Methods and Effects of Spyware

Response to FTC Call for Comments

Benjamin Edelman, Harvard University
March 19, 2004

Introduction & Disclosures

1. My name is Benjamin Edelman. I am a Ph.D. candidate in Economics at Harvard University and a student at the Harvard Law School. My research interests include Internet economics, architecture, and regulation. My attached CV lists some of my publications in this field, while my web site details some of the occasions in which I have given related presentations.[1]

2. I write in response to the FTC's call for comments on monitoring software, spyware, and adware.

3. I have served as an expert in multiple cases about adware and spyware. I prepared written and oral testimony on behalf of the plaintiffs in Wells Fargo & Co. and Quicken Loans, Inc. v. WhenU.com, Inc., 293 F.Supp.2d 734, E.D.Mich. 2003. I gave a deposition and was prepared to testify as an expert on behalf of the plaintiffs in Washingtonpost.Newsweek Interactive Co. LLC, et al. v. the Gator Corporation, E.D.Va. 2002.

4. I have consulted for additional firms concerned about the effects of adware and spyware. My agreements with some of these firms prevent me from revealing their identities. However, I can disclose that I have served as a consultant to 1-800 Contacts as to its litigation against WhenU.

5. I am submitting this comment purely on my own behalf – not on behalf of or at the request of any client. I am not being compensated by any client for this submission.

6. My prior research about spyware includes *Documentation of Gator Advertisements and Targeting*, available at http://cyber.law.harvard.edu/people/edelman/ads/gator. More recently, I have posted a draft of *A Close Reading of the Spyware Control Act*, available at http://www.benedelman.org/spyware/utah-mar04. In addition to reviewing a bill recently passed by the Utah legislature and now awaiting signature by the governor of Utah, this document analyzes arguments offered by opponents of the bill, and it also evaluates related news coverage (namely, the MediaDailyNews article that is comment number 23 on the FTC's listing at http://www.ftc.gov/os/comments/spyware/index.html). My *"Spyware": Research, Testing, Legislation, and Suits* site, at http://www.benedelman.org/spyware, provides a unified index to my various publications and references in this field.

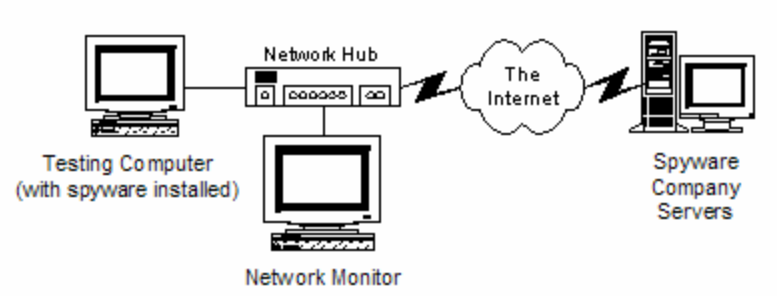
---

[1] http://www.benedelman.org/presentations

Methodology

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

8. My method of monitoring network communications (of computers in my lab) bears special mention both because it is subtle (sometimes misunderstood as sort of "hacking") and because it is powerful (allowing key insights into the method of operation of spyware). By arranging the computers in my lab in the manner shown below, I can perform a procedure called *network monitoring* that lets me view and record programs' transmissions over my Internet connection.



As shown in the diagram, all communications from the computer with spyware installed 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.

9. This monitoring technique allows me to learn what information spyware programs obtain from their servers and what information they send back to those servers. Using network monitoring software, I can record all network communications to a file, 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.

10. I want to be explicit in noting that this document relies on absolutely no confidential information received in the course of litigation against any spyware companies. In the course of litigation against makers of spyware, I have sometimes received documents labeled as confidential by the defendants, and I have sometimes attended courtroom proceedings designated as confidential. I respect courts' orders of confidentiality to the utmost. I have not revealed and will not reveal any confidential information I receive from confidential documents or from confidential courtroom proceedings. Rather, the information contained in this document results solely from the

methods of analysis described above – e.g. monitoring the network communications of my own computers.

11. Technically knowledgeable readers should be able to verify and confirm my conclusions using only the methods described in this document. Furthermore, 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.

Transmission of Personal Information by Spyware

12. The FTC's call for comments specifically asks whether and how "adware" is different from spyware. Having reviewed multiple programs that display targeted popup advertisements according to users' web browsing patterns – programs that some analysts, myself included, have sometimes called adware – it is my opinion that these programs are also properly called spyware. The spyware classification is appropriate because these programs transmit extensive personal information from users' computers to the servers of these programs' designers. Such transmission are often contrary to stated license agreements and are typically contrary to consumer expectations as I understand them. In this document, I discuss WhenU and Gator specifically.

Transmission of Personal Information by WhenU

13. Software provided by WhenU tracks (and sends to WhenU servers) information about selected specific web pages visited by WhenU users. Whenever a user visits a web page and is shown a WhenU advertisement, according to WhenU's advertisement-targeting algorithm, WhenU's software sends a message to a WhenU web server. Among other information, this message includes the specific web page URL that the user was viewing prior to being shown the advertisement.

14. A typical WhenU transmission looks like the following, sent to a WhenU web server at `web.whenu.com`:

```
GET /offerb?url=fci_cheaptix108&pattern=akwdId_20_2944
&patid=A20_2944&src=http%3A//www.expedia.com/default.a
sp%3F&ver=2.54&partner=CAST1202&insttime=3500.81&msa=M
1120%2CSMA%2CR5%2CY1122
```

Notice the http://www.expedia.com/default.asp reference embedded within the WhenU transmission – reflecting that an advertisement was shown to a user when that user visited the specified Expedia URL. (In particular, the advertisement displayed was `fci_cheaptix108`, which is available on the web at http://spweb.whenu.com/pop_up/fci_cheaptix108_popup.html.[2]) Note also the inclusion of the

[2] Note that attempts to view the pop-up ad at this address may be stymied by the fact that the pop-up seems to recognize that it is being viewed outside of the WhenU program, and typically closes itself quickly for that reason. However, on most computers, the ad can be viewed for one to two seconds before it closes itself.

user's MSA (roughly equivalent to zip code) as well as information about how and when the user obtained WhenU. As part of their IP headers, these transmissions also include users' IP addresses.

15. This transmission record is also shown in Attachment 1, a screenshot of the CommView program I use to monitor transmissions over my Internet connection.

16. 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, in relevant part, as follows:

> "As the user surfs the Internet, URLS visited by the user (i.e. the user's 'clickstream data') are NOT transmitted to WhenU.com or any third party server."[3]

17. In my examinations, it is true that WhenU software does not transmit to its server *all* URLs visited by WhenU users. But WhenU software does transmit to its server *some* URLs visited by WhenU users. Since WhenU's privacy policy seems to promise not to transmit *any* URLs visited by WhenU users ("URLs … are not transmitted"), I consider WhenU's transmissions to be in violation of its privacy policy.

Transmission of Personal Information by Gator

18. In my testing, software provided by the Gator Corporation (recently renamed to Claria) tracks and sends to Gator servers all web sites visited by Gator users. Whenever a user visits a new web site (defined by its second-level domain name, e.g. *ftc.gov*), and whenever a user returns to a web site the user has not recently visited, Gator software sends to Gator servers a message including the specific web site visited (e.g. its second-level domain name), as well as a unique user ID and computer ID assigned by Gator, along with the user's zip code and IP address.

19. As of the spring of 2003, a typical Gator transmission looked like the following, sent to a Gator web server at `bannerserver.gator.com`:

```
POST /bannerserver/bannerserver.dll?GetBannerList
MachineID=RTJCNzI4QjktRkU4MS00RjIzLUE2REQtNzZEM0M2MThG
OTA4&MachineInt=103900267&Banner-Version=3%2e0&Product
Version=4%2e1%2e2%2e6&OEMID=0&Locale=0409&ZipCode=2&Us
erID=OTNBMEFDNDMxOUE5NDJDM0E0REFBQTA3M0JFQUY1RDk%3d%3d
%3d&UserInt=146699728&LocalTime=04%2f19%2f2003+01%3a26
%3a18+%2d0500&GMTTime=04%2f19%2f2003+05%3a26%3a18+%2b0
000&BnrTypes=7df&AIC-0=gator%5faic&Site=yale%2eedu&Def
Browser=1&InstDate=04%2f18%2f2003+09%3a00%3a18+%2d0500
&GTRGF=0%2c0&PA=0&
```

[3] http://www.whenu.com/privacy.html , checked March 12, 2004.

Notice the &Site=yale.edu parameter on the eighth line of this transmission, reporting that a user had just requested a page on the yale.edu domain. Note also additional information transmitted by Gator's client software to Gator's server: A unique machine ID and user ID, the user's zip code, the local time, the version of Gator software installed.[4] In my testing of spring 2003, transmissions of this form reliably took place every time a user visited a new second-level domain or returned to a domain not recently visited.

20. My more recent monitoring of transmissions by Gator software shows no directly analogous transmission that includes, in plain text, the specific domain names that users visit. However, I have found ample basis for concluding that domain visit information continues to be transmitted by Gator software, but now in some obfuscated or encrypted form. When observing the transmissions of a computer in my lab with a more recent version of Gator installed, I see no more transmissions to `bannerserver.dll`, but instead transmissions to a "`/gbs/gbs.dll?GBL`" program on a Gator web server. These transmissions seem precisely to track the situations in which `bannerserver.dll` requests were made in the past: `gbs.dll` requests are made whenever a user visits a new domain or a domain not recently visited. However, these `gbs.dll` transmissions are not as easy to interpret as the old `bannerserver.dll` requests: `gbs.dll` requests are typically followed by gibberish data, unlike the readable text shown above as to `bannerserver.dll`, and the response to a `gbs.dll` request is another string of gibberish. But seemingly on the basis of that gibberish result, the Gator client software often then requests a file with a meaningful filename. For example, when I requested a page on the harvard.edu web server, the Gator client shortly issued the following request to a Gator web server at `bc2.gator.com`:

```
GET /gbsf/gd/ha/harvard.edu.gtrg2ze
```

21. On this basis, I think there is ample evidence to conclude that Gator continues to transmit to its servers the specific domain names visited by a user. Certainly Gator transmitted to its servers the fact that I visited (for example) a `harvard.edu` web site, and it may have made this transmission repeatedly or in multiple formats. The only significant change from Gator's behavior of last spring is that some Gator transmissions are now encoded or obfuscated in some way, making it more difficult for users to observe (via network monitors, personal firewalls, or other methods) what information is being transmitted from their computers to Gator's servers.

22. Gator currently maintains databases among the largest in the world – the seventh largest "decision support" database in the world, according to a recent eWeek article.[5] Gator's *Employment* page confirms that the company maintains exceptionally large data

---

[4] In this example, the user's purported zip code is "2" – which I believe reflects that when I installed this version of Gator on a testing PC in my lab, I had entered "2" as my zip code, rather than telling Gator my true zip code.

[5] "Survey: Biggest Databases Approach 30 Terabytes." November 8, 2003. http://www.eweek.com/print_article/0,3048,a=111787,00.asp , checked March 12, 2004. "Claria Corp., 12.1 terabytes."

systems: Gator currently offers a position as a "Business or Marketing Analyst" which entails the responsibility of querying "very large (20TB, 100 billion records)" databases.[6] I have no way to know the specific contents of these databases, and to my knowledge Gator has not explicitly disclosed their contents to the public. However, noticing that Gator receives extensive data as to which specific users visit which specific web sites, I think there is ample evidence for an inference that users' site visit data is stored on Gator servers for an extended period, if not indefinitely.

23. Gator's Feedback Research division apparently makes data available for purchase as to users' visits to particular web sites.[7] Indeed, some Feedback Research service offerings specifically confirm that Gator tracks and stores information about which users have visited which web sites. See e.g. "we can identify users who have viewed parenting sites in the past 30 days."[8]

What Can and Can't Be Learned from Analyzing Other Advertisement-Supported Programs

24. Comparing "controversial" advertisement display programs with "benign" advertisement display programs is unlikely to provide insight as to whether advertisement display programs, taken as a whole, are or are not properly considered spyware.

25. Certainly some advertisement display programs are not properly classified as spyware. In its comment of March 5, CDT correctly offers the laudable example of Eudora's in-window advertising, which is implemented without giving rise to privacy or security concerns, and which in my view would not correctly be called spyware. Similarly, the in-window advertisements displayed by instant messenger programs also lack privacy concerns – like Eudora, they do not transmit information about users' web activities to remote servers. Indeed, these programs are not anything close to "tough" cases: To the best of my knowledge, no one has ever called Eudora or IM programs spyware, for the term is clearly inapt as applied to these programs.

26. But it would be erroneous to see the benign activities of Eudora and IM programs, and conclude that all advertisement display programs are not spyware. Instead, the harmless nature of Eudora and the IM programs only demonstrates that *some* advertisement display programs are not spyware.

27. As to the more controversial programs discussed above, their classification as spyware should follow from their actual activities. Certain programs' transmissions of personal information, as described above, lead me to the conclusion that these programs are correctly classified as spyware.

28. Finally, I share CDT's sense that spyware programs – including the context-triggered advertisement display programs described above, as well as other programs that all or nearly all analysts agree are properly called spyware – tend to share common

---

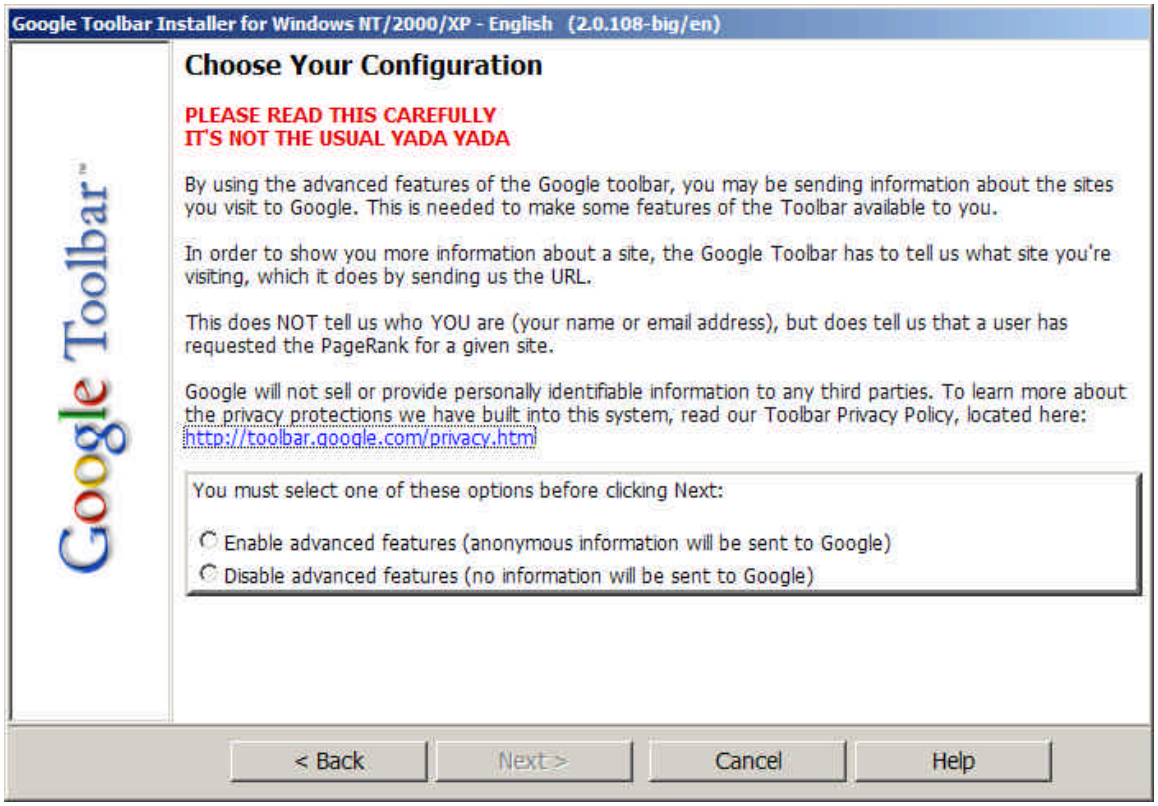
[6] http://www.claria.com/companyinfo/careers/#analytics , checked March 12, 2004. "Uses advanced SQL knowledge to query very large (20TB, 100 billion records) data base."
[7] http://www.feedbackresearch.com/capabilities/index.html , checked March 12, 2004.
[8] http://www.feedbackresearch.com/targeting/index.html , checked March 12, 2004.

distribution methods and other characteristics, with the net effect that users generally do not know what software is being installed or what effects the software will have. This similarity further bolsters the classification of context-triggered advertisement display programs as spyware.

Distinguishing Spyware from Legitimate Programs that Transmit Sensitive Information over the Internet

29. Like spyware, certain legitimate programs transmit sensitive information (such as which web sites users visit) over the Internet to company servers. For example, the Google Toolbar can be configured to transmit user visit data to Google servers. Nonetheless, I do not consider the Google Toolbar spyware. I reach this conclusion because Google's transmissions are 1) exceptionally clearly disclosed to users via a plain-language statement intended to get users' attention, 2) consistent with reasonable user expectations given the nature of the functionality to be provided, and 3) optional.

30. Understanding condition (1) benefits substantially from reviewing the actual on-screen display that the Google Toolbar installation program shows users. This screen is as shown below:



I consider this disclosure particularly laudable because it features the following characteristics: It discusses privacy concerns on a screen dedicated to this topic, separate from unrelated information and separate from information that may be of lesser concern to users. It uses color and layout to signal the importance of the information presented. It uses plain language, simple sentences, and brief paragraphs. It offers the user an

opportunity to opt out of the transmission of sensitive information, without losing any more functionality than necessary (given design constraints), and without suffering penalties of any kind (e.g. forfeiture of use of some unrelated software). As a result of these characteristics, users viewing this screen have the opportunity to make a meaningful, informed choice as to whether or not to enable the advanced features of the Google Toolbar.

Other Programs are Available at No Charge, that Perform the Same Features as Programs Bundled with Spyware

31. The FTC's call for comments asks what effects would result on the market for software if spyware were eliminated or reduced. Some programs, e.g. those programs currently receiving funding from spyware programs, might see a loss of revenue unless and until they found alternative funding sources. However, I believe consumers would continue to have essentially equal choices of software programs available at no out-of-pocket cost. Other programs would remain available that, for whatever reason, distribute their software without out-of-pocket cost and without spyware.

32. For example, Atomic Clock Sync 2.6[9] is an automatic computer clock synchronization program, but unlike WhenU's ClockSync and Gator's Precision Time, Atomic Clock Sync does not require that users accept popup advertisements. Similarly, Weather Watcher 5.0[10] provides local weather monitoring and reporting, and unlike WhenU's WeatherCast and Gator's Precision Time, Weather Watcher entails no popups.

Installation Methods of Spyware

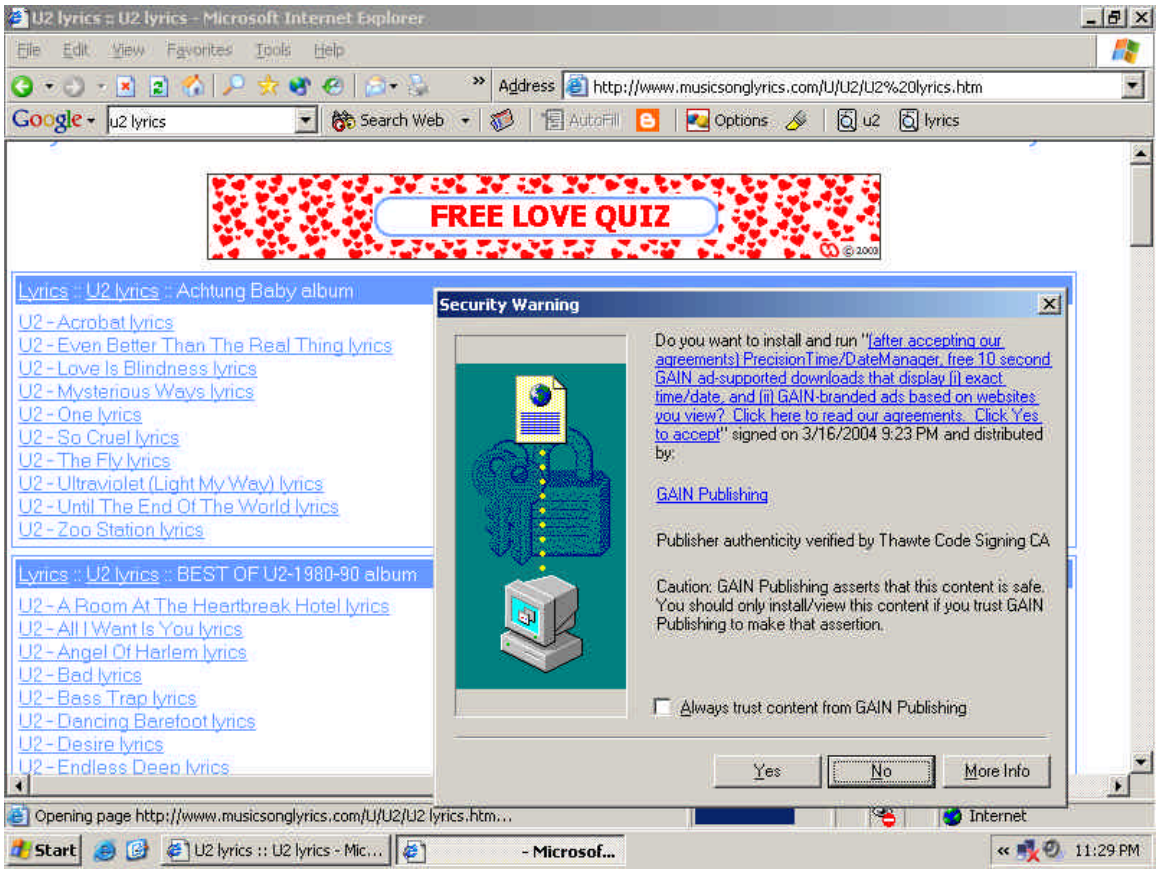
33. In my experience, spyware programs typically come to be installed on users' computers in three distinct ways (precisely as described by CDT in its comment of March 5).

Drive-By Downloads

34. First, some programs come to be installed on users' computers via so-called "drive-by downloads." Via this method of installation, a web site transmits HTML code to a user's computer that causes the user's Internet Explorer web browser to prompt the users to install specified software. In a drive-by download, the software is offered is, by hypothesis, not required to view the site; rather, it is unrelated, perhaps providing payment to the site, or distributed by the site for some other outside purpose. Internet Explorer's installation prompt system asks the user to decide whether to install the software without first seeing the program's license agreement, although the license may be available via a link from the installation prompt dialog box. In some instances, depending on users' security configurations, software may be installed without the dialog box appearing and therefore without the user ever being asked for consent to install the software. The screen-shot below gives an example of a Gator drive-by download attempt, along with a typical security warning dialog box:

---

[9] Available at http://www.worldtimeserver.com/atomic-clock/ , checked March 12, 2004.
[10] Available at http://www.singerscreations.com/ , checked March 12, 2004.



35. In my view, drive-by downloads are a deceptive and dishonorable method of causing or encouraging users to obtain software.[11] This is so for at least two different reasons. First, many users, especially novices, have the understanding that if a security warning dialog box suggests that they install software, then the software is in fact required in order to fully view the web site they are visiting. They have this understanding for good reason: When software installation prompts are used as Microsoft intended when it designed this feature, and as mainstream legitimate sites use this feature, their purpose is to necessary browser plug-ins necessary to view requested web content. This is the case for, for example, media players like the widely-used Macromedia Flash Player. Given this background understanding and its legitimate basis, use of software installation prompts tends to play on users' confusion, to their detriment.

36. The second reason why drive-by downloads are not an ethical or honorable method of providing software is that drive-by downloads cause executable software code to be downloaded to a user's computer even before the user consents to the software's installation, and even if the user ultimately denies consent. This behavior can readily be viewed with a network monitor: When Internet Explorer (in its default security configuration) receives a web page that uses a specified format to reference a software program (namely, a reference via a HTML OBJECT tag pointing to a .CAB file on a remote HTTP server), Internet Explorer begins to download that program, however large

[11] Here too, I agree with CDT's comment, which I take to refer to drive-by downloads when it mentions "deceptive download practices" on page two.

it may be and however slow the user's connection may be. Only later does Internet Explorer show the user a security warning confirmation dialog box requesting consent to the program's installation. In particular, even if the user denies consent, the program is nonetheless transferred over the user's Internet connection. [12] In my view, the preferable way for software developers to offer their programs to users would be to assure that no executable software code is transferred to users' computers unless and until users have expressed their consent for the installation of such code. The fact that no such assurance is possible via Internet Explorer's security warning system provides further support to the claim that this is not an appropriate method for encouraging users to install software, other than software actually necessary to view web pages users had specifically requested.

Bundling

37. Some spyware comes bundled with third-party applications. For example, some spyware programs are bundled with P2P filesharing programs.

38. In some instances in the past, and perhaps continuing to this day, the presence of these bundled programs was not disclosed to users until mid-way through the software installation process (e.g. after users had spent some time in obtaining software and beginning to install it), or on some occasions was not disclosed at all.

One Spyware Program Installs Others

39. Some spyware programs include within their functionality the ability to install other spyware programs. I gather this can be quite profitable for spyware makers: Spyware providers often pay royalties to whatever entities cause their software to be installed on additional computers.

40. Casual review of spyware listings and reports on the web indicates that this genre of spyware is growing in prevalence.

41. In my hands-on testing, I have confirmed that a program called ClientMan is among the spyware programs that install other spyware programs.

42. Rigorous testing of spyware installation paths can be particularly tricky because it can be difficult to tell precisely how programs came to be installed even on a carefully-configured test machine in a laboratory setting. For example, it can be difficult to determine whether one spyware program installed ten more, or whether that one program installed only two more programs, but each of those then installed four more of its own. However, I am currently working to develop methods of distinguishing between these scenarios, and I intend to publish research in this vein in the coming months.

---

[12] This behavior may sound like a bad design, and there is arguably a sense in which it is a bad design. But it is necessary to download the program before showing the software installation prompt in order for Internet Explorer to confirm that the program has in fact been digitally "signed" in the manner typical of software distributed in this way.

Frequency of Advertisement Display

43. The FTC's call for comments asks whether spyware interferes with use of the Internet. By showing multiple, frequent pop-up advertisements, spyware can significantly interfere with use of the Internet.

44. Of spyware programs that display advertisements, some programs make claims about the frequency with which advertisements are shown. For example, Gator's Date Manager states on its home page that it "occasionally" displays pop-up ads.[13] On its Products page, WhenU states "the average is one ad shown per user per day."[14]

45. Notwithstanding ambiguity in terms like "occasionally," my hands-on testing indicates that these claims understate the frequency with which advertisements are displayed. For example, in one video I prepared during the summer of 2003, I received four Gator pop-ups and one Gator pop-under during a two and a half minute visit to a major web-based travel site. In another video, this one made on a computer with WhenU, I received *the same* WhenU popup twice, separated by less than a minute of delay.

Other Effects on Users' Computers: Performance and Security

46. The FTC's call for comments asks whether spyware affects the functioning of computers on which it is installed. I have used computers infected with dozens or scores of spyware programs, including computers in libraries, schools, hotels, and Internet cafes. My hands-on testing indicates that these programs, collectively, can cause computers to become nearly unusable due to the excessive memory, processor, and network loads the programs jointly impose.

47. Some spyware programs entail security risks. For example, spyware can allow the installation of additional software without a user's consent. Improperly designed spyware can allow "man in the middle" attacks that let hostile software be installed via, among other methods, spoofed DNS responses. Section 5.1 of *Measurement and Analysis of Spyware in a University Environment*[15] describes these problems in some detail, citing related prior research and identifying at least two new vulnerabilities not previously known, including a vulnerability in widely-deployed software from Gator.

Comments on *Measurement and Analysis of Spyware in a University Environment*

48. I have read *Measurement and Analysis of Spyware in a University Environment* by Stefan Saroiu, Steven D. Gribble, and Henry M. Levy.[16]

49. I consider this an excellent article. Its key contribution is that it provides a rigorous, robust, and automated methodology for measuring the prevalence of certain spyware programs on a given network.

---

[13] "occasionally" on http://www.date-manager.com/ , checked March 12, 2004

[14] "We show these offers infrequently so as not to be intrusive. In fact, the average is one ad shown per user per day." http://www.whenu.com/products.html , checked March 12, 2004

[15] http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf , checked March 12, 2004.

[16] http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf , checked March 12, 2004.

50. I want to offer two comments that correct small errors in this article:

51. First, WhenU does transmit information about URLs visited, precisely contrary to the authors' statement in section 3.3. Perhaps the authors' review of network monitor logs failed to notice these transmissions, but I have seen them repeatedly, as shown in detail above.

52. Second, the article likely considerably understates the amount of network traffic caused by WhenU. Appendix A.2. lists the servers the authors consider to be responsible for WhenU traffic – twelve servers each bearing the second-level domain whenu.com. But much WhenU content, including the WhenU "directory" of advertisements and "trigger" conditions for advertisement display, is obtained from web servers bearing not the domain name whenu.com but instead from "global content delivery services" such as akamai.net. These services distribute WhenU's database and advertisements on WhenU's behalf – but the underlying traffic is caused solely by WhenU's software and is properly attributed to WhenU. Since these transmissions constitute the brunt of WhenU data retrieval – at least several megabytes of database download per computer per month, as well as scores or hundreds of ads of at least several kilobytes each – this omission causes a substantial downward bias in their conclusion as to WhenU's total network load. Correcting this omission, WhenU's total network load would be closer to the other spyware programs considered in the article, likely on the order of at least several hundred megabytes.

53. I also want to offer one comment as to the generalizability of the article's results:

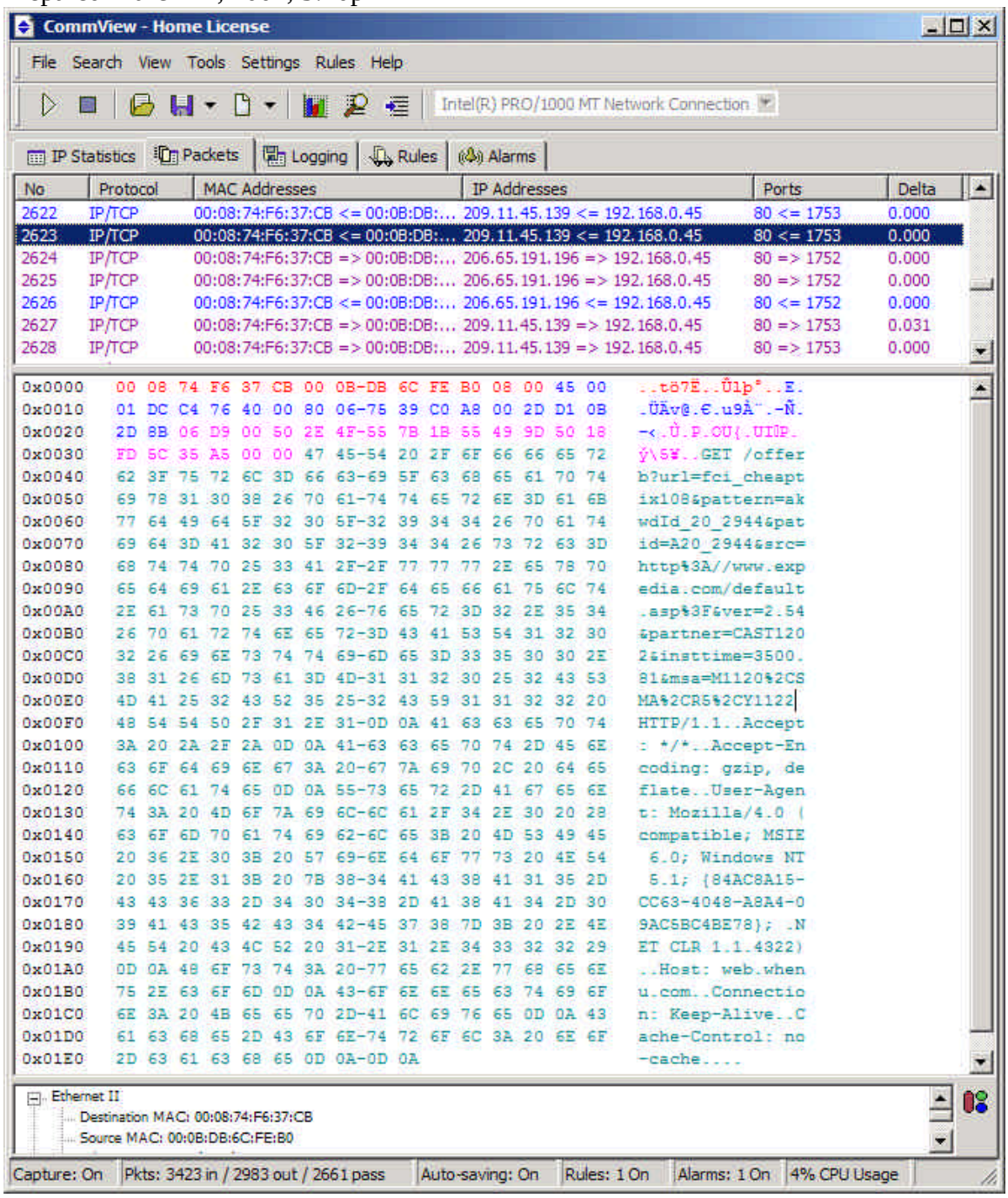
54. The rate of prevalence of spyware at the University of Washington may be a poor proxy for the rate of prevalence of spyware elsewhere. The authors recognize and discuss this divergence when they specifically study and document the fact that users' home computers have spyware to a greater extent than official university computers (section 4.2.2). The lower infection rate among campus computers likely reflects that campus computers are maintained by systems administrators who periodically remove spyware, or even put in place systems that, with at least some level of success, block spyware from becoming installed in the first instance. (My own university, Harvard, uses such systems on most public computers: Public computers are typically "reimaged" nightly with a fresh hard disk copy, such that any spyware installed in the prior day is automatically removed. This system comes at high costs in flexibility, network traffic, and staff time, but it does mitigate a portion of the risk of spyware.)

55. In short, then, the rate of spyware installation in other environments – homes, primary and secondary schools, libraries, Internet cafes, hotels, and the like – is likely to differ greatly from what the authors report. In particular, in my experience, the spyware infection rate in other environments is likely to be far higher.

56. However, the data collection methods proposed by Saroiu et al. could be generalized to these other populations. For example, an ISP could readily determine the rate of prevalence of spyware among its customers. I'd be pleased to work on this project with any interested ISP, subject only to data availability and privacy concerns.

Attachment 1: Transmission of Personal Information by WhenU – Screen Shot

Prepared March 12, 2004, 3:40pm



CommView is the program I have selected to monitor and record transmission between my computers and the Internet. Here, 192.168.45 is a computer in my lab, while 209.11.45.139 is the `web.whenu.com` web server.