Blake D. Miller (4090)
Paxton R. Guymon (8188)
Joel T. Zenger (8926)
**MILLER MAGLEBY & GUYMON, P.C.**
170 South Main Street, Suite 350
Salt Lake City, Utah 84101
Telephone: (801) 363-5600
Facsimile:(801) 363-5601
Special Assistant Attorneys General

Mark Shurtleff (4666)
Philip C. Pugsley (2661)
**UTAH ATTORNEY GENERAL'S OFFICE**
160 East 300 South
Suite 500
Post Office Box 140811
Salt Lake City, UT 84114-0811
Telephone: (801) 366-0245
Facsimile: (801) 366-0352

Attorneys for Defendants

**IN THE THIRD JUDICIAL DISTRICT COURT**

**SALT LAKE COUNTY, STATE OF UTAH**

| | |
|---|---|
| **WHENU.COM, INC. a Delaware corporation,**<br><br>**Plaintiff,**<br>**vs.**<br><br>**THE STATE OF UTAH, a body politic, OLENE S. WALKER, in her official capacity as Governor of Utah., and MARK SHURTLEFF in his official capacity as Utah Attorney General,**<br><br>**Defendants.** | **AFFIDAVIT OF BENJAMIN G. EDELMAN**<br><br>**Civil No. 040907578**<br><br>**Honorable Joseph C. Fratto** |

DECLARATION OF BENJAMIN G. EDELMAN

I, Benjamin G. Edelman, state and declare as follows:

1. I make this statement under penalty of perjury and from my own personal knowledge.

2. I have been retained by the State of Utah as an expert in the above-captioned lawsuit to provide analysis of, and testimony concerning, the operation of spyware programs generally and the plaintiff's software specifically.

3. Attached hereto as Exhibit "A" is a true and correct copy of my current Curriculum Vitae.

4. I have conducted research on spyware software on several previous occasions. My research has included software produced by WhenU.COM, Inc. ("WhenU") as well as by its leading competitor, Claria, Inc. ("Claria," formerly known as "Gator"). I am familiar with the operation of these programs as well as other spyware programs.

Employment History and Experience

5. I am a Ph.D. candidate in Economics at Harvard University, a student at the Harvard Law School, and an Olin Fellow in Law and Economics. My research interests include Internet architecture and regulation, with methodological emphasis on quantitative analysis, modeling, and writing software to collect data.

6. While enrolled in these programs, and previously, I have also taken on a variety of outside consulting projects. To the extent that these projects have

culminated in expert testimony, they are detailed in the section that follows, *Prior Expert Testimony.* Representative examples of my non-litigation consulting projects include tracking large-scale domain name registrations that might be taken to infringe on the rights of others, assisting web sites blocked by China in reconfiguring their servers to be reachable to users in that country, and advising clients as to the technical merits of certain web-based business investments.

7. Until January 2004, I was employed as a Student Fellow at the Berkman Center for Internet & Society at Harvard Law School. I had been employed as a technical consultant at the Berkman Center since May 1998. My work at the Berkman Center included original research on all aspects of the Internet's design, operation, and use, with a focus on domain names, filtering, electronic commerce, and multimedia. In the course of this work, I designed a number of web pages, web sites, and web-based applications, and I sought to design these sites for maximum accessibility and ease of use.

8. Between 1998 and 2001, I had operational responsibility for the Berkman Center network, including setting up and maintaining server, network and PC equipment; providing technical support; and designing web content. My equipment responsibilities included configuring and maintaining multiple web servers as well as dozens of user PCs. In the course of this work, I assured the proper and stable operation of user PCs, including removing undesired software unintentionally or mistakenly installed on these PCs. My support responsibilities included answering

inquiries from faculty, staff, and students on subjects including PC reliability, web site operation and use, and software installation and removal. My web design responsibilities included creating Berkman Center web sites, web pages, and web-based applications for maximum accessibility and ease of use, as well as critiquing sites, pages, and applications designed by others.

9. Between 1996 and 1998, I was employed as a technical consultant at Stand for Children, a non-profit organization in Washington, DC. My responsibilities at Stand for Children included setting up server, network, and PC equipment; providing technical support; designing databases and database user interfaces; and designing web interfaces to database data. My equipment responsibilities included configuring and maintaining multiple servers as well as 60 user PCs. In the course of this work, I assured the proper and stable operation of user PCs, including removing undesired software unintentionally or mistakenly installed on these PCs. My support responsibilities included answering user inquiries on subjects including PC reliability, web site operation and use, and software installation and removal. My database responsibilities included designing appropriate data structures for centralized information storage, as well as designing functional and intuitive systems to allow users to enter, search, and use this data. I was also asked to critique systems and interfaces designed by others. My web design responsibilities included creating database-driven web sites and creating web interfaces to database content, as well as critiquing systems and interfaces designed by others.

10. Beyond my prior expert declarations, in matters listed below, I have written five articles related to spyware software, practices, and regulation.

1) *Documentation of Gator Advertisements and Targeting* (May 2003, http://cyber.law.harvard.edu/people/edelman/ads/gator) analyzes Gator's method of communications from users' computers to servers, and interprets these communications to understand which ads may be shown under which circumstances.

2) *Methods and Effects of Spyware* (March 2004, http://www.benedelman.org/spyware/ftc-031904.pdf) reports the personal information transmitted by programs including those made by WhenU, as well as offering more general analysis as to installation methods, advertisement display frequency, security risks, measurement complexities, and related matters.

3) *A Close Reading of Utah's Spyware Control Act* (February 2004, http://www.benedelman.org/spyware/utah-mar04) analyzes the specific provisions of the Spyware Control Act, traces its requirements and likely effects, and evaluates concerns offered by selected critics of the act.

4) *WhenU Spams Google, Breaks Google "No Cloaking" Rules* (May 2004, http://www.benedelman.org/spyware/whenu-spam) presents WhenU web pages in violation of search engine rules, their effects in boosting visibility of

pro-WhenU content at the expense of critics, and search engines' response to the presence of these pages.

5) *WhenU Copies 26+ Articles from 20+ News Sites* (May 2004, http://www.benedelman.org/spyware/whenu-copy) captures scores of news articles copied in full to a dozen WhenU web servers, without any mention of authorization from the respective rights-holders, and without even their original copyright notices.

Prior Expert Testimony

11. I have been retained as a consulting expert in a number of pending and completed matters, and I have provided oral expert testimony in three matters.

12. In 2000, I was asked by the National Football League to study the security systems and methods of transmission used by iCraveTV, a Canadian company retransmitting American network television content over the Internet. My work for the National Football League investigated the means of determining the geographic location of users receiving certain streaming video content as well as the nature and effectiveness of security systems restricting access to that content. My work culminated in providing oral testimony in the United States District Court for the Western District of Pennsylvania in a lawsuit captioned *National Football League, et al., vs. TVRADIONOW Corporation, et al.*, No. CIV.A. 00-120 and 00-121, 2000 U.S. Dist. LEXIS 1013 (W.D. Pa. 2000).

13. In 2000, I was asked by the American Civil Liberties Union to study the design of certain commercial Internet filtering products. My work for the ACLU investigated the design of the Internet, the implementation of computer networks, and the capabilities of proposed methods of filtering access to certain types of Internet content. In 2002, my work culminated in qualification as an expert in the United States District Court for the Eastern District of Pennsylvania, where I provided oral testimony in a lawsuit captioned *Multnomah County Public Library v. United States of America*, No. CIV.A. 01-1322, 2002 WL 1126046 (E.D. Pa. 2002).

14. In 2001, a group of media companies asked me to study the method of operation of software provided by The Gator Corporation. Like software provided by WhenU, Gator software shows targeted pop-up ads according to users' web browsing activities. My work for these media companies investigated the methods of advertising display used by Gator as well as its methods of installation and targeting. I served as an expert in the lawsuit captioned *Washingtonpost.Newsweek Interactive Company, LLC, et al. v. The Gator Corporation*, No. Civ.A. 02-909-A (E.D. Va. 2002).

15. In 2003, Quicken Loans and Wells Fargo asked me to study the method of operation of software provided by WhenU. My work for Quicken Loans and Wells Fargo investigated the design of WhenU software, including the specific method of targeting of particular WhenU advertisements to be shown when users visit particular web sites. I served as an expert and gave oral testimony in the lawsuit

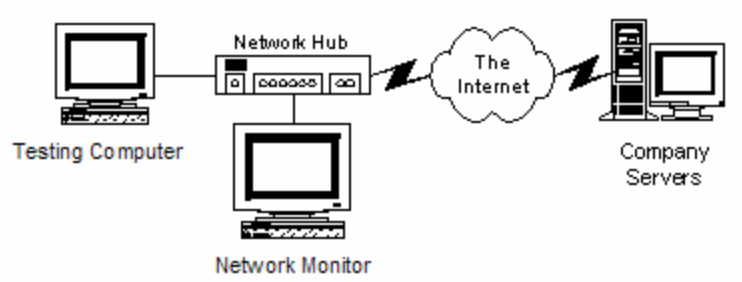
captioned *Wells Fargo & Company, et al., v. WhenU.com, Inc.*, 293 F. Supp.2d 734 (E.D. Mich. 2003).

Methodology

16. My knowledge of spyware software results from three separate sources. First, I have observed spyware as installed on ordinary computers in homes, offices, libraries, and other public areas, and I have discussed the programs with ordinary users. These methods give me a sense of the typical effects of the programs, as installed on ordinary computers and as perceived by ordinary users. Second, I have monitored the effects of spyware on computers in my lab, including making screen shots and video captures. Finally, again using dedicated computers in my lab, I have tracked the effects of spyware software on computers' file systems, registries, memory, and network transmissions.

17. My method of monitoring network communications of computers in my lab bears special mention for at least two reasons. First, it is subtle, sometimes misunderstood as some sort of "hacking." Second, it is powerful, allowing key insights into the method of operation of networked software programs.

18. By arranging the computers in my lab in the manner shown below, I can perform a procedure called network monitoring. This procedure lets me view and record programs' transmissions over my Internet connection. The diagram below demonstrates the way in which my computers are arranged in my lab:




19. As shown in the diagram above, all communications from the testing computer must pass through a network hub on their way to the Internet. My network monitor computer, also connected to that hub, sees all such communications and preserves them for my subsequent review.

20. This monitoring technique allows me to learn what information spyware software obtains from its company servers and what information spyware software sends back to those servers. Using network monitoring software, I can record all network communications, allowing careful and detailed analysis after the fact, even if communications occur quickly. Much of the discussion that follows uses facts I learned via this method of network monitoring.

21. In preparing the statements and opinions in this declaration, I have relied on absolutely no confidential information received from WhenU or Claria, e.g. in the course of prior litigation against these companies. In the course of the WashingtonPost matter referenced above, I received documents labeled confidential by Claria. In the course of the Quicken Loans and Wells Fargo matter referenced above, I was present during courtroom proceedings that were sealed to the public. But these documents and proceedings were in no way related to my ability to

conduct network monitoring of spyware software, and these documents and discussions do not form the basis of the conclusions expressed in this declaration.

22. My methods are consistent with those generally used by other technical analysts – such that others could derive these results independently. Indeed, I have reason to believe that other researchers have reached similar conclusions, independently from me and in some instances before me.

The Internet Generally

23. The Internet is a global network of millions of interconnected computers. The World Wide Web is a portion of the Internet especially suited to displaying images and sound in addition to text. Much of the information on the World Wide Web is stored in the form of "web pages" which can be accessed through a computer connected to the Internet (via a commercial Internet service provider or "ISP") and equipped with a computer program called a browser. Leading web browsers include Microsoft Internet Explorer and Netscape Navigator. "Web sites" are locations on the World Wide Web containing collections of web pages. A web page is identified by its unique Uniform Resource Locator or "URL" (e.g. http://www.uscourts.gov), and a URL ordinarily incorporates its site's "domain name" (e.g. uscourts.gov).

24. Users view web pages through web browsers. Technical staff of a web site may be able to view a web page's code as retrieved directly from their web server's hard disk, without the use of an intervening web browser. However, ordinary users lack the skills, tools, and access privileges to do so. In any case, a web page viewed

in this way typically lacks images and links. Accordingly, it is meaningless to speak of the appearance of a web site in the abstract. Instead, it is necessary to consider web sites as actually viewed in leading web browsers installed on users' computers.

Spyware Generally

25. The term "spyware" refers to a broad class of software that is installed on users' computers and performs functions including, typically among others, monitoring users' activities. Spyware programs also typically perform other functions, which vary from program to program, but often include transmitting personal information to remote web sites; adding undesired icons or links to users' desktop, Favorites list, or other locations; installing other programs; and showing pop-up advertisements.

26. The term "spyware" does not include functionality delivered without the installation of software on users' computers. For example, the term "spyware" is not properly used to refer to the ordinary pop-up ads shown by web sites when users visit those sites. These ordinary pop-up ads are shown using only code in web sites' own web pages, without any software installed on users' PCs.

27. The term "spyware" is also not properly used to refer to "cookies." Cookies are data files that web sites can place on a user's PC so as to be able to recognize the user if he later returns to that web site. These cookies are not properly classified as spyware because they operate only within the limited parameters permitted by web browsers. In particular, a web site cannot use cookies to learn anything about the

user other than what the user has told that site either explicitly (e.g. by filling out a form) or implicitly (e.g. through web browsing and purchasing habits). In contrast, spyware can track users' behavior across all web sites, and spyware can interact with users in arbitrary ways not constrained by browser design.

WhenU Software Generally

28. Software written and distributed by WhenU causes the display of popup advertisements when a user attempts to view certain third-party web sites. WhenU causes the display of these popup advertisements without the permission of the third-party web sites and without payment to them. WhenU's popup advertisements cover portions of web sites created by third parties, preventing users from viewing these sites as their designers intended.

29. The design of WhenU software allows WhenU to cause advertisements to be displayed subsequent to user requests for any web site desired. WhenU popup advertisements often target the web sites of the advertisers' competitors. WhenU is equally capable of targeting advertisements at web sites that do not sell advertising or that refuse to permit certain types of advertising.

30. WhenU software operates in three steps. First, WhenU software gets installed on a user's computer. Second, WhenU software monitors which web pages and web sites a user views. Finally, WhenU software shows ads according to which web pages and sites a user views.

The Advertisements Displayed by WhenU Software

31. When computer users visit certain web sites on a computer with WhenU software installed, WhenU causes on-screen display of designated advertisements. These advertisements typically cover portions of the content that the creators of the requested web sites intended to be displayed. Although these advertisements can be moved or removed by a computer user, the user's on-screen display remains altered by WhenU's advertisements unless and until the user does so.

32. WhenU's popup advertisements typically appear at approximately the same time the web page that the user has requested is downloading onto the user's computer and opening on the user's computer screen. As a result of WhenU's popup advertisements, users ordinarily do not see the requested web page in the manner that the web site owner intended to display it. Instead, users see the WhenU popup advertisement superimposed above a portion of the web page, covering and concealing some of the content the site owner intended to be displayed on the requested web page. In order for a user to see the requested web page displayed as intended by the site's creator, the user must move his mouse to each popup advertisement and click the mouse to close each advertisement, thus delaying access to the site's content.

33. Because WhenU's advertisements appear on a user's screen simultaneously, or nearly simultaneously, with the downloading and opening of the requested web

page of the targeted web site, the WhenU popup advertisements appear to be an integral and fully authorized part of the original underlying web page.

34. WhenU's advertisements differ substantially from the American Express billing-insert offers Avi Naider describes in his affidavit (paragraph 4). For example, the origin of Amex's advertising inserts is intuitive and easy to understand: They come in an envelope along with other Amex content. In contrast, WhenU's advertisements appear at the same time as content from web sites users request. Because Amex advertisements arrive with Amex content, consumers are reinforced in their belief that the advertising at issue is delivered by Amex. In contrast, when WhenU delivers an advertisement that appears above and at the same time as a third-party web site, many users cannot help but conclude that the advertisement is part of or is affiliated with that third-party web site. In addition, Amex's advertising inserts are presented to customers well after they have completed the purchases that give rise to Amex's targeting decisions. In contrast, WhenU's advertisements interrupt users as they are working towards making a purchase. In my judgment, a better analogy for WhenU's advertisements is a competitor who walks into a store and interrupts the customer as the customer hands his purchase to the checkout cashier.

WhenU's Methods of Operation and Targeting

35. WhenU's methods of operation and targeting are discernible from hands-on testing of WhenU's software as well as from detailed inspection of the data files WhenU sends and receives over users' Internet connections.

36. As an empirical matter, hands-on use of computers with WhenU software makes it clear that WhenU targets its ads according to user activities. Visit a travel web site, and WhenU is likely to show ads for a competing travel web site. Visit one car rental company and WhenU is likely to show ads for another.

37. This business model – showing ads for a site's direct competitors when users visit that site – is consistent with WhenU's prior statements to the public. WhenU frames these practices as "precision targeting" and "contextual marketing,"[1] but the empirical reality is that when users visit one web site, WhenU is likely to show ads for the site's competitors.

Spyware Installation is Not Consensual

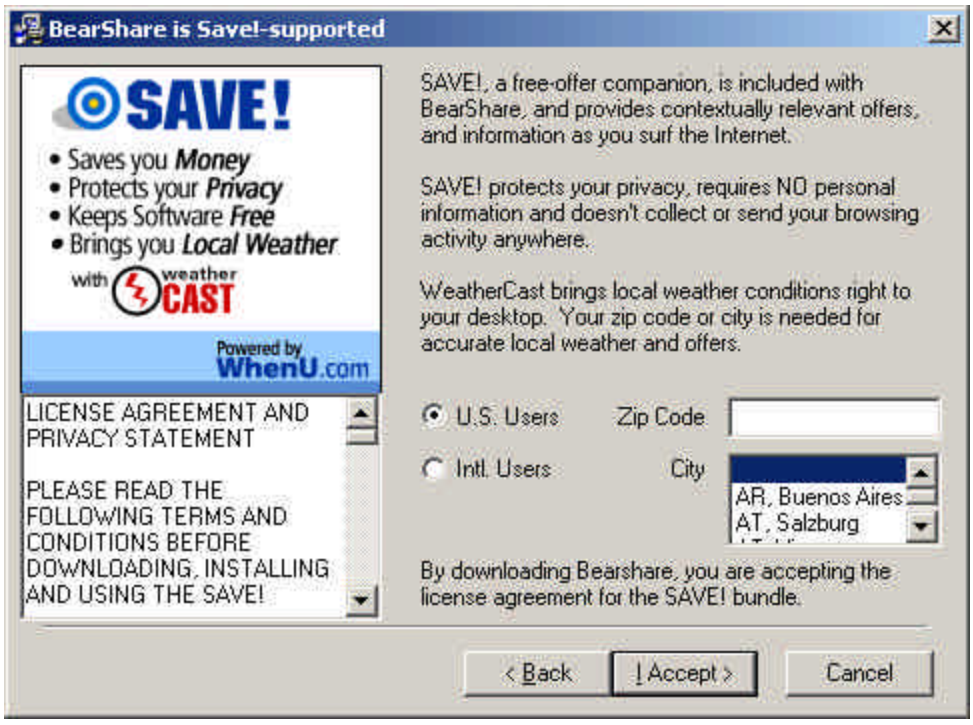
38. In general, spyware software is unwanted: Users receive spyware programs, including software from WhenU, without knowingly consenting to its installation.

39. Users typically obtain spyware software in one of two distinct ways. These are: 1) As an unrequested add-on provided with a third-party program a user

[1] http://www.whenu.com , checked May 3, 2004

requests; 2) As an unrequested addition to a user's computer as the user browses an unrelated web site.

40. First, some users obtain spyware (including WhenU software) via bundles with third-party applications, including peer-to-peer filesharing programs used to copy music, video, and other files. A user seeking any of these third-party programs will often receive spyware software also, and in the past it was often impossible to obtain the desired third-party software without also obtaining spyware. Many of these third-party programs install spyware without a user's knowledge or consent, without displaying license agreements, and/or without displaying the license agreements in a time, format and style in which it can be meaningfully reviewed and evaluated. For example, BearShare (version 4.4.3, the latest version available as of April 2004) places the WhenU license agreement in a subwindow so small that it is broken into forty four distinct pages of text, of which the first is shown below.




41. The remainder of the BearShare installer, including each of the other forty three distinct pages of WhenU license, is available on the web at http://www.benedelman.org/spyware/whenu-license .

42. Second, some users obtain spyware software (including WhenU software) via a process often called "drive-by downloads." When users visit certain web pages, those pages may cause the user's computer to download and offer to install spyware software – all without a user's prior approval. Under the default configuration of most computers, drive-by installations cause the display of a single popup message box that sometimes offers a link to a program's license agreement. However, a user can click the "yes" button to complete the installation without seeing the license, not to mention reading it or understanding it. In addition, depending on the configuration of a user's computer, some spyware may be installed without the

user's knowledge or consent and without the display of even a single confirmation screen or reference to a license agreement.

43. Drive-by downloads are, in my judgment, inherently misleading. When a user is merely reading some other, unrelated web site, a pop-up message appears, suggesting to the user that the specified program is necessary in order to view the requested web site. Users' belief to this effect is well-founded; Microsoft developed the auto-install process precisely to easily provide plug-in software actually required to view certain web pages. At a recent FTC workshop, a senior Microsoft staff person characterized drive-by downloads as "tricks" and "not what we [Microsoft] intended."[2] In addition, drive-by downloads cause software to be downloaded to users' computer even before the user is told that software is available for installation, and certainly before the user has consented to such installation.[3]

44. When users receive WhenU software via drive-by download, they may or may not consent to WhenU's license agreements. For one, users may never even see WhenU's license agreement, because WhenU's drive-by installer does not show WhenU's license to users, even in part. Instead, WhenU's installer merely offers users a link to the license. In addition, even users who specifically seek out the

---

[2] Jeffrey Friedberg, Director of Windows Privacy, Microsoft Corporation. Oral comments to the FTC - Washington DC, April 19, 2004.

[3] *Methods and Effects of Spyware*, http://www.benedelman.org/spyware/ftc-031904.pdf, paragraph 36, checked May 16, 2004.

license agreement, by clicking on the link, may be unable to view it. Consider the result shown in the video called WhenU-Driveby-License_no_scroll-051504.wmv video on the CD attached to my declaration. This video shows that in a WhenU drive-by installation of May 15, 2004, WhenU's license agreement was provided in a window too small to show the entire license, without scroll bars to allow the user to browse to see the rest of the license.

45. Both bundling and drive-by downloads cause spyware software to be installed as a mere byproduct of some other activity a user sought to complete – installing unrelated software, or viewing an unrelated web site. These methods of distribution are, in my opinion, a large part of the reason why, in my experience, users tend to be uncertain and confused as to where and how they obtained spyware.

46. WhenU uses both of the practices described above, as well as other installation practices that cause users to obtain their software with even less notice or consent. For example, WhenU's software is automatically installed by "IE PLUGIN" from a company calling itself "IE PLUGIN LTD," a product that itself uses the drive-by download installation strategy. IE Plugin purports to offer users a link to the license agreements for IE Plugin and the programs it installs, but in fact that link is sometimes defective and wholly non-operational. As a result, even users who specifically seek out the license for IE Plugin (and its bundled programs) cannot obtain that license, and users who install IE Plugin necessarily do so without first reviewing IE Plugin's license or the licenses of the various programs IE Plugin

then installs. Users who receive WhenU software in this way cannot possibly have seen – not to mention consented to – WhenU's license agreement. On the CD attached to my declaration, the video Driveby-WhenU_bundle-050204.wmv shows installation of WhenU in this way, while the video Driveby-WhenU_bundle-050204-nolicense.wmv demonstrates the defective design of IE Search's license display technology.

47. The net effect of these various misleading installation techniques is that users overwhelmingly do not know what spyware they have installed, or even that they have spyware installed, not to mention having consented to the installation of such software. PC Pitstop, a web site that provides technical support to users with computer problems, showed a survey to users whose computers were diagnosed as including software from WhenU. According to PC Pitstop's survey results, more than 87% of WhenU users do not even know that they have WhenU software installed.[4]

The Effects of Spyware in Utah

48. In my judgment, spyware poses a substantial harm to users and companies in Utah.

49. To users in Utah, spyware has numerous negative effects. Spyware slows computers, as I have confirmed in my own research and as other experts have also

[4] http://www.pcpitstop.com/spycheck/whenu.asp, checked May 3, 2004.

confirmed.[5] Spyware slows users' Internet connections.[6] Spyware sends personal information to remote web sites. Indeed, my own research indicated that WhenU's software makes transmissions precisely contrary to its own license agreements.[7]

50. These problems are particularly pronounced as to public computers. In my experience, spyware is especially prevalent on computers available to the public, including in primary and secondary schools, as well as in public libraries. My testing of earlier this year confirmed that multiple computers in the Utah State Legislature were infected with spyware, in fact some with software provided by

---

[5] See e.g. PestPatrol comments to FTC, http://www.ftc.gov/os/comments/spyware/040423pestpatrolstatement.pdf , checked May 3, 2004. "Testing earlier this month at the PestPatrol research laboratory revealed that the addition of just one adware pest slowed a computer's boot time (the amount of time it took to start up and function) by 3.5 times. Instead of just under 2 minutes to perform this operation, it took the infected PC close to 7 minutes to start up."

[6] See e.g. PestPatrol comments to FTC, http://www.ftc.gov/os/comments/spyware/040423pestpatrolstatement.pdf , checked May 3, 2004. "We also tested web page access, and again it took much longer once a pest was added to a clean machine. Almost five times longer in fact for a web page to load on an infected PC. The pest also caused 3 web sites to be accessed, rather than the one requested, and caused the PC to transmit and receive much greater amounts of unknown data."

[7] Methods and Effects of Spyware, Edelman comments to FTC. http://www.benedelman.org/spyware/ftc-031904.pdf , pages 3-4, checked May 3, 2004. "I have reviewed the WhenU privacy policy, and I have concluded that WhenU violates this policy when it transmits to its servers some of the specific URLs viewed by WhenU users. … The policy reads … : 'As the user surfs the Internet, URLs visited by the user … are NOT transmitted to WhenU."

WhenU, although in each instance the assigned user of the corresponding computer denied knowledge of or consent to its installation.

51. Utah companies also suffer as a result of spyware programs. When Utah companies are targeted by spyware, the spyware pop-up ads reduce the companies' ability to present their web sites to their customers, in Utah and beyond, in the ways that the companies intended. Furthermore, the pop-up ads have a detrimental effect on users' perception of the companies. A recent survey by D2 Research indicated that popup ads cause users to have a less favorable opinion of the sites on which the ads appear.[8] My discussions with staff of targeted sites indicate that targeting had significant, quantifiable harm on their business.

The Actions At Issue and the Harm At Issue Both Take Place within Utah

52. Spyware software is installed on computers within Utah. Many of these computers are permanently installed in Utah, e.g. permanently placed in Utah businesses, homes, schools, and libraries.

53. In the relevant sense, spyware resides permanently on the computers on which it is installed. Of course, some spyware can be removed, and in that sense certain spyware programs are not permanently present. But when spyware is installed on a computer, it remains on the computer for the indefinite future – until

---

[8] http://www.ftc.gov/os/comments/spyware/040323hertzllbeanwithpopupsurvey.pdf page 7, checked May 3, 2004. "33.2% of respondents said that the appearance of the pop-up ad would cause them to have a less favorable opinion of the website (vs. only 2.4% who said it would give them a more favorable opinion)."

the computer is discarded or erased, or until the owner of the computer takes special steps to remove the spyware. Spyware is not a mere transitory visitor to a computer, like a web page briefly shown on screen but shortly replaced with a new page. Rather, spyware is a permanent addition, which will remain installed even if a computer is turned off and turned back on.

54. Relevant actions taking place within Utah include the offer of the software for installation, the installation of the software, the use of the software by the user, and the operation of the software to cause causing the results prohibited by the Act.

Spyware Makers Can Easily Comply with the Act by Failing to Install in Utah or by Modifying Their Behavior When Installed In Utah

55. Spyware makers can easily comply with the Spyware Control Act, without modifying their behavior elsewhere. They can do this both by modifying their software so as not to install in Utah, so as to operate differently (or not at all) when installed in Utah, and/or so as not to target advertisements at web sites run by Utah companies.

56. Consider the WhenU installer, as bundled with the current version of BearShare. As shown in the screenshot at paragraph 40 above, the WhenU installation program asks the user for the user's zip code. If the user enters a zip code in Utah, the WhenU installer could simply reconfigure WhenU's software in a way that complies with the Act. Alternatively, if WhenU declines to modify its software to achieve such compliance, the WhenU installer could simply fail to install WhenU's software. WhenU already asks users for the sole piece of

information necessary to make this determination – the user's zip code – and WhenU can readily proceed on the basis of that answer.

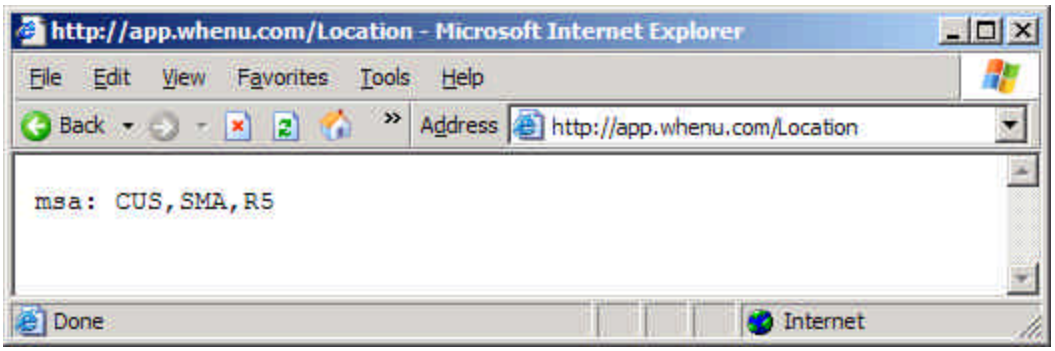
57. Even programs that do not currently ask the user for his zip code could readily comply with the Spyware Control Act. For one, the programs could be modified so that they do ask for state, zip code, area code, or other location-identifying information. These additions would be straightforward, as would be the simple logic to install or not install the software according to the user's answer.

58. Alternatively, programs could use the user's IP address (Internet Protocol address) to determine the user's geographic location. While such a determination is not always perfectly accurate, it is in many instances sufficiently accurate to draw a robust inference as to the user's location. For example, if the user is connected to the Internet through the facilities of the Utah Legislature, the user's IP address would be associated with a domain name that included the identifier "utah.gov." Similarly, a user from Brigham Young University would have an IP address associated with a domain that included "byu.edu." On this basis, it would be easy to determine that the user is almost certain to be located in Utah. Commercial services provide this service in an automated, centralized implementation.[9]

---

[9] See e.g. Quova GeoPoint, http://www.quova.com/shtml/technology/tech_geopoint.shtml , checked May 3, 2004. GeoBytes IP Locator, http://www.geobytes.com , checked May 3, 2004. NetGeo, http://www.netgeo.com/ , checked May 3, 2004.

59. In fact, some WhenU software already performs precisely this sort of IP address lookup in order to determine where users are located, without asking users for their zip codes. At the URL http://app.whenu.com/Location (note case-sensitivity), WhenU's web server tells a user his or her location – country (two-letter abbreviation preceded by the letter "C") and state (two-letter abbreviation preceded by the letter "S"). Certain WhenU software automatically asks the WhenU web server for this /Location information, then stores this data in the "registry" of users' computers, and periodically transmits it to WhenU servers. With location data already collected, stored, and tracked by WhenU, it would be particularly puzzling for WhenU to claim an inability to alter its behavior according to users' apparent locations.




60. Because WhenU's software is location-aware, it differs substantially both from the other Internet-transmitted content that has been the subject of earlier litigation (i.e. *ACLU*) and from the other chattels that have been the subject of interstate commerce claims. *See, e.g., Southern Pacific Co. v. Arizona*, 325 U.S. 761 (1945) (passenger trains). Static web pages and physical chattels are incapable

of altering their behavior when they cross state lines: The harmful content in *ACLU* is the same when it reaches other states as when it reaches New Mexico, and the passenger railcars in *Southern Pacific* are the same when in California as in Arizona. But here the object of regulation has within it the active capacity to reshape itself – to disable itself, or to otherwise modify itself – based on its location, which it is capable of determining and which, in the case of WhenU and as to numerous other spyware programs also, the software in fact already actively knows.

61. In addition, the Internet-transmitted information in *ACLU* was generated by access to a passive website located in a different state. The website operator in *ACLU* was unable to prevent access to its site from persons outside of New Mexico. In this case, spyware distributors can take appropriate steps to ensure that they do not download spyware in violation of the Act in Utah.

Spyware Makers Can Easily Comply with the Act by Avoiding Targeting Utah Companies

62. Spyware designers can also readily modify their programs to avoid showing context-triggered pop-up advertisements that cover the sites of Utah companies. WhenU's software already includes features to avoid displaying popup ads on designated web sites. WhenU has been ordered to use these features in prior litigation.[10] My prior inspection of WhenU software has shown that WhenU

[10] Preliminary injunction order in *1-800 Contacts, Inc., v. WhenU.com and Vision Direct, Inc.* 02 Civ. 8043 (S.D.N.Y., Dec. 22, 2003).

maintains and actively updates a list of sites not to target, including its own site, its competitors' sites, sites of companies that have sued or threatened to sue WhenU, and sites of companies that have sued or threatened to sue WhenU's competitors.

63. In any event, WhenU significantly overstates the number of companies that would have to modify their behavior to comply with the Act, both as to the modifications discussed in this section and as to those of the preceding section. Of the legitimate companies that write software that transmits users' usage data for legitimate reasons, the overwhelming majority already provide notice, obtain consent, and include uninstall routines. Such companies need not change anything about their products. Only the companies that currently fail to provide notice, consent, and uninstall, or that show context-triggered popups that cover web sites, would have to modify their behavior to comply with the Act's requirements.

WhenU's Existing Business Relationships Make It Particularly Easy for WhenU to Differentially Treat Utah Users or to Avoid Serving Utah Users

64. WhenU's use of sophisticated "content distribution services" (CDSs) to distribute its "directory" (which advertisements to display under which conditions) means WhenU could comply with the Act without changing any WhenU SaveNow code. To proceed in this way, WhenU need only tell its CDS partners never to distribute the directory to users in Utah – a service its CDS partners already provide in their ordinary course of business.

65. In my examinations, WhenU obtains its directories from CDSs Akamai and Speedera, two leading CDS services. Both of these companies offer geolocation

targeting services that can provide different content depending on users' locations. They describe these services as follows: "EdgeSuite Content Targeting provides the following data: Geographic Origin (Country, region, city, DMA, MSA, etc.) ... Applications for Content Targeting ... Include ... Controlled Distribution - Ensure that your digital goods are not delivered to restricted geographies."[11] "Rights Management - GeoInsight enables you to comply with licensing and distribution agreements and/or legal restrictions that apply to different states or countries by providing the capability to selectively block users based on geography."[12]

66. While the public materials I have reviewed from Akamai and Speedera's web sites do not specifically speak to the accuracy of their geo-targeting systems, they both state that the systems can be used for rights management and regulatory compliance purposes. From my conversations with senior Akamai staff, I believe Akamai's methods to be extremely robust and reliable as to the overwhelming majority of Internet users.

Security Flaws in WhenU Products and in Other Spyware Products

67. Legislators and other policy-makers are rightly concerned about security flaws in spyware products, including in software from WhenU. Badly-designed

---

[11] *Akamai Edgescape,* http://www.akamai.com/devnet/pdf/EdgeSuite_Service_Description.pdf , pages 18-19, checked May 16, 2004.

[12] *Speedera Geo-targeting,* http://www.speedera.com/primary/services/geotarget.htm , checked May 16, 2004.

spyware can expose users to serious security vulnerabilities, including allowing attackers to send the user's personal data or behavior to any server on the Internet; to add, modify, or delete files; to install other programs (including other spyware programs); or to use the computer to send junk email or cause a denial of service attack.

68. These kinds of vulnerabilities have previously been found in other spyware programs. For example, *Measurement and Analysis of Spyware in a University Environment*[13] presents serious security vulnerabilities in widely-deployed software from both Claria and eZula.

69. My testing indicates that certain software from WhenU contains similar vulnerabilities. I have notified WhenU staff of this problem, affecting software on WhenU's ordinary public web site until mere days ago. WhenU staff have generally confirmed the scope and effect of the vulnerability I found, and they assure me that they have since corrected the problem. I am presently in the course of completing my write-up of this security vulnerability, and I expect to release my research to the public in the coming weeks.

Response to the Affidavit of Avi Naider

70. I have reviewed the Affidavit of Avi Naider, dated April 12, 2004.

---

[13] Saroiu, Stefan, Steven D. Gribble, and Henry M. Levy. *Measurement and Analysis of Spyware in a University Environment.* http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf , checked May 12, 2004.

71. Mr. Naider's declaration is false in as much as it claims that WhenU does not collect information concerning the history of the web pages users visit. In my *Methods and Effects of Spyware*,[14] I demonstrate that WhenU collects and transmits to its servers precisely this information, whenever WhenU shows an advertisement.

72. Mr. Naider claims that any change WhenU makes would have to be made system-wide, not just in Utah. (Paragraph 52) This is false. As shown in paragraph 40 of my declaration and discussed in the section entitled *Spyware Makers Can Easily Comply with the Act by Modifying Their Behavior When Installed In Utah or by Modifying Their Behavior When Installed In Utah*, WhenU software knows where it is located because it asked users for this information. It would be a simple change for WhenU to refuse to install if the user specified a zip code in Utah, or for WhenU to operate in a different way if the user specified a zip code in Utah.

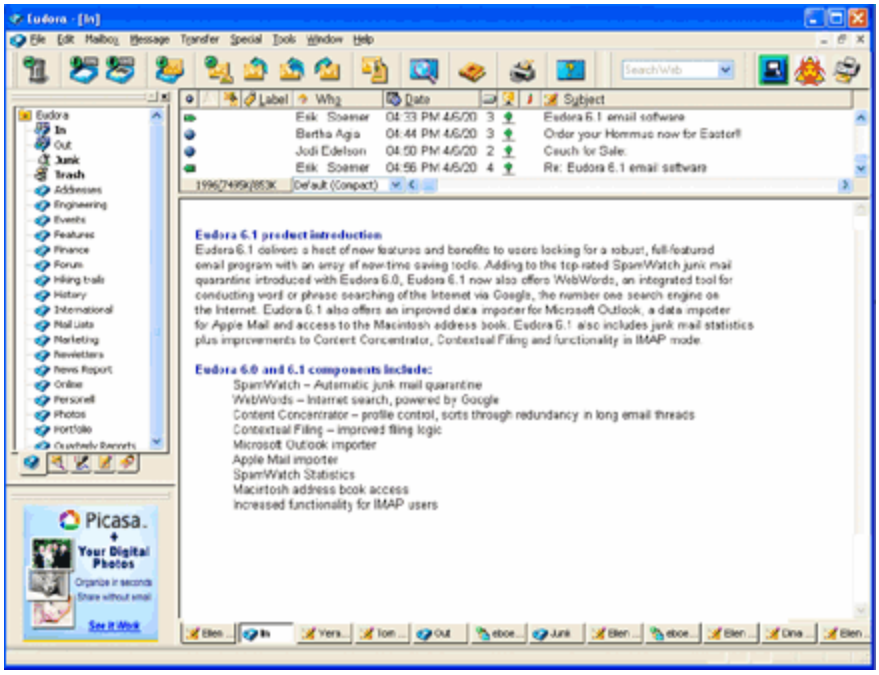
73. The fact that the Act exempts pop-ups from search engines and web sites is not "ironic" as Naider suggests (paragraph 62). Rather, this approach precisely reflects that search engines and web sites do not pose the same threat as spyware to users' privacy and to the reliability of their computers.

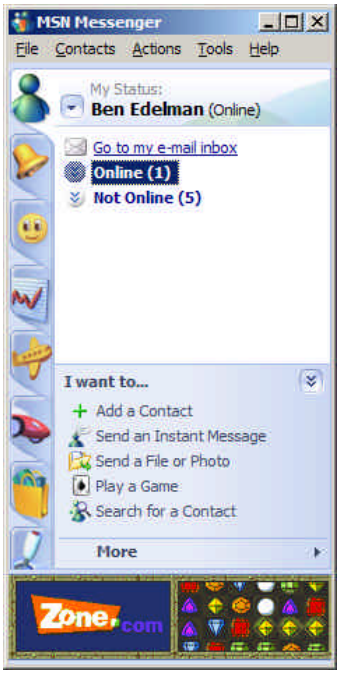
74. The Act will not have "terrible consequences for the Internet" (¶66) by preventing "software based advertising" (¶67). Contrary to Naider's declaration, the

---

[14] http://www.benedelman.org/spyware/ftc-031904.pdf , paragraphs 12-17, checked May 3, 2004.

Act does not prohibit all advertisement-supported software; it merely prohibits advertisements that are context-triggered and cover web sites without their permission. Other kinds of advertisement-supported software remain perfectly permissible under the Act. For example, programs remain free to display advertisements within their own application windows, an approach used by the free version of Eudora and by MSN Messenger (both shown below).




Response to the Affidavit of Arnold Reinhold

75. I have reviewed the Affidavit of Arnold Reinhold, dated April 11, 2004.

76. Reinhold is in error when he claims that software distributors cannot reliably determine in which state a user resides upon downloading software (paragraph 31). The services I describe in paragraphs 59 and 64 to 66 are capable of making such a determination. These services do not claim 100% accuracy, but they are sufficient for ordinary commercial purposes. For example, Major League Baseball apparently

uses Quova technology to determine a user's location, on a state-by-state basis, to avoid transmitting webcasts in violation of local broadcast rights.[15] In any event, spyware programs can easily ask users for their locations, as a backup or secondary approach. For example, WhenU's WeatherCast already asked for a user's Zip Code prior to installation.

77. Reinhold's interpretation of the Act is in error in as much as, in paragraph 36, he discusses provisions (4)(a) and (4)(b)(i) alone, without noting the exceptions in (4)(c), even as he acknowledged those exceptions a mere two paragraphs earlier. As a result, Reinhold's examples of iTunes is only an example of a program required to satisfy provision (c), not an example of a program in fact in violation of the Act as drafted. From my initial review of iTunes, I am confident that it already satisfies the requirements of (c). To the extent that I understand the vague additional examples Reinhold mentions in paragraph 36, I believe none is in fact in violation of the Act.

78. Neither is the parental monitoring software IamBigBrother.com in violation of the Act. From my initial review of this program, it includes a license agreement and it can readily be removed by the computer owner who initially installed it. As a

---

[15] http://www.quova.com/shtml/story/story_jack.shtml , checked May 3, 2004. "Quova's technology helps MLB.TV generate new webcast revenues without infringing on local broadcast rights, which are crucial to the teams and local stations. This historic initiative wouldn't be possible without Quova's 99% accuracy verification of every viewer's location."

result, it satisfies both requirements in section (4)(c) and is not spyware within the meaning of the Act.

79. In paragraph 33, Reinhold refers to a letter from AOL and other companies that claims certain errors in the Act. I have reviewed this letter at great length and believe its concerns to be misplaced. My analysis of the letter is posted to the web in my *A Close Reading of Utah's Spyware Control Act*.[16] In short, I believe AOL and its cosignators made the same analytical error flagged in the preceding paragraphs – failing to fully understand how the various sections of the Act fit together, and therefore failing to correctly determine which software is in fact subject to the Act.

80. I declare under penalty of perjury under the laws of the State of Utah that the foregoing is true and correct.

Executed this ___ day of May, 2004, at Boston, Massachusetts.

Benjamin Edelman

[16] http://www.benedelman.org/spyware/utah-mar04/ , checked May 3, 2004.