

1 Blake D. Miller (4090)  
Paxton R. Guymon (8188)  
2 Joel T. Zenger (8926)  
**MILLER MAGLEBY & GUYMON, P.C.**  
3 170 South Main Street, Suite 350  
Salt Lake City, Utah 84101  
4 Telephone: (801) 363-5600  
Facsimile: (801) 363-5601  
5 Special Assistant Attorneys General

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

11 Attorneys for Defendants

---

12 **IN THE THIRD JUDICIAL DISTRICT COURT**  
13 **SALT LAKE COUNTY, STATE OF UTAH**

---

15 **WHENU.COM, INC.** a Delaware  
16 corporation,

17 **Plaintiff,**

18 vs.

19 **THE STATE OF UTAH, a body**  
**politic, OLENE S. WALKER, in**  
**her official capacity as Governor**  
**of Utah., and MARK**  
20 **SHURTLEFF in his official**  
21 **capacity as Utah Attorney**  
**General,**

22 **Defendants.**

**AFFIDAVIT OF**  
**BENJAMIN G. EDELMAN**

**Civil No. 040907578**

**Honorable Joseph C. Fratto**

23  
24  
25  
26  
27  
28



1 culminated in expert testimony, they are detailed in the section that follows, *Prior*  
2 *Expert Testimony*. Representative examples of my non-litigation consulting projects  
3 include tracking large-scale domain name registrations that might be taken to  
4 infringe on the rights of others, assisting web sites blocked by China in  
5 reconfiguring their servers to be reachable to users in that country, and advising  
6 clients as to the technical merits of certain web-based business investments.  
7

8  
9 7. Until January 2004, I was employed as a Student Fellow at the Berkman  
10 Center for Internet & Society at Harvard Law School. I had been employed as a  
11 technical consultant at the Berkman Center since May 1998. My work at the  
12 Berkman Center included original research on all aspects of the Internet's design,  
13 operation, and use, with a focus on domain names, filtering, electronic commerce,  
14 and multimedia. In the course of this work, I designed a number of web pages, web  
15 sites, and web-based applications, and I sought to design these sites for maximum  
16 accessibility and ease of use.  
17  
18

19  
20 8. Between 1998 and 2001, I had operational responsibility for the Berkman  
21 Center network, including setting up and maintaining server, network and PC  
22 equipment; providing technical support; and designing web content. My equipment  
23 responsibilities included configuring and maintaining multiple web servers as well  
24 as dozens of user PCs. In the course of this work, I assured the proper and stable  
25 operation of user PCs, including removing undesired software unintentionally or  
26 mistakenly installed on these PCs. My support responsibilities included answering  
27  
28

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

7  
8 9. Between 1996 and 1998, I was employed as a technical consultant at Stand  
9 for Children, a non-profit organization in Washington, DC. My responsibilities at  
10 Stand for Children included setting up server, network, and PC equipment;  
11 providing technical support; designing databases and database user interfaces; and  
12 designing web interfaces to database data. My equipment responsibilities included  
13 configuring and maintaining multiple servers as well as 60 user PCs. In the course  
14 of this work, I assured the proper and stable operation of user PCs, including  
15 removing undesired software unintentionally or mistakenly installed on these PCs.  
16 My support responsibilities included answering user inquiries on subjects including  
17 PC reliability, web site operation and use, and software installation and removal.  
18 My database responsibilities included designing appropriate data structures for  
19 centralized information storage, as well as designing functional and intuitive  
20 systems to allow users to enter, search, and use this data. I was also asked to  
21 critique systems and interfaces designed by others. My web design responsibilities  
22 included creating database-driven web sites and creating web interfaces to database  
23 content, as well as critiquing systems and interfaces designed by others.  
24  
25  
26  
27  
28

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

- 3
- 4 1) *Documentation of Gator Advertisements and Targeting* (May 2003,  
5 <http://cyber.law.harvard.edu/people/edelman/ads/gator>) analyzes Gator's  
6 method of communications from users' computers to servers, and interprets  
7 these communications to understand which ads may be shown under which  
8 circumstances.
- 9
- 10 2) *Methods and Effects of Spyware* (March 2004,  
11 <http://www.benedelman.org/spyware/ftc-031904.pdf>) reports the personal  
12 information transmitted by programs including those made by WhenU, as  
13 well as offering more general analysis as to installation methods,  
14 advertisement display frequency, security risks, measurement complexities,  
15 and related matters.
- 16
- 17 3) *A Close Reading of Utah's Spyware Control Act* (February 2004,  
18 <http://www.benedelman.org/spyware/utah-mar04>) analyzes the specific  
19 provisions of the Spyware Control Act, traces its requirements and likely  
20 effects, and evaluates concerns offered by selected critics of the act.
- 21
- 22 4) *WhenU Spams Google, Breaks Google "No Cloaking" Rules* (May 2004,  
23 <http://www.benedelman.org/spyware/whenu-spam>) presents WhenU web  
24 pages in violation of search engine rules, their effects in boosting visibility of  
25  
26  
27  
28

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

3  
4 5) *WhenU Copies 26+ Articles from 20+ News Sites* (May 2004,  
5 <http://www.benedelman.org/spyware/whenu-copy>) captures scores of news  
6 articles copied in full to a dozen WhenU web servers, without any mention of  
7 authorization from the respective rights-holders, and without even their  
8 original copyright notices.  
9

10 Prior Expert Testimony

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

13  
14 12. In 2000, I was asked by the National Football League to study the security  
15 systems and methods of transmission used by iCraveTV, a Canadian company  
16 retransmitting American network television content over the Internet. My work for  
17 the National Football League investigated the means of determining the geographic  
18 location of users receiving certain streaming video content as well as the nature and  
19 effectiveness of security systems restricting access to that content. My work  
20 culminated in providing oral testimony in the United States District Court for the  
21 Western District of Pennsylvania in a lawsuit captioned *National Football League,*  
22 *et al., vs. TVRADIONOW Corporation, et al.,* No. CIV.A. 00-120 and 00-121, 2000  
23 U.S. Dist. LEXIS 1013 (W.D. Pa. 2000).  
24  
25  
26  
27  
28

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

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

17 15. In 2003, Quicken Loans and Wells Fargo asked me to study the method of  
18 operation of software provided by WhenU. My work for Quicken Loans and Wells  
19 Fargo investigated the design of WhenU software, including the specific method of  
20 targeting of particular WhenU advertisements to be shown when users visit  
21 particular web sites. I served as an expert and gave oral testimony in the lawsuit  
22  
23  
24  
25  
26  
27  
28

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

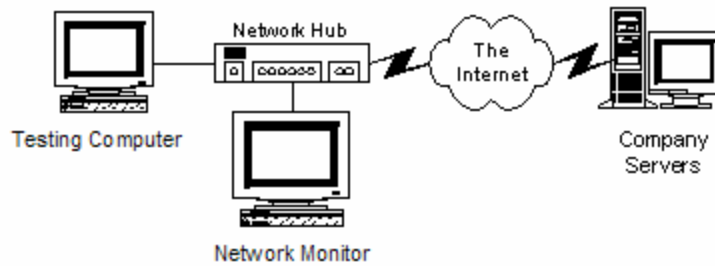
### 3 4 Methodology

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

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

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





1  
2  
3  
4  
5  
6 19. As shown in the diagram above, all communications from the testing  
7 computer must pass through a network hub on their way to the Internet. My  
8 network monitor computer, also connected to that hub, sees all such  
9 communications and preserves them for my subsequent review.  
10

11 20. This monitoring technique allows me to learn what information spyware  
12 software obtains from its company servers and what information spyware software  
13 sends back to those servers. Using network monitoring software, I can record all  
14 network communications, allowing careful and detailed analysis after the fact, even  
15 if communications occur quickly. Much of the discussion that follows uses facts I  
16 learned via this method of network monitoring.  
17

18  
19 21. In preparing the statements and opinions in this declaration, I have relied on  
20 absolutely no confidential information received from WhenU or Claria, e.g. in the  
21 course of prior litigation against these companies. In the course of the  
22 WashingtonPost matter referenced above, I received documents labeled confidential  
23 by Claria. In the course of the Quicken Loans and Wells Fargo matter referenced  
24 above, I was present during courtroom proceedings that were sealed to the public.  
25  
26 But these documents and proceedings were in no way related to my ability to  
27  
28

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

3  
4 22. My methods are consistent with those generally used by other technical  
5 analysts – such that others could derive these results independently. Indeed, I have  
6 reason to believe that other researchers have reached similar conclusions,  
7  
8 independently from me and in some instances before me.

### 9 The Internet Generally

10 23. The Internet is a global network of millions of interconnected computers. The  
11 World Wide Web is a portion of the Internet especially suited to displaying images  
12 and sound in addition to text. Much of the information on the World Wide Web is  
13 stored in the form of “web pages” which can be accessed through a computer  
14 connected to the Internet (via a commercial Internet service provider or “ISP”) and  
15 equipped with a computer program called a browser. Leading web browsers include  
16  
17 Microsoft Internet Explorer and Netscape Navigator. “Web sites” are locations on  
18 the World Wide Web containing collections of web pages. A web page is identified  
19  
20 by its unique Uniform Resource Locator or “URL” (e.g. <http://www.uscourts.gov>),  
21  
22 and a URL ordinarily incorporates its site’s “domain name” (e.g. [uscourts.gov](http://www.uscourts.gov)).

23 24. Users view web pages through web browsers. Technical staff of a web site  
24  
25 may be able to view a web page’s code as retrieved directly from their web server’s  
26 hard disk, without the use of an intervening web browser. However, ordinary users  
27  
28 lack the skills, tools, and access privileges to do so. In any case, a web page viewed

1 in this way typically lacks images and links. Accordingly, it is meaningless to speak  
2 of the appearance of a web site in the abstract. Instead, it is necessary to consider  
3 web sites as actually viewed in leading web browsers installed on users' computers.  
4

### 5 Spyware Generally

6 25. The term "spyware" refers to a broad class of software that is installed on  
7 users' computers and performs functions including, typically among others,  
8 monitoring users' activities. Spyware programs also typically perform other  
9 functions, which vary from program to program, but often include transmitting  
10 personal information to remote web sites; adding undesired icons or links to users'  
11 desktop, Favorites list, or other locations; installing other programs; and showing  
12 pop-up advertisements.  
13  
14

15 26. The term "spyware" does not include functionality delivered without the  
16 installation of software on users' computers. For example, the term "spyware" is  
17 not properly used to refer to the ordinary pop-up ads shown by web sites when users  
18 visit those sites. These ordinary pop-up ads are shown using only code in web sites'  
19 own web pages, without any software installed on users' PCs.  
20  
21

22 27. The term "spyware" is also not properly used to refer to "cookies." Cookies  
23 are data files that web sites can place on a user's PC so as to be able to recognize the  
24 user if he later returns to that web site. These cookies are not properly classified as  
25 spyware because they operate only within the limited parameters permitted by web  
26 browsers. In particular, a web site cannot use cookies to learn anything about the  
27  
28

1 user other than what the user has told that site either explicitly (e.g. by filling out a  
2 form) or implicitly (e.g. through web browsing and purchasing habits). In contrast,  
3 spyware can track users' behavior across all web sites, and spyware can interact  
4 with users in arbitrary ways not constrained by browser design.  
5

### 6 WhenU Software Generally

7 28. Software written and distributed by WhenU causes the display of popup  
8 advertisements when a user attempts to view certain third-party web sites. WhenU  
9 causes the display of these popup advertisements without the permission of the  
10 third-party web sites and without payment to them. WhenU's popup advertisements  
11 cover portions of web sites created by third parties, preventing users from viewing  
12 these sites as their designers intended.  
13

14 29. The design of WhenU software allows WhenU to cause advertisements to be  
15 displayed subsequent to user requests for any web site desired. WhenU popup  
16 advertisements often target the web sites of the advertisers' competitors. WhenU is  
17 equally capable of targeting advertisements at web sites that do not sell advertising  
18 or that refuse to permit certain types of advertising.  
19

20 30. WhenU software operates in three steps. First, WhenU software gets installed  
21 on a user's computer. Second, WhenU software monitors which web pages and web  
22 sites a user views. Finally, WhenU software shows ads according to which web  
23 pages and sites a user views.  
24  
25  
26  
27  
28

The Advertisements Displayed by WhenU Software

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

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

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

3  
4 34. WhenU's advertisements differ substantially from the American Express  
5 billing-insert offers Avi Naider describes in his affidavit (paragraph 4). For  
6 example, the origin of Amex's advertising inserts is intuitive and easy to  
7 understand: They come in an envelope along with other Amex content. In contrast,  
8 WhenU's advertisements appear at the same time as content from web sites users  
9 request. Because Amex advertisements arrive with Amex content, consumers are  
10 reinforced in their belief that the advertising at issue is delivered by Amex. In  
11 contrast, when WhenU delivers an advertisement that appears above and at the same  
12 time as a third-party web site, many users cannot help but conclude that the  
13 advertisement is part of or is affiliated with that third-party web site. In addition,  
14 Amex's advertising inserts are presented to customers well after they have  
15 completed the purchases that give rise to Amex's targeting decisions. In contrast,  
16 WhenU's advertisements interrupt users as they are working towards making a  
17 purchase. In my judgment, a better analogy for WhenU's advertisements is a  
18 competitor who walks into a store and interrupts the customer as the customer hands  
19 his purchase to the checkout cashier.  
20  
21  
22  
23  
24  
25  
26  
27  
28

## WhenU's Methods of Operation and Targeting

1  
2 35. WhenU's methods of operation and targeting are discernible from hands-on  
3 testing of WhenU's software as well as from detailed inspection of the data files  
4  
5 WhenU sends and receives over users' Internet connections.

6 36. As an empirical matter, hands-on use of computers with WhenU software  
7 makes it clear that WhenU targets its ads according to user activities. Visit a travel  
8 web site, and WhenU is likely to show ads for a competing travel web site. Visit  
9  
10 one car rental company and WhenU is likely to show ads for another.

11 37. This business model – showing ads for a site's direct competitors when users  
12 visit that site – is consistent with WhenU's prior statements to the public. WhenU  
13 frames these practices as "precision targeting" and "contextual marketing,"<sup>1</sup> but the  
14 empirical reality is that when users visit one web site, WhenU is likely to show ads  
15  
16 for the site's competitors.

## Spyware Installation is Not Consensual

17  
18  
19 38. In general, spyware software is unwanted: Users receive spyware programs,  
20 including software from WhenU, without knowingly consenting to its installation.

21  
22 39. Users typically obtain spyware software in one of two distinct ways. These  
23 are: 1) As an unrequested add-on provided with a third-party program a user  
24  
25  
26

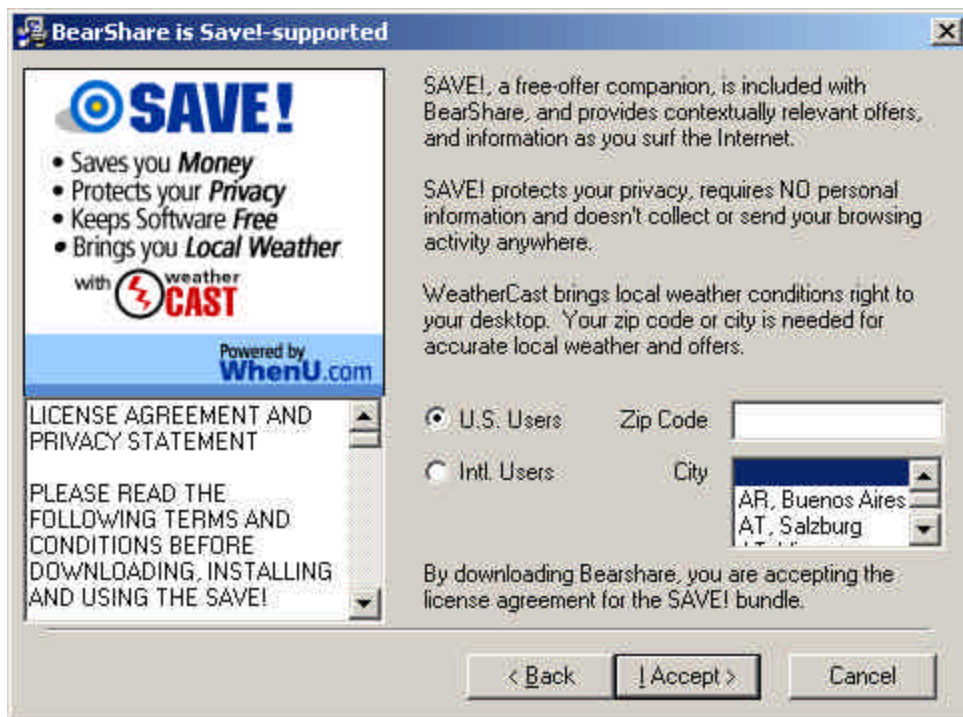
---

27 <sup>1</sup> <http://www.whenu.com> , checked May 3, 2004  
28

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

3  
4 40. First, some users obtain spyware (including WhenU software) via bundles  
5 with third-party applications, including peer-to-peer filesharing programs used to  
6 copy music, video, and other files. A user seeking any of these third-party programs  
7 will often receive spyware software also, and in the past it was often impossible to  
8 obtain the desired third-party software without also obtaining spyware. Many of  
9 these third-party programs install spyware without a user's knowledge or consent,  
10 without displaying license agreements, and/or without displaying the license  
11 agreements in a time, format and style in which it can be meaningfully reviewed and  
12 evaluated. For example, BearShare (version 4.4.3, the latest version available as of  
13 April 2004) places the WhenU license agreement in a subwindow so small that it is  
14 broken into forty four distinct pages of text, of which the first is shown below.  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28





1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13 41. The remainder of the BearShare installer, including each of the other forty  
14 three distinct pages of WhenU license, is available on the web at  
15 <http://www.benedelman.org/spyware/whenu-license> .  
16

17 42. Second, some users obtain spyware software (including WhenU software) via  
18 a process often called “drive-by downloads.” When users visit certain web pages,  
19 those pages may cause the user’s computer to download and offer to install spyware  
20 software – all without a user’s prior approval. Under the default configuration of  
21 most computers, drive-by installations cause the display of a single popup message  
22 box that sometimes offers a link to a program’s license agreement. However, a user  
23 can click the “yes” button to complete the installation without seeing the license, not  
24 to mention reading it or understanding it. In addition, depending on the  
25 configuration of a user’s computer, some spyware may be installed without the  
26  
27  
28

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

3  
4 43. Drive-by downloads are, in my judgment, inherently misleading. When a  
5 user is merely reading some other, unrelated web site, a pop-up message appears,  
6 suggesting to the user that the specified program is necessary in order to view the  
7 requested web site. Users' belief to this effect is well-founded; Microsoft developed  
8 the auto-install process precisely to easily provide plug-in software actually required  
9 to view certain web pages. At a recent FTC workshop, a senior Microsoft staff  
10 person characterized drive-by downloads as "tricks" and "not what we [Microsoft]  
11 intended."<sup>2</sup> In addition, drive-by downloads cause software to be downloaded to  
12 users' computer even before the user is told that software is available for  
13 installation, and certainly before the user has consented to such installation.<sup>3</sup>  
14  
15  
16

17 44. When users receive WhenU software via drive-by download, they may or  
18 may not consent to WhenU's license agreements. For one, users may never even  
19 see WhenU's license agreement, because WhenU's drive-by installer does not show  
20 WhenU's license to users, even in part. Instead, WhenU's installer merely offers  
21 users a link to the license. In addition, even users who specifically seek out the  
22  
23

---

24  
25 <sup>2</sup> Jeffrey Friedberg, Director of Windows Privacy, Microsoft Corporation. Oral  
26 comments to the FTC - Washington DC, April 19, 2004.

27 <sup>3</sup> *Methods and Effects of Spyware*, <http://www.benedelman.org/spyware/ftc-031904.pdf>, paragraph 36, checked May 16, 2004.  
28

1 license agreement, by clicking on the link, may be unable to view it. Consider the  
2 result shown in the video called WhenU-Driveby-License\_no\_scroll-051504.wmv  
3  
4 video on the CD attached to my declaration. This video shows that in a WhenU  
5 drive-by installation of May 15, 2004, WhenU's license agreement was provided in  
6 a window too small to show the entire license, without scroll bars to allow the user  
7  
8 to browse to see the rest of the license.

9 45. Both bundling and drive-by downloads cause spyware software to be installed  
10 as a mere byproduct of some other activity a user sought to complete – installing  
11 unrelated software, or viewing an unrelated web site. These methods of distribution  
12  
13 are, in my opinion, a large part of the reason why, in my experience, users tend to be  
14 uncertain and confused as to where and how they obtained spyware.

15  
16 46. WhenU uses both of the practices described above, as well as other  
17 installation practices that cause users to obtain their software with even less notice  
18 or consent. For example, WhenU's software is automatically installed by "IE  
19 PLUGIN" from a company calling itself "IE PLUGIN LTD," a product that itself  
20 uses the drive-by download installation strategy. IE Plugin purports to offer users a  
21 link to the license agreements for IE Plugin and the programs it installs, but in fact  
22  
23 that link is sometimes defective and wholly non-operational. As a result, even users  
24  
25 who specifically seek out the license for IE Plugin (and its bundled programs)  
26 cannot obtain that license, and users who install IE Plugin necessarily do so without  
27  
28 first reviewing IE Plugin's license or the licenses of the various programs IE Plugin

1 then installs. Users who receive WhenU software in this way cannot possibly have  
2 seen – not to mention consented to – WhenU’s license agreement. On the CD  
3 attached to my declaration, the video Driveby-WhenU\_bundle-050204.wmv shows  
4 installation of WhenU in this way, while the video Driveby-WhenU\_bundle-  
5 050204-nolicense.wmv demonstrates the defective design of IE Search’s license  
6 display technology.  
7  
8

9 47. The net effect of these various misleading installation techniques is that users  
10 overwhelmingly do not know what spyware they have installed, or even that they  
11 have spyware installed, not to mention having consented to the installation of such  
12 software. PC Pitstop, a web site that provides technical support to users with  
13 computer problems, showed a survey to users whose computers were diagnosed as  
14 including software from WhenU. According to PC Pitstop’s survey results, more  
15 than 87% of WhenU users do not even know that they have WhenU software  
16 installed.<sup>4</sup>  
17  
18

#### 19 The Effects of Spyware in Utah

20 48. In my judgment, spyware poses a substantial harm to users and companies in  
21 Utah.  
22

23 49. To users in Utah, spyware has numerous negative effects. Spyware slows  
24 computers, as I have confirmed in my own research and as other experts have also  
25

---

26  
27 <sup>4</sup> <http://www.pcpitstop.com/spycheck/whenu.asp>, checked May 3, 2004.  
28

1 confirmed.<sup>5</sup> Spyware slows users' Internet connections.<sup>6</sup> Spyware sends personal  
2 information to remote web sites. Indeed, my own research indicated that WhenU's  
3 software makes transmissions precisely contrary to its own license agreements.<sup>7</sup>  
4

5 50. These problems are particularly pronounced as to public computers. In my  
6 experience, spyware is especially prevalent on computers available to the public,  
7 including in primary and secondary schools, as well as in public libraries. My  
8 testing of earlier this year confirmed that multiple computers in the Utah State  
9 Legislature were infected with spyware, in fact some with software provided by  
10  
11

---

12  
13  
14 <sup>5</sup> See e.g. PestPatrol comments to FTC,  
15 <http://www.ftc.gov/os/comments/spyware/040423pestpatrolstatement.pdf> , checked  
16 May 3, 2004. "Testing earlier this month at the PestPatrol research laboratory  
17 revealed that the addition of just one adware pest slowed a computer's boot time  
18 (the amount of time it took to start up and function) by 3.5 times. Instead of just  
19 under 2 minutes to perform this operation, it took the infected PC close to 7 minutes  
20 to start up."

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

28 <sup>7</sup> 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.'"

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

3  
4 51. Utah companies also suffer as a result of spyware programs. When Utah  
5 companies are targeted by spyware, the spyware pop-up ads reduce the companies'  
6 ability to present their web sites to their customers, in Utah and beyond, in the ways  
7 that the companies intended. Furthermore, the pop-up ads have a detrimental effect  
8 on users' perception of the companies. A recent survey by D2 Research indicated  
9 that popup ads cause users to have a less favorable opinion of the sites on which the  
10 ads appear.<sup>8</sup> My discussions with staff of targeted sites indicate that targeting had  
11 significant, quantifiable harm on their business.

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

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

19 53. In the relevant sense, spyware resides permanently on the computers on  
20 which it is installed. Of course, some spyware can be removed, and in that sense  
21 certain spyware programs are not permanently present. But when spyware is  
22 installed on a computer, it remains on the computer for the indefinite future – until  
23

24 \_\_\_\_\_  
25 <sup>8</sup> <http://www.ftc.gov/os/comments/spyware/040323hertzllbeanwithpopupsurvey.pdf>  
26 [page 7](#), checked May 3, 2004. “33.2% of respondents said that the appearance of the  
27 pop-up ad would cause them to have a less favorable opinion of the website (vs.  
28 only 2.4% who said it would give them a more favorable opinion).”

1 the computer is discarded or erased, or until the owner of the computer takes special  
2 steps to remove the spyware. Spyware is not a mere transitory visitor to a computer,  
3 like a web page briefly shown on screen but shortly replaced with a new page.  
4 Rather, spyware is a permanent addition, which will remain installed even if a  
5 computer is turned off and turned back on.  
6

7  
8 54. Relevant actions taking place within Utah include the offer of the software for  
9 installation, the installation of the software, the use of the software by the user, and  
10 the operation of the software to cause causing the results prohibited by the Act.  
11

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

14 55. Spyware makers can easily comply with the Spyware Control Act, without  
15 modifying their behavior elsewhere. They can do this both by modifying their  
16 software so as not to install in Utah, so as to operate differently (or not at all) when  
17 installed in Utah, and/or so as not to target advertisements at web sites run by Utah  
18 companies.  
19

20 56. Consider the WhenU installer, as bundled with the current version of  
21 BearShare. As shown in the screenshot at paragraph 40 above, the WhenU  
22 installation program asks the user for the user's zip code. If the user enters a zip  
23 code in Utah, the WhenU installer could simply reconfigure WhenU's software in a  
24 way that complies with the Act. Alternatively, if WhenU declines to modify its  
25 software to achieve such compliance, the WhenU installer could simply fail to  
26 install WhenU's software. WhenU already asks users for the sole piece of  
27  
28

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

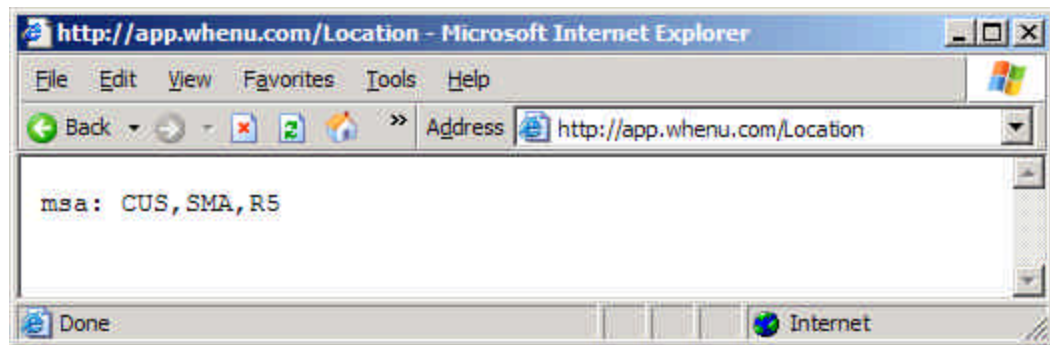
3  
4 57. Even programs that do not currently ask the user for his zip code could  
5 readily comply with the Spyware Control Act. For one, the programs could be  
6 modified so that they do ask for state, zip code, area code, or other location-  
7  
8 identifying information. These additions would be straightforward, as would be the  
9 simple logic to install or not install the software according to the user’s answer.

10 58. Alternatively, programs could use the user’s IP address (Internet Protocol  
11 address) to determine the user’s geographic location. While such a determination is  
12 not always perfectly accurate, it is in many instances sufficiently accurate to draw a  
13 robust inference as to the user’s location. For example, if the user is connected to  
14 the Internet through the facilities of the Utah Legislature, the user’s IP address  
15 would be associated with a domain name that included the identifier “utah.gov.”  
16  
17 Similarly, a user from Brigham Young University would have an IP address  
18 associated with a domain that included “byu.edu.” On this basis, it would be easy to  
19 determine that the user is almost certain to be located in Utah. Commercial services  
20 provide this service in an automated, centralized implementation.<sup>9</sup>

21  
22  
23  
24  
25 \_\_\_\_\_  
26 <sup>9</sup> See e.g. Quova GeoPoint,  
27 [http://www.quova.com/shtml/technology/tech\\_geopoint.shtml](http://www.quova.com/shtml/technology/tech_geopoint.shtml) , checked May 3,  
28 2004. GeoBytes IP Locator, <http://www.geobytes.com> , checked May 3, 2004.  
NetGeo, <http://www.netgeo.com/> , checked May 3, 2004.



1 59. In fact, some WhenU software already performs precisely this sort of IP  
2 address lookup in order to determine where users are located, without asking users  
3  
4 for their zip codes. At the URL <http://app.whenu.com/Location> (note case-  
5 sensitivity), WhenU's web server tells a user his or her location – country (two-letter  
6 abbreviation preceded by the letter “C”) and state (two-letter abbreviation preceded  
7  
8 by the letter “S”). Certain WhenU software automatically asks the WhenU web  
9 server for this /Location information, then stores this data in the “registry” of users’  
10 computers, and periodically transmits it to WhenU servers. With location data  
11  
12 already collected, stored, and tracked by WhenU, it would be particularly puzzling  
13 for WhenU to claim an inability to alter its behavior according to users’ apparent  
14 locations.



15  
16  
17  
18  
19  
20  
21  
22 60. Because WhenU's software is location-aware, it differs substantially both  
23 from the other Internet-transmitted content that has been the subject of earlier  
24 litigation (i.e. *ACLU*) and from the other chattels that have been the subject of  
25 interstate commerce claims. See, e.g., *Southern Pacific Co. v. Arizona*, 325 U.S.  
26 761 (1945) (passenger trains). Static web pages and physical chattels are incapable  
27  
28

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

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

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

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

---

26  
27 <sup>10</sup> Preliminary injunction order in *1-800 Contacts, Inc., v. WhenU.com and Vision*  
28 *Direct, Inc.* 02 Civ. 8043 (S.D.N.Y., Dec. 22, 2003).

1 maintains and actively updates a list of sites not to target, including its own site, its  
2 competitors' sites, sites of companies that have sued or threatened to sue WhenU,  
3 and sites of companies that have sued or threatened to sue WhenU's competitors.  
4

5 63. In any event, WhenU significantly overstates the number of companies that  
6 would have to modify their behavior to comply with the Act, both as to the  
7 modifications discussed in this section and as to those of the preceding section. Of  
8 the legitimate companies that write software that transmits users' usage data for  
9 legitimate reasons, the overwhelming majority already provide notice, obtain  
10 consent, and include uninstall routines. Such companies need not change anything  
11 about their products. Only the companies that currently fail to provide notice,  
12 consent, and uninstall, or that show context-triggered popups that cover web sites,  
13 would have to modify their behavior to comply with the Act's requirements.  
14  
15

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

19 64. WhenU's use of sophisticated "content distribution services" (CDSs) to  
20 distribute its "directory" (which advertisements to display under which conditions)  
21 means WhenU could comply with the Act without changing any WhenU SaveNow  
22 code. To proceed in this way, WhenU need only tell its CDS partners never to  
23 distribute the directory to users in Utah – a service its CDS partners already provide  
24 in their ordinary course of business.  
25  
26

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

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

9  
10  
11  
12 66. While the public materials I have reviewed from Akamai and Speedera's web  
13 sites do not specifically speak to the accuracy of their geo-targeting systems, they  
14 both state that the systems can be used for rights management and regulatory  
15 compliance purposes. From my conversations with senior Akamai staff, I believe  
16 Akamai's methods to be extremely robust and reliable as to the overwhelming  
17 majority of Internet users.  
18

19  
20 Security Flaws in WhenU Products and in Other Spyware Products

21 67. Legislators and other policy-makers are rightly concerned about security  
22 flaws in spyware products, including in software from WhenU. Badly-designed  
23

24 <sup>11</sup> *Akamai Edgescape*,  
25 [http://www.akamai.com/devnet/pdf/EdgeSuite\\_Service\\_Description.pdf](http://www.akamai.com/devnet/pdf/EdgeSuite_Service_Description.pdf), pages 18-  
26 19, checked May 16, 2004.

27 <sup>12</sup> *Speedera Geo-targeting*,  
28 <http://www.speedera.com/primary/services/geotarget.htm>, checked May 16, 2004.

1 spyware can expose users to serious security vulnerabilities, including allowing  
2 attackers to send the user's personal data or behavior to any server on the Internet; to  
3 add, modify, or delete files; to install other programs (including other spyware  
4 programs); or to use the computer to send junk email or cause a denial of service  
5 attack.  
6

7  
8 68. These kinds of vulnerabilities have previously been found in other spyware  
9 programs. For example, *Measurement and Analysis of Spyware in a University*  
10 *Environment*<sup>13</sup> presents serious security vulnerabilities in widely-deployed software  
11 from both Claria and eZula.  
12

13 69. My testing indicates that certain software from WhenU contains similar  
14 vulnerabilities. I have notified WhenU staff of this problem, affecting software on  
15 WhenU's ordinary public web site until mere days ago. WhenU staff have generally  
16 confirmed the scope and effect of the vulnerability I found, and they assure me that  
17 they have since corrected the problem. I am presently in the course of completing  
18 my write-up of this security vulnerability, and I expect to release my research to the  
19 public in the coming weeks.  
20  
21

22 Response to the Affidavit of Avi Naider

23 70. I have reviewed the Affidavit of Avi Naider, dated April 12, 2004.  
24

25 <sup>13</sup> Saroiu, Stefan, Steven D. Gribble, and Henry M. Levy. *Measurement and*  
26 *Analysis of Spyware in a University Environment*.  
27 <http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf> , checked May 12,  
28 2004.

1 71. Mr. Naider's declaration is false in as much as it claims that WhenU does not  
2 collect information concerning the history of the web pages users visit. In my  
3  
4 *Methods and Effects of Spyware*,<sup>14</sup> I demonstrate that WhenU collects and transmits  
5 to its servers precisely this information, whenever WhenU shows an advertisement.

6 72. Mr. Naider claims that any change WhenU makes would have to be made  
7  
8 system-wide, not just in Utah. (Paragraph 52) This is false. As shown in paragraph  
9 40 of my declaration and discussed in the section entitled *Spyware Makers Can*  
10 *Easily Comply with the Act by Modifying Their Behavior When Installed In Utah or*  
11 *by Modifying Their Behavior When Installed In Utah*, WhenU software knows  
12 where it is located because it asked users for this information. It would be a simple  
13 change for WhenU to refuse to install if the user specified a zip code in Utah, or for  
14  
15 WhenU to operate in a different way if the user specified a zip code in Utah.

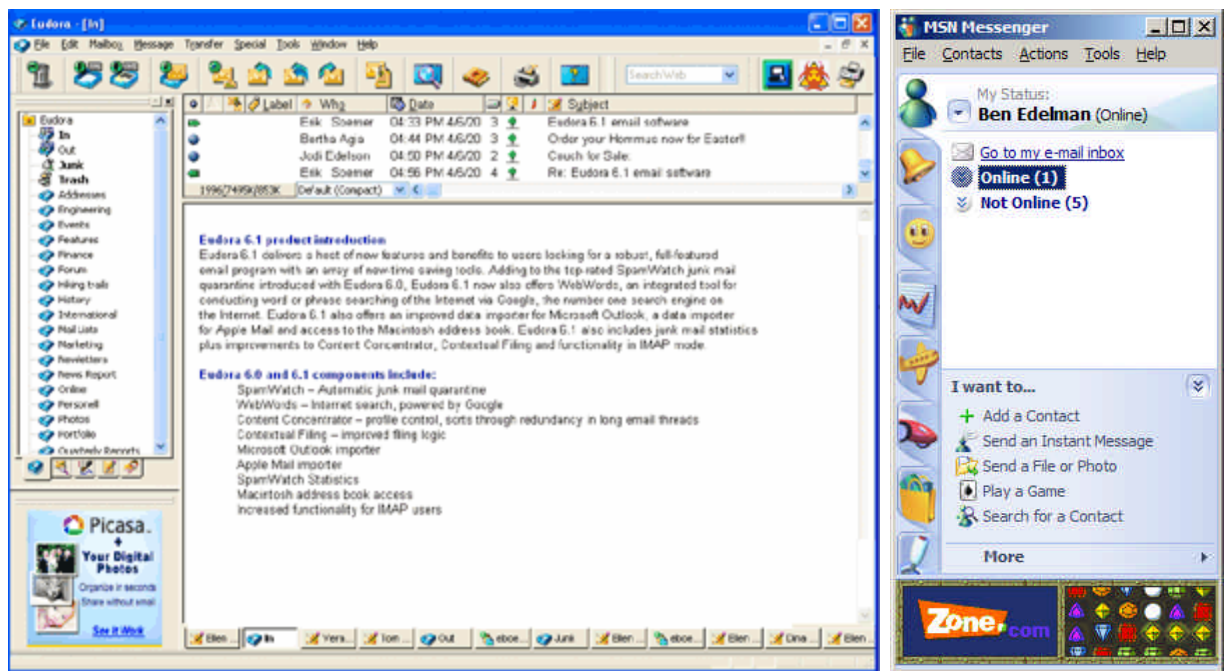
17 73. The fact that the Act exempts pop-ups from search engines and web sites is  
18 not "ironic" as Naider suggests (paragraph 62). Rather, this approach precisely  
19  
20 reflects that search engines and web sites do not pose the same threat as spyware to  
21 users' privacy and to the reliability of their computers.

22 74. The Act will not have "terrible consequences for the Internet" (§66) by  
23  
24 preventing "software based advertising" (§67). Contrary to Naider's declaration, the  
25

---

26  
27 <sup>14</sup> <http://www.benedelman.org/spyware/ftc-031904.pdf> , paragraphs 12-17, checked  
28 May 3, 2004.

1 Act does not prohibit all advertisement-supported software; it merely prohibits  
2 advertisements that are context-triggered and cover web sites without their  
3 permission. Other kinds of advertisement-supported software remain perfectly  
4 permissible under the Act. For example, programs remain free to display  
5 advertisements within their own application windows, an approach used by the free  
6 version of Eudora and by MSN Messenger (both shown below).  
7  
8



### Response to the Affidavit of Arnold Reinhold

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

22 76. Reinhold is in error when he claims that software distributors cannot reliably  
23 determine in which state a user resides upon downloading software (paragraph 31).

24 The services I describe in paragraphs 59 and 64 to 66 are capable of making such a  
25 determination. These services do not claim 100% accuracy, but they are sufficient  
26 for ordinary commercial purposes. For example, Major League Baseball apparently  
27  
28

1 uses Quova technology to determine a user's location, on a state-by-state basis, to  
2 avoid transmitting webcasts in violation of local broadcast rights.<sup>15</sup> In any event,  
3 spyware programs can easily ask users for their locations, as a backup or secondary  
4 approach. For example, WhenU's WeatherCast already asked for a user's Zip Code  
5 prior to installation.  
6

7  
8 77. Reinhold's interpretation of the Act is in error in as much as, in paragraph 36,  
9 he discusses provisions (4)(a) and (4)(b)(i) alone, without noting the exceptions in  
10 (4)(c), even as he acknowledged those exceptions a mere two paragraphs earlier. As  
11 a result, Reinhold's examples of iTunes is only an example of a program required to  
12 satisfy provision (c), not an example of a program in fact in violation of the Act as  
13 drafted. From my initial review of iTunes, I am confident that it already satisfies the  
14 requirements of (c). To the extent that I understand the vague additional examples  
15 Reinhold mentions in paragraph 36, I believe none is in fact in violation of the Act.  
16

17  
18 78. Neither is the parental monitoring software IamBigBrother.com in violation  
19 of the Act. From my initial review of this program, it includes a license agreement  
20 and it can readily be removed by the computer owner who initially installed it. As a  
21

22  
23  
24  
25 <sup>15</sup> [http://www.quova.com/shtml/story/story\\_jack.shtml](http://www.quova.com/shtml/story/story_jack.shtml) , checked May 3, 2004.  
26 "Quova's technology helps MLB.TV generate new webcast revenues without  
27 infringing on local broadcast rights, which are crucial to the teams and local  
28 stations. This historic initiative wouldn't be possible without Quova's 99% accuracy  
verification of every viewer's location."



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

3  
4 79. In paragraph 33, Reinhold refers to a letter from AOL and other companies  
5 that claims certain errors in the Act. I have reviewed this letter at great length and  
6 believe its concerns to be misplaced. My analysis of the letter is posted to the web  
7 in my *A Close Reading of Utah's Spyware Control Act*.<sup>16</sup> In short, I believe AOL  
8 and its cosignators made the same analytical error flagged in the preceding  
9 paragraphs – failing to fully understand how the various sections of the Act fit  
10 together, and therefore failing to correctly determine which software is in fact  
11 subject to the Act.  
12  
13

14 80. I declare under penalty of perjury under the laws of the State of Utah that the  
15 foregoing is true and correct.  
16

17  
18 Executed this \_\_\_\_ day of May, 2004, at Boston, Massachusetts.

19  
20  
21 \_\_\_\_\_  
22 Benjamin Edelman  
23  
24  
25  
26

27 \_\_\_\_\_  
28 <sup>16</sup> <http://www.benedelman.org/spyware/utah-mar04/> , checked May 3, 2004.