar's adware
11 program. For example, in February 2005, SmartComputing featured an article titled *How to*
12 *Get Rid of Hotbar* that describes Hotbar's software and provides instructions on how to
13 remove it: "[T]he Hotbar toolbars help you decorate your browser and email client with
14 colorful animations, vivid images, and fun emoticons while tracking your online activities
15 for the purpose of delivering targeted pop-up ads to your Desktop." See Exhibit I. An
16 article on HowToUniverse.com titled *How to Get Rid of HotBar and Other Parasites,*
17 *Adware and Spyware* states: "What do I have against Hotbar? For one thing I get more
18 errors and lock ups and ad popup windows when Hotbar is installed. It eats up resources I
19 prefer to have for other things. It installs all kinds of adware that runs behind the scenes
20 using even more of my disc space and resources." See Exhibit J. Warnings and removal
21 instructions for Hotbar's product can also be found on various other websites. See, e.g.,
22 Exhibit K.

23 23. One commentator's review of the user experience downloading Hotbar is
24 found in an article titled *Hotbar Installs via Banner Ads at Kids Sites.*" See Exhibit L. This
25 review notes that a user downloading Hotbar from www.thekidzsite.com is not
26 automatically presented with Hotbar's license agreement during installation. See *id.*
27 Instead, the user will only see Hotbar's license agreement by taking the additional step of
28 clicking on a specified link. See *id.* Without this independent action by the user, Hotbar

1 will install without ever showing the user the license agreement. *See id.* This installation
2 procedure is not unique to www.thekidzpage.com. Similarly, a user downloading Hotbar
3 from websites such as www.bullseyegames.com and www.squiglyplayhouse.com may not
4 be presented with Hotbar's license agreement unless the user takes the additional step of
5 clicking on the specified link.

6 24. Hotbar's license agreement itself has been labeled "hidden and half-hearted."
7 *Id.* It is thirty-seven on-screen pages and a discussion of Hotbar's advertising practices
8 does not appear until pages sixteen and seventeen. *See id.* Even then, the license agreement
9 "uses complicated language like 'will be exposed to' rather than directly stating that Hotbar
10 will 'show' ads." *Id.*

11 25. Though one screen in Hotbar's installation apparently does ask the user to
12 choose between a "free ad-supported version" or a "paid version," this screen does not give
13 the user the option to cancel the installation. *See id.* The review explains: "No cancel
14 button is shown. Note also the absence of a an X in the upper-right corner of the installer,
15 and even right-clicking on the taskbar entry does not work (does not yield a menu with a
16 Close button)." *Id.* Without an obvious way to cancel the installation, users may "choose
17 the ad-supported option without understanding its true effects." *Id.*

18 26. Hotbar is also criticized for targeting its application to children, who are
19 unlikely to be able to "assess the merits of an Hotbar offer." *Id.* Hotbar is targeted to
20 children both through banner ads placed on websites aimed at children, such as
21 www.thekidzpage.com, and advertisements that are "likely to be particularly attractive to
22 kids -- with overstated smiley faces, including an enlarged central image with its eyes,
23 tongue, and hands in a characteristically child-like pose." *Id.* Whether children could
24 understand any license agreement, even if presented, is itself questionable.

25 27. A Penn State University article titled *Just Say "No" to Hotbar* discusses
26 Hotbar's adware program and recommends the removal of Hotbar: "Spyware, adware, and
27 other malware (malicious software) have become real threats to our online privacy, security,
28 anonymity, and efficiency. . . . One common piece of malware . . . is called 'Hotbar.' This

1 program is often listed in your Add or Remove Programs control panel as 'Hotbar,' 'Outlook
2 Tools from Hotbar,' or 'Web Tools from Hotbar.' Although this program does add some
3 interesting features to Outlook and Internet Explorer--such as animated smilies, background
4 pictures for e-mail messages, and search toolbars--it violates your online privacy and
5 anonymity by tracking your Web surfing habits." See Exhibit M.

6 28. Other colleges and universities that have issued online warnings about Hotbar
7 and recommended against downloading the program include: Auburn University,
8 California State University, Colorado College, Dakota Wesleyan University, Duke
9 University, East Carolina University, East Tennessee State University, Fayette State
10 University, Gettysburg College, Howard University, Montana State University, National
11 University of Singapore, Northern Virginia Community College, Saint John's University,
12 Tufts Medical School, University of Akron, University of Northern Florida, University of
13 Southern Indiana, Wellesley College and Winona State University. See Exhibit N; Exhibit
14 O; Exhibit P.

15 29. Several of these universities caution readers that aside from privacy concerns
16 related to Hotbar, installing Hotbar may also affect system performance and compromise
17 network security. A University of Southern Indiana message to the university community
18 regarding Hotbar serves as an example: "It is strongly recommended that you do not install
19 [Hotbar] on your system. If it is already installed, it should be uninstalled. If you have
20 already installed this, you may have noticed that you have more pop-ups, more junk e-mail,
21 and a slow down in system performance." See Exhibit O.

22 30. California State University, Chico, has a notice titled *Beware of Hotbar* on its
23 Information Resources web page: "Hotbar . . . can shut down your computer or make it
24 vulnerable to outside intrusion. . . . Hotbar also records network information so it can punch
25 a hole through network security systems which can make the entire network open to virus or
26 other attack." See Exhibit P. The Chico notice also warns that Hotbar may track
27 information not only from Internet Explorer, but also from Microsoft Outlook: "E-mail you
28 send to anyone else can also be affected. The recipients can be tracked, and hidden code

1 within the mail may also retrieve information from our servers (such as text and/or banner
2 promotions) which will, in such case, also appear in the e-mail sent." *Id.*

3 31. Notably, these university warnings are premised on computer security risks to
4 computer and network operations without regard to disclosures.

5 32. On August 18, 2003, Symantec identified and classified various Hotbar files
6 as adware ("Adware.Hotbar"). *See* Exhibit Q.

7 33. On or about July 28, 2004, Ziv Eliraz, Hotbar's Vice President of Strategic
8 Alliances, sent Symantec an e-mail message regarding Symantec's detection of
9 Adware.Hotbar. In response, Symantec evaluated its detection of Hotbar's free ad-
10 supported program. Based on this evaluation, Symantec explained to Hotbar that it
11 remained comfortable with its detection of Hotbar's program as adware. Symantec did
12 revise its Security Response description to reflect updated technical information on Hotbar's
13 installation and tracking behavior.

14 34. The summary of the Symantec Security Response description for Hotbar's
15 program states: "Adware.Hotbar adds graphical skins to Internet Explorer, Microsoft
16 Outlook, and Outlook Express toolbars and adds it own toolbar and search button. These
17 custom toolbars have keyword-targeted advertisements built into them. Adware.Hotbar can
18 send information on browsing habits to various servers, which may be used for targeted
19 marketing." *See* Exhibit Q.

20 35. During the correspondence between Symantec and Hotbar regarding
21 Symantec's evaluation of Hotbar's program as adware, Hotbar threatened to bring litigation
22 against Symantec no less than five times. In its February 28, 2005 threat, Hotbar threatened
23 legal action against Symantec under federal trademark laws and related state laws.

24 36. Symantec has concluded and ended its discussions with Hotbar. It now seeks
25 declaratory relief to clarify its ongoing right to detect Adware.Hotbar as described, without
26 any legal cloud.

27
28

CLAIM FOR DECLARATORY RELIEF

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

37. Symantec realleges each and every allegation of Paragraphs 1 through 36 of this Complaint and incorporates them by reference as if fully set forth herein.

38. Hotbar operates an adware program through its website located at www.hotbar.com. When Hotbar's adware program is downloaded, it displays targeted advertising content.

39. Hotbar's adware program collects information about a computer user's browsing habits and communicates that information to remote servers for advertising purposes. The computer user has no control over the adware program's operation; only the entity operating the adware program controls its operation and the type of information collected about a computer user.

40. Symantec has classified the Hotbar program as adware in its security definitions and Security Response descriptions.

41. Hotbar has threatened Symantec with legal action based on Symantec's detection and classification of Hotbar's adware program, without any indication of how or when. Hotbar has threatened Symantec with legal action no less than five times.

42. There is a ripe and justiciable controversy between Hotbar and Symantec regarding Symantec's right to detect and classify Hotbar's adware program as a computer security risk.

PRAYER FOR RELIEF

Plaintiff Symantec therefore prays for judgment as follows:

A. For a declaration that Symantec's Security Response description and classification for Adware.Hotbar is correct and accurate;

B. For a declaration that Symantec's Security Response description and classification for Adware.Hotbar does not violate Section 43 of the Lanham Act, 15 U.S.C. §1125;

C. For a declaration that Symantec's Security Response description and classification for Adware.Hotbar is not actionable as trade libel, product libel or product

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

disparagement;

D. For a declaration that Symantec's Security Response description and classification for Adware.Hotbar is not actionable as intentional interference with contract;


E. For a declaration that Symantec's Security Response description and classification for Adware.Hotbar is not actionable as negligent interference with contract;

F. For a declaration that Symantec's Security Response description and classification for Adware.Hotbar is not actionable as intentional interference with prospective economic advantage;

G. For all such further equitable and legal relief as the Court may deem just and proper.

DATED: June 7, 2005

HELLER EHRMAN LLP

By 
NORMAN J. BLEARS
MICHAEL P.A. COHEN
SHARI A. ROSE

Attorneys for Plaintiff
SYMANTEC CORPORATION