

**SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK**

-----X
THE PEOPLE OF THE STATE OF NEW YORK
by **ELIOT SPITZER, Attorney General**
of the State of New York,

**AFFIRMATION OF
JUSTIN BROOKMAN**

Petitioners,

Index No. _____

-against-

INTERMIX MEDIA, INC.

Respondent.
-----X

JUSTIN BROOKMAN, an attorney admitted to practice before the Courts of the State of New York, makes the following affirmation under the penalty of perjury:

1. I am an Assistant Attorney General in the office of ELIOT SPITZER, Attorney General of the State of New York, assigned to the Internet Bureau. I am familiar with the facts and circumstances of this proceeding.
2. The facts set forth in this affirmation are based upon information contained in the files of the Internet Bureau.
3. I submit this affirmation in support of the Attorney General's application for an Order which, inter alia, (a) enjoins Respondent's violation of New York General Business Law §§ 349-50, Executive Law § 63(12) and New York common law; (b) requires Respondent to issue an accounting; and (c) requires Respondent to pay disgorgement of unjust enrichment, as appropriate, and penalties and costs to the State of New York.

A. Parties

4. Petitioners are the people of the State of New York, by their attorney, Eliot Spitzer, Attorney General of the State of New York. Petitioners have offices in the County of New York, located at 120 Broadway, New York, New York.

5. Defendant Intermix Media, Inc. (“Intermix”) is a Delaware corporation with its principal offices in Los Angeles, California. See Exh. 1 hereto (Intermix 10-Q, dated February 14, 2005). Since at least 2003, Intermix has placed spyware programs onto the computers of several million users, including over three million New York state residents. See Exh. 2 (facsimile from A. DeVore to K. Dreifach, dated April 4, 2005). In most (if not all) cases, Intermix has done so without disclosing these programs to users, and without obtaining users’ consent. Intermix installs this spyware onto the computers of unsuspecting users both through its own proprietary websites, and through the websites of third party agents.

6. Intermix describes itself as “a leading Internet marketing company combining extensive consumer reach, innovative technologies, and superior content to provide advertisers, partners, and affiliates with unique and effective Internet marketing opportunities.” See Exh. 3 (screen shot from <http://www.intermix.com>). Intermix’s business operations are divided into two primary divisions: (1) Alena, a product marketing group, which sells a wide range of Intermix products, ranging from skin lotion to nutritional supplements; and (2) the Intermix Network, which sells internet advertising. See id. Because the Attorney General’s Verified Petition focuses entirely on the activities of the latter business group, references to “Intermix” refer to the Intermix Network division.

B. Intermix's Deceptive Spyware Installations: Background

7. Intermix operates more than 40 distinct web domains offering a wide range of interactive content, including games, screensavers and cursors for users to download. See, e.g., Exh. 4 (screen shot from www.flowgo.com). By embedding additional hidden programs within such content, Intermix has surreptitiously installed onto users' computers several types of invasive and annoying computer programs, which advertise and promote the products of its clients. It has engaged agents to do likewise, from similar websites.

8. These advertising programs, commonly known as "spyware" or "adware," include Intermix programs such as "KeenValue" (which delivers pop-up ads); "IncrediFind" (which automatically redirects web addresses to Intermix websites); "Updater" (a program that allows Intermix to add or update programs and functionality to a user's computer); and various "Toolbar" programs (programs that overlay onto users' web browsers a "toolbar" linking to Intermix's services and clients). Because these programs are permanently installed on the user's hard drive and run during subsequent web browsing sessions, they continue to advertise Intermix clients and report information about the user long after the user has left the websites of Intermix or its agents.

9. Generally speaking, Intermix does not obtain users' consent before it uploads and installs spyware onto their computers. In tests of all known Intermix distribution sites performed by Attorney General Investigator Vanessa Ip, Intermix spyware was each time installed on undercover computers without proper notice. See accompanying Affidavit of Investigator Vanessa Ip dated April 18, 2005 ("Ip Aff."). These tests were conducted across seven websites operated by Intermix and its agents during a four month period.

10. These tests, and other information Intermix has provided to this office, document how Intermix and its agents deceptively and surreptitiously disseminated Intermix spyware. First, they offer a “free” software program for users to download, such as a screensaver or game. Upon download, however, Intermix surreptitiously tacks onto that program various spyware programs without disclosure to consumers. In this way, known as “bundling,” Intermix has spread its advertising programs onto millions of consumers’ hard drives. Documents that Intermix has provided to this office indicate that the company’s products were downloaded more than three million times by New Yorkers alone during 2003 and 2004. See Exh. 2 (facsimile from A. DeVore to K. Dreifach, dated April 4, 2005).

11. When bundling its spyware with other programs, Intermix offers either no notice or only token notice to consumers about the hidden spyware programs. Intermix either fails to disclose these additional programs in any manner, or hides mention of them deep within a lengthy, legalistic license agreement. Even in the latter case, the information provided is vague, incomplete and often factually incorrect.

C. The Attorney General Has Recorded Intermix’s Deceptive Spyware Installations

12. Between November 2004 and February 2005, Attorney General Investigator Vanessa Ip has on ten separate investigative sessions downloaded Intermix’s spyware, both from Intermix’s proprietary websites, and from sites that Intermix has enlisted and paid to distribute its spyware by bundling it with other programs.

13. In every single session, Investigator Ip documented that one or more undisclosed

Intermix spyware programs had been silently installed along with the advertised free programs.¹ The following sections discuss several examples of this bundling practice in detail. The tests conducted by the Attorney General’s Office are described in greater detail in the Ip Affidavit ¶¶ 3-192.

(i) Deceptive Spyware Practices
At Intermix’s MyCoolScreen.com Website

14. One such website through which Intermix has spread its spyware programs is <http://www.MyCoolScreen.com>. This website is registered to and operated by Intermix. See Exh. 5 (whois.net registration listing); see also Exh. 6 (letter dated December 23, 2004, from W. Heberer to J. Brookman at pp. 1, 3).

15. On MyCoolScreen.com (as on its other proprietary websites), Intermix advertises several “free” screensavers for users to download,² including “Hot Jalapeno Dance”; “Gobbler Garden” (a Thanksgiving screen saver); and “Fairy Wonderland” (cavorting fairies). See Ip. Aff. ¶¶ 3-41. On three separate occasions, Investigator Ip downloaded and installed each of these screensavers at least once. On each occasion, Intermix also installed several undisclosed spyware programs,

¹ Before beginning each test, Ip ran multiple diagnostic programs and analyses to document the programs and files installed on the test computer. After downloading a “free” program from Intermix or its agents, Ip then ran the same tests thereby obtaining a list of the same programs and files, plus additional programs and files that had been installed on the computer during the test.

² “Screensavers” are animated programs that are activated when a computer has been idle for a specified amount of time, e.g., fifteen minutes. Originally, these programs were designed to prevent images from being “burned” onto a user’s screen – a phenomenon that sometimes occurs on cathode ray screens when a static image has been consistently displayed over an extended period of time. While modern computer screens are less susceptible to this problem, screensavers remain popular programs for displaying an amusing cartoon, an entrancing graphical animation or a series of family photos whenever the computer is not in use.

as described below.

16. For instance, on November 15, 2004, Investigator Ip downloaded the “Hot Jalapeno Dance” screensaver. Prominently advertised on the MyCoolScreen home page, this program promised users an extended cartoon of dancing jalapeno peppers. See Ip. Aff. ¶ 6. Nothing on the MyCoolScreen homepage, shown below as Screen Shot No. 1, made any mention of other programs that would be bundled with this (or any other) screensaver. See id.³

³ For reference, several of the screen shots referred to herein are included as graphics in this Affirmation; a complete set of these screen shots is annexed to the accompanying Ip Affidavit.

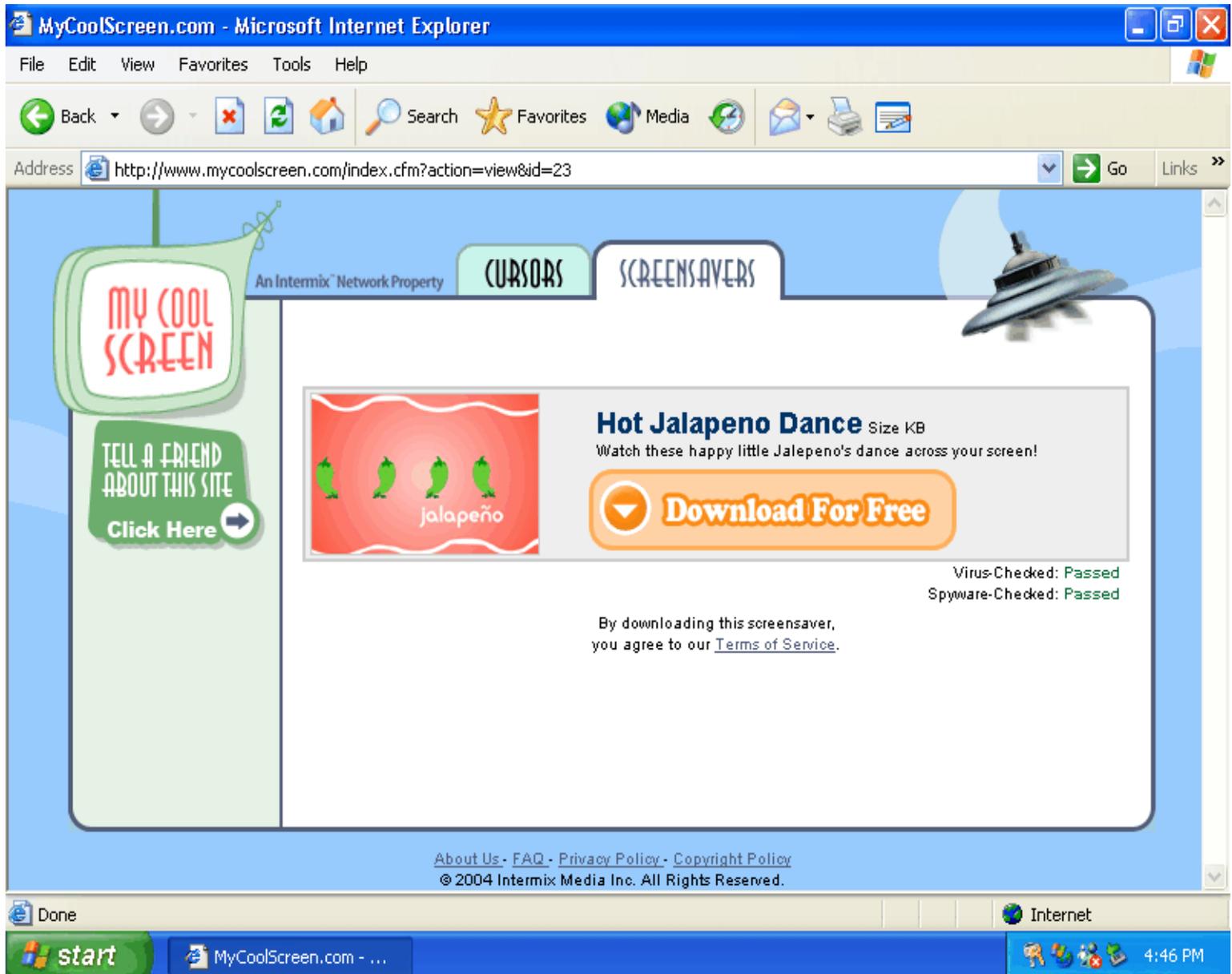
SCREEN SHOT NO. 1



17. After clicking on the offer to “Download Now!” (seen above), Investigator Ip was taken to a screen further describing the software to be downloaded. Again, no description of any bundled spyware products appeared; rather, the entire description of the “Hot Jalapeno Screensaver,” shown below as Screen Shot No. 2, was simply an invitation to “[w]atch these

happy little Jalepeno's [sic] dance across your screen!," above a button offering users to "Download for Free." See Ip. Aff. ¶ 7. Two inaccurate disclaimers on that same page even falsely promised "Virus-Checked: Passed" and "Spyware-Checked: Passed." See id.

SCREEN SHOT NO. 2

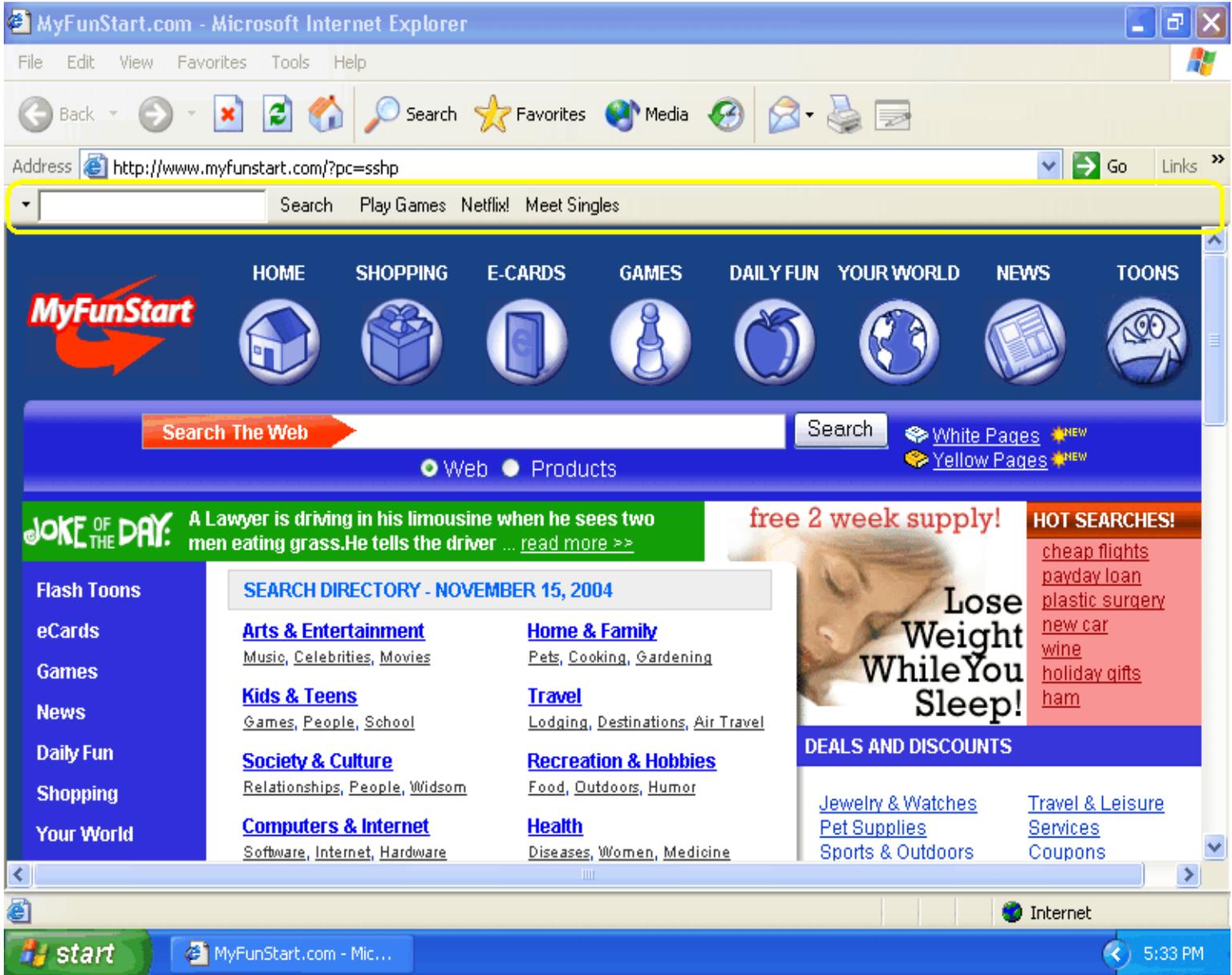


18. When Investigator Ip clicked on the “Download For Free” button, she was asked to provide personal information (including date of birth, country of residence and email address), presented with offers from Intermix affiliates (offering suspect deals such as online degrees and free gift cards and laptops) and finally shown a dialog box asking whether to open the program file from Intermix. See Ip Aff. ¶¶ 9-12. Again, spyware and other bundled programs were never mentioned or disclosed on any of these screens. See id. ¶ 6. The only hint of disclosure came from a vague statement, on just one screen and in tiny print, that “[b]y downloading this screensaver, you agree to our Terms of Service.” See Screen Shot no. 2, supra p. 8; Ip Aff. ¶ 7 (discussed infra ¶¶ 26-29).

19. When Investigator Ip opened the executable program file, our test computer downloaded the linked file from Intermix’s servers. See Ip. Aff. ¶¶ 13-14. This file was self-executing, i.e., after downloading, the file immediately began to install a number of programs on our computer without further interaction. See id. ¶ 14. One of those programs was the “Hot Jalapeno Dance” screensaver program advertised. See id. ¶¶ 15-18. In addition, however, a number of spyware programs that were never disclosed were installed on the test computer. See id. ¶¶ 16-24

20. For instance, in addition to the promised “Hot Jalapeno Dance,” Intermix had surreptitiously installed a “*FloGo*” *toolbar* that appeared under the traditional toolbars on our computer’s Internet Explorer browser program. See Ip. Aff. ¶ 16. In other words, under the common buttons found on users’ screens (“Back,” “Forward,” “History, ” etc.) and the web address, Intermix had installed onto our computer its own toolbar with its own buttons and forms. See Screen Shot No. 3, below (“FloGo” toolbar circled in yellow).

SCREEN SHOT NO. 3



21. This “FloGo” toolbar contained several buttons linking to various Intermix (and Intermix affiliate) websites and also provided a permanent form for users to directly search the internet using Intermix’s search engine. Intermix derives a substantial amount of its revenue from its search engine service, as advertisers pay to be placed prominently within the search engine’s

results. See Exh. 1 (Intermix 10-Q, dated February 14, 2005, pp. 23, 36).

22. During that same download of the “Hot Jalapeno Dance,” Intermix also surreptitiously installed a program called “**IncrediFind**” that *redirects domain addresses* that users typed into the address bar to Intermix’s own websites instead. See Ip. Aff. ¶¶ 17, 20-21. Thus, for instance, when our Investigator sought to access the website <http://www.search.netscape.com> (the default search page for the popular Netscape Navigator web browser), Intermix’s spyware program instead hijacked this request and redirected it to the Intermix search page <http://www.incredifind.com> instead. See id. ¶¶ 40, 94, 126, 187, 190. Similarly, mistyped and erroneous addresses were redirected to Intermix’s IncrediFind page. See id. ¶¶ 41, 95, 186. Equally intrusive, when our Investigator sought to exit the IncrediFind web page, either by entering another web address or by closing the browser window, Intermix generated one or more pop-up advertisements. See id. ¶¶ 191-92.

23. As if all of this were not enough, Intermix installed during this same session yet another undisclosed and unwanted program called “**KeenValue**” which *displays pop-up advertisements* to users as they surf the web. See Ip Aff. ¶¶ 17-19. Unlike pop-up ads that are generated directly by a particular website, KeenValue remained permanently active on our test computer and continued to display pop-up ads long after the Investigator left Intermix’s website. Worse still, the program automatically reactivated every time our computer was turned on, meaning it could (and did) display pop-up advertisements during any subsequent browsing session in the future. See id. ¶ 39; Screen Shot No. 4, below (example of KeenValue pop-up ad for Vonage).

SCREEN SHOT NO. 4

The screenshot shows a Microsoft Internet Explorer browser window displaying the New York Times website. The address bar shows <http://www.nytimes.com/>. The page features the newspaper's masthead, a search bar, and a navigation menu. A large advertisement for Vonage is overlaid on the page, featuring a hand holding a telephone receiver and the text "Add one for only \$14.99/mo. more please". The advertisement URL is <http://images.keenvalue.com/kv/rb/AdDotCom.asp?id=64A4F05C-FFB4-4EE3-A53A-B1B68017BEAE...>. The website content includes news articles such as "Will More Power for Intelligence Chief Mean Better Results?" and "Ukraine Parliament Vote Sweeping Electoral Change".

24. Finally, during this same “Hot Jalapeno Dance” installation, Intermix secretly hijacked our test computer’s home page, changing it to <http://www.MyFunStart.com> – an Intermix website (see Screen Shot No. 3, *supra* p. 10). See Ip. Aff. ¶ 16. (A user’s “home page” is the initial page a web browser displays when opened.)

25. Intermix did not disclose any of the above programs during the “Hot Jalapeno Dance” download process. Indeed, none of the six screens which consumers were required to view before downloading “Hot Jalapeno Dance” from Intermix mentioned these programs, their functions or the fact that downloading them was a condition to receiving the screensaver.

26. The sole trace of disclosure anywhere on the MyCoolScreen.com site occurred in a license agreement reached only when Investigator Ip clicked through the tiny “Terms of Service” link on Intermix’s website, shown above in Screen Shot No. 2. See supra p. 8; Ip. Aff. ¶¶ 7-8.

The user was not required to view these Terms before downloading the programs, and was never even shown them, either during or after download and installation. Only once on the six screens leading up to download was the user told she was implicitly agreeing to these “Terms,” and even then, the statement was made beneath the rest of the text on the screen, in an extremely small font, and after the user was promised that the software was virus-free and spyware-free. See id.

27. Users who happened to open this “Terms of Service” link would find a purportedly binding “End User License Agreement,” encompassing arcane matters from liability limitations to jurisdiction to license restrictions. See Ip. Aff. ¶ 8. In the middle of one long, untitled paragraph, Intermix cryptically revealed that:

by installing this software, you will automatically receive the GripPack. The GripPack is comprised of two applications: 1) the Grip toolbar 2) NetGuide, a redirect page. NetGuide is a piece of navigational software that offers results and suggested sites for misspelled web addresses (instead of taking you to a standard error page). NetGuide also enables users to conduct web searches directly from the browser.

See id.

28. Thus, the sum total of information provided to consumers about the spyware they are about to receive is buried in a license agreement that is itself poorly disclosed. Yet, even this

disclosure mis-describes Intermix’s software. For instance, it omits that “NetGuide” (presumably the IncrediFind redirect program described supra ¶ 22) hijacks certain website addresses as well as mistyped addresses. It likewise inaccurately states that NetGuide offers “results and suggested sites” for erroneous web addresses; in reality, it merely redirects users to Intermix’s own search engine’s home page. See Ip Aff. ¶¶ 41, 95, 186.

29. This hidden “disclosure” – plainly deceptive even as to the toolbar and IncrediFind – fails even to mention the other KeenValue spyware program installed. Furthermore, the disclaimer inaccurately states that the user “will be given the opportunity to . . . choose to have [the] default page reset to <http://www.MyFunStart.com>.” In fact, users’ home pages are changed automatically and without notice. See Ip Aff. ¶ 16.

30. Investigator Ip recorded the installation of screensaver programs from MyCoolScreen.com on two other occasions. See Ip Aff. ¶¶ 22-41. Both times, the above-described spyware programs were installed in the same fashion, without notice or consent. See id.

**(ii) Deceptive Spyware Practices at
Intermix’s Cursorzone.com Website**

31. Investigator Ip recorded similar practices at <http://www.CursorZone.com>, another website registered to and operated by Intermix. See Exh. 7 (whois.net registration page); see also Exh. 6 (letter dated December 23, 2004, from W. Heberer to J. Brookman at pp. 1, 3).

32. For instance, during a download conducted on November 16, 2004, Investigator Ip found that Looney Toon cursors marketed by this website were secretly bundled with another toolbar program (very similar to the FloGo toolbar bundled with Intermix’s screensavers), as well as the NetGuide redirect program. See Ip. Aff. ¶¶ 42-64. As with MyCoolScreen.com, none of the ten

web pages through which a user had to navigate to download and install the cursor program made any mention of NetGuide, either by name or description. See id. ¶¶ 44-56. To the contrary, Intermix falsely promised users (many of whom presumably are children) that the software contained “No Adware!” and “No Spyware!” See id. ¶ 52.

(iii) Deceptive Spyware Practices on Acez.com

33. In addition to bundling its spyware products with its own seemingly innocuous software, Intermix directed and paid other companies to sneak spyware onto users’ systems.

34. One such Intermix agent was Acez Software LLC (“Acez”), which operates websites including Acez.com. Acez.com is operated out of New York by Bryan Sambrook, a resident of East Greenbush, New York. See Exh. 8 (Network Solutions whois page). Between June 2003 and February 2005, Acez on Intermix’s behalf distributed at least 1,118,588 distinct bundles of IncrediFind, KeenValue and/or the “PowerSearch” toolbar (another Intermix toolbar variation). Intermix contracted with Acez to distribute these programs (see Exh. 9) and paid Mr. Sambrook \$173,810, based on the revenue generated by Acez’s installations of Intermix spyware. See accompanying Affidavit of Bryan Sambrook, President of Acez, dated April 7, 2005 (“Sambrook Aff.”), ¶¶ 3-4, 10.

35. As described below, Acez, on Intermix’s behalf, spread spyware to consumers from <http://www.acez.com> by deceptively bundling it with screensavers – in methods virtually identical to the methods on Intermix’s proprietary sites described above.⁴

36. On November 30, 2004 and January 26, 2005, Investigator Ip downloaded two screensavers from Acez.com; each time, Intermix spyware was surreptitiously installed as well.

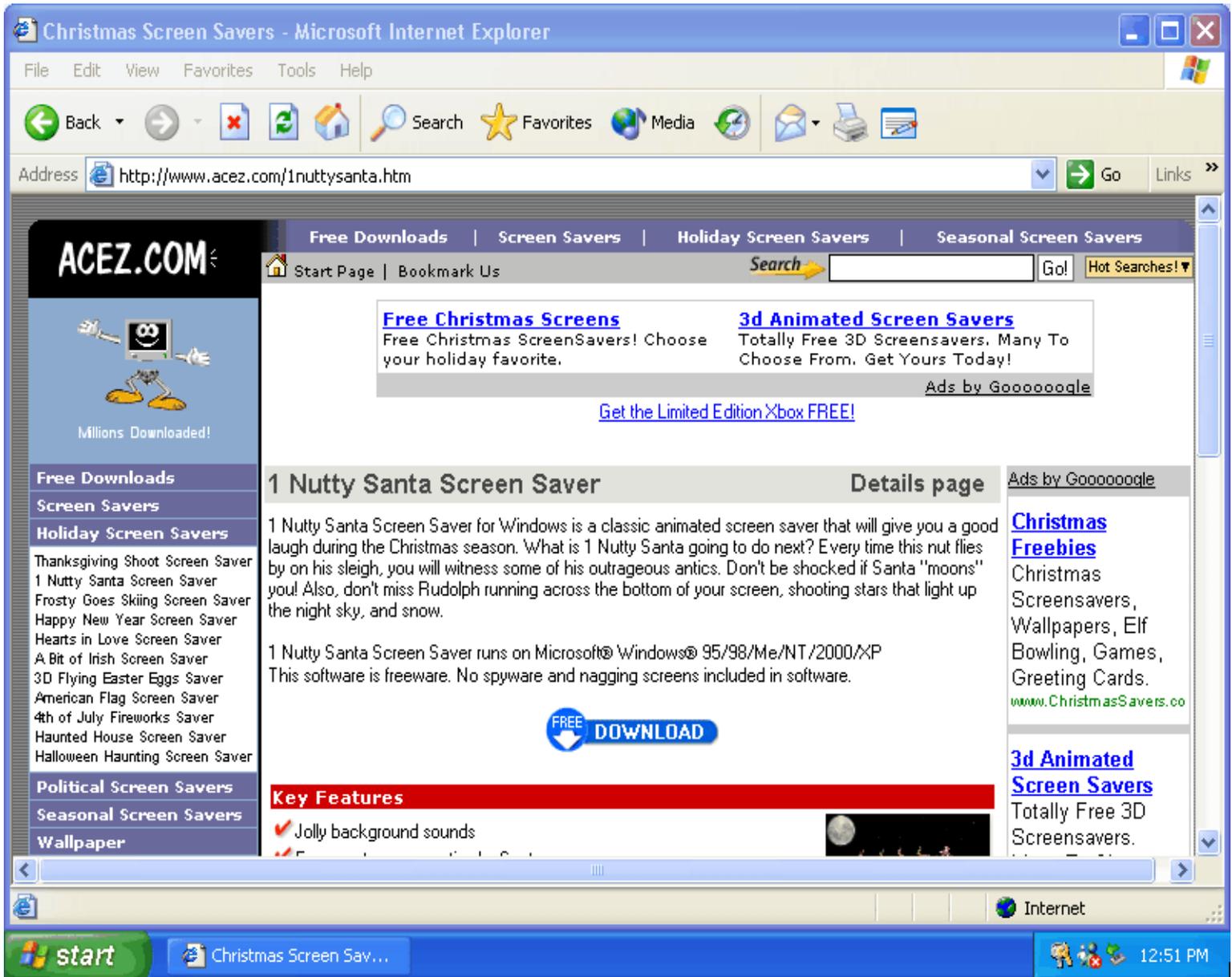
⁴ Mr. Sambrook and Acez settled with the Attorney General’s Office via Assurance of Discontinuance dated April 15, 2005, agreeing to injunctive, equitable and punitive relief.

See Ip. Aff. ¶¶ 65-97. As on MyCoolScreen.com, any mention of additional programs to be received was buried within a license agreement, and even this information was deceptive, vague and incomplete.

37. For instance, on November 30, 2004, Investigator Ip downloaded a “free” Christmas screensaver labeled “1 Nutty Santa Screen Saver” (a dancing Santa that drops his trousers), prominently advertised on the main Acez page. See Ip. Aff. ¶ 68. When Ip clicked on the “Nutty Santa” icon, the site presented a description of the screensaver and a “Free Download” button. See id. ¶ 69.

38. The same web page also explicitly promised, “This software is freeware. No spyware and nagging screens included in software.” See Ip Aff. ¶ 69. A similar statement on the same page emphasized, “Free. No spyware or nagging screens.” See id.; Screen Shot No. 5, below.

SCREEN SHOT NO. 5



39. Neither these pages, nor any other on the Acez website, contained any disclosure or reference regarding the spyware programs bundled with Acez screensavers. See Ip Aff. ¶ 67.

40. Nonetheless, as set forth in the Ip Affidavit, each time an Acez screensaver was installed, the IncrediFind spyware program was also installed, without warning or disclosure. (As noted supra ¶ 22, IncrediFind redirects certain web addresses, searches and erroneous addresses to

Intermix websites.)

41. The sole reference to Intermix's software is deep within an End User License Agreement, which runs over 10 pages and is provided on a small screen that cannot be expanded or printed by the user. See Ip Aff. ¶ 73. This Agreement is presented to users only after they have downloaded the software.⁵

42. Several pages into this license agreement, it is cryptically revealed (under the vague heading "Additional Information") that users will receive "eUniverse's helper object (IncrediFind)," which "provides a results page for unsuccessful search results."⁶ Even this hidden description is wildly inaccurate: there is no "results page," and users are redirected not from "unsuccessful search results" but from unavailable or non-existent web addresses. The description conveniently fails to mention that IncrediFind redirects actual web addresses as well. See Ip Aff. ¶ 73.

43. Acez deceptively bundled this program on Intermix's behalf between June 2003 and February 2005. Until January 2004 and October 2004, respectively, Acez also bundled the even more intrusive "KeenValue" pop-up program and "PowerSearch" toolbar. See Sambrook Aff. ¶¶ 3-4, 10.

44. Intermix was at all times aware of, directed and controlled Sambrook's deceptive actions. For instance, Intermix's Todd Smith provided Sambrook with the code for Intermix's spyware programs, and determined what disclosure would be provided to Acez's customers. See

⁵ Unlike the file downloaded from MyCoolScreen.com, the Acez file did not self-install. Instead, an installer interface called "Installation Wizard" guided us through the process of installing the software on our test computer. See Ip Aff. ¶ 72.

⁶ Intermix was known as eUniverse, Inc. prior to July 15, 2004. See Exh. 1 (Intermix 10-Q, dated February 14, 2005, p. 6).

Sambrook Aff. ¶¶ 4-5.

45. Sambrook had no prior experience bundling spyware with his screensavers before, and simply integrated the code and descriptions that Intermix gave him. See Sambrook Aff. ¶¶ 2, 5. During his two-year relationship with Intermix, he informed Mr. Smith several times that makers of security software such as Symantec and McAfee considered Intermix's programs spyware or adware. See id. ¶ 8. Smith, with whom most of Sambrook's communications occurred, was at the time the head of Intermix's "downloads" division and is listed in several news stories as the company's "spokesperson." See, e.g., Exh. 10 (MSNBC.com article, dated May 20, 2004). Sambrook also told Smith about criticisms he had read about Intermix's bundling practices on several prominent web forums. See Sambrook Aff. ¶ 7.

46. Not only did Intermix fail to heed these warnings, after Sambrook informed Intermix executive Todd Smith that the Attorney General's office was investigating their practices, and that he therefore wished to terminate his contract with Intermix, Mr. Smith urged him to continue. Smith wrote, "I just hate for you to give up all the revenue when I don't think you have done anything wrong. I just don't want to send the wrong message to the AG office that you did something wrong by discontinuing." See Sambrook Aff. ¶ 9.

47. In fact, on February 20, 2005, more than two months after the Attorney General first contacted Intermix, Smith again urged Sambrook to continue. Even when Mr. Sambrook pointed out that Intermix had included functionality that even he had not known about, Mr. Smith insisted, "I just don't see how anyone did anything wrong." See Sambrook Aff. ¶ 9.

48. On February 9, 2005, Mr. Sambrook discontinued bundling Intermix spyware with Acez screensavers. See Sambrook Aff. ¶ 10. However, over the previous 20 months, Intermix had spread its spyware to over 1.1 million computers by secretly bundling its spyware with Acez's

screensavers. See Exh. 11 (letter from W. Heberer to J. Brookman, February 16, 2005).

(iv) Deceptive Spyware Practices at JenniferLopez.net

49. At <http://www.JenniferLopez.net>, Investigator Ip recorded another variation in how Intermix deceptively installs its spyware onto users' computers. See Ip. Aff. ¶¶ 98-111. In this example, Intermix's spyware was installed by another spyware program that had surreptitiously installed itself on our test computer.

50. On its face, JenniferLopez.net is a typical fan site, offering pictures, news and gossip about the popular actress and singer. (The site appears to have no direct affiliation with Ms. Lopez.)

51. However, many of the website's pages contain malicious code that installs spyware programs onto users' computers. This code is written in common scripting languages such as ActiveX and Javascript, languages designed to make given websites more graphically dynamic by executing small programs on users' computers when the users visit that site. While these languages were originally developed to help developers offer interactive (and wholly innocuous) features such as animations and drop-down menus, some companies have exploited the languages as a means to gain access to users' computers to spread spyware. Intermix pays agents, often other spyware companies, to install Intermix programs in just this way.

52. For instance, in tests that Investigator Ip performed on November 18, 2004, each time she entered the "Galleries" section of the JenniferLopez.net website, the site immediately attempted to execute a spyware program written in the ActiveX scripting language.

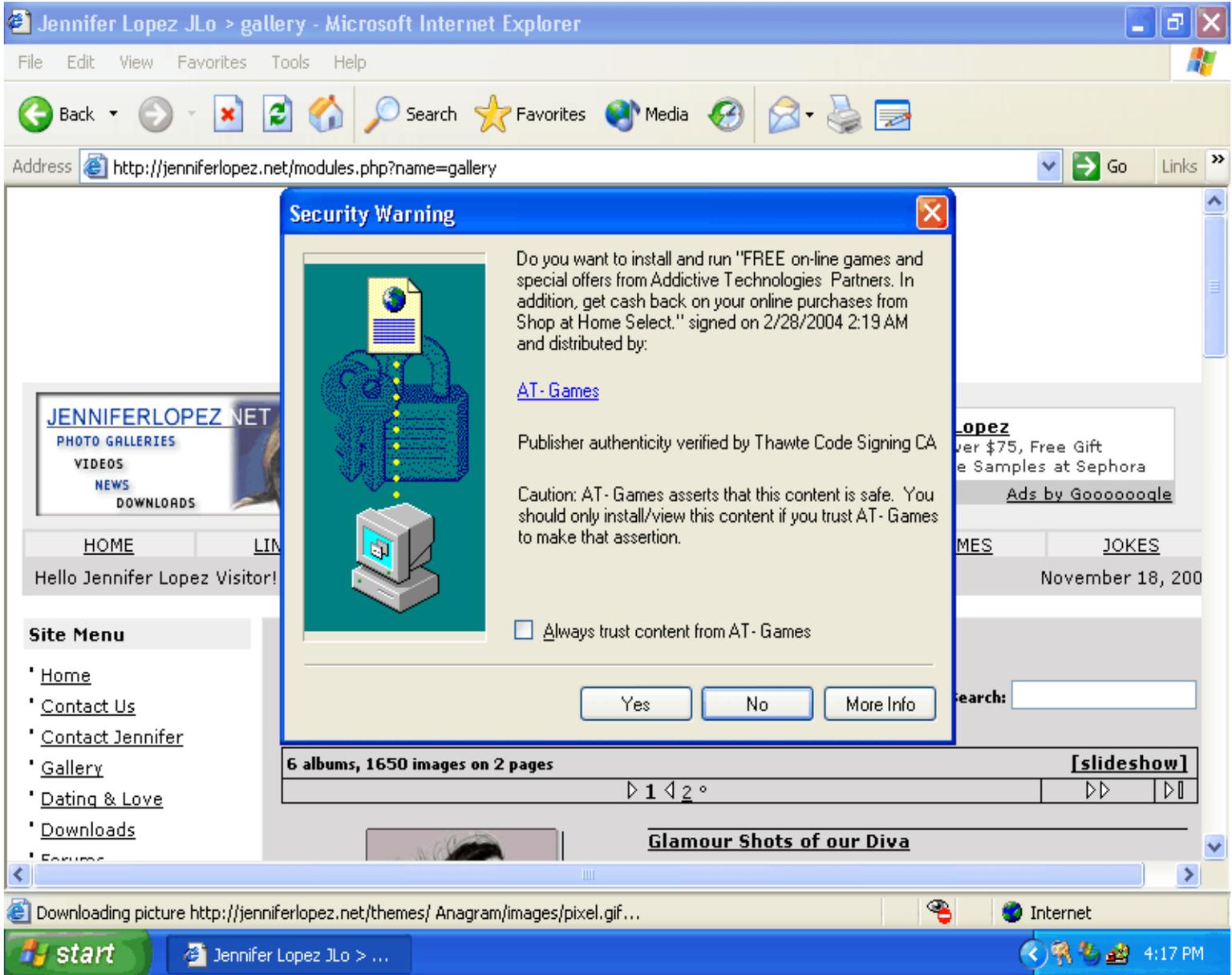
53. In one representative test, after Investigator Ip clicked on the "Galleries" link on the main page of JenniferLopez.net, our security parameters detected an ActiveX program written by the

company Mindset Interactive (“Mindset”),⁷ and we were presented with a box titled “Security Warning,” offering “FREE on-line games and special offers from Addictive Technologies Partners. In addition, get cash back on your online purchases from Shop at Home Select.”⁸ See Ip. Aff. ¶ 104. This box, shown below as Screen Shot No. 6, made no mention of any spyware or other programs from Intermix. See id.

⁷ Mindset owns and operates Addictive Technologies, the identified author of this particular ActiveX program. See Exh. 12 (archive.org screen shot of <http://www.addictivetechologies.com>). The precise relationship between Mindset and the proprietors of the JenniferLopez.net website is not known at this time. However, Mindset is a paid contractual agent of Intermix. See infra ¶ 58.

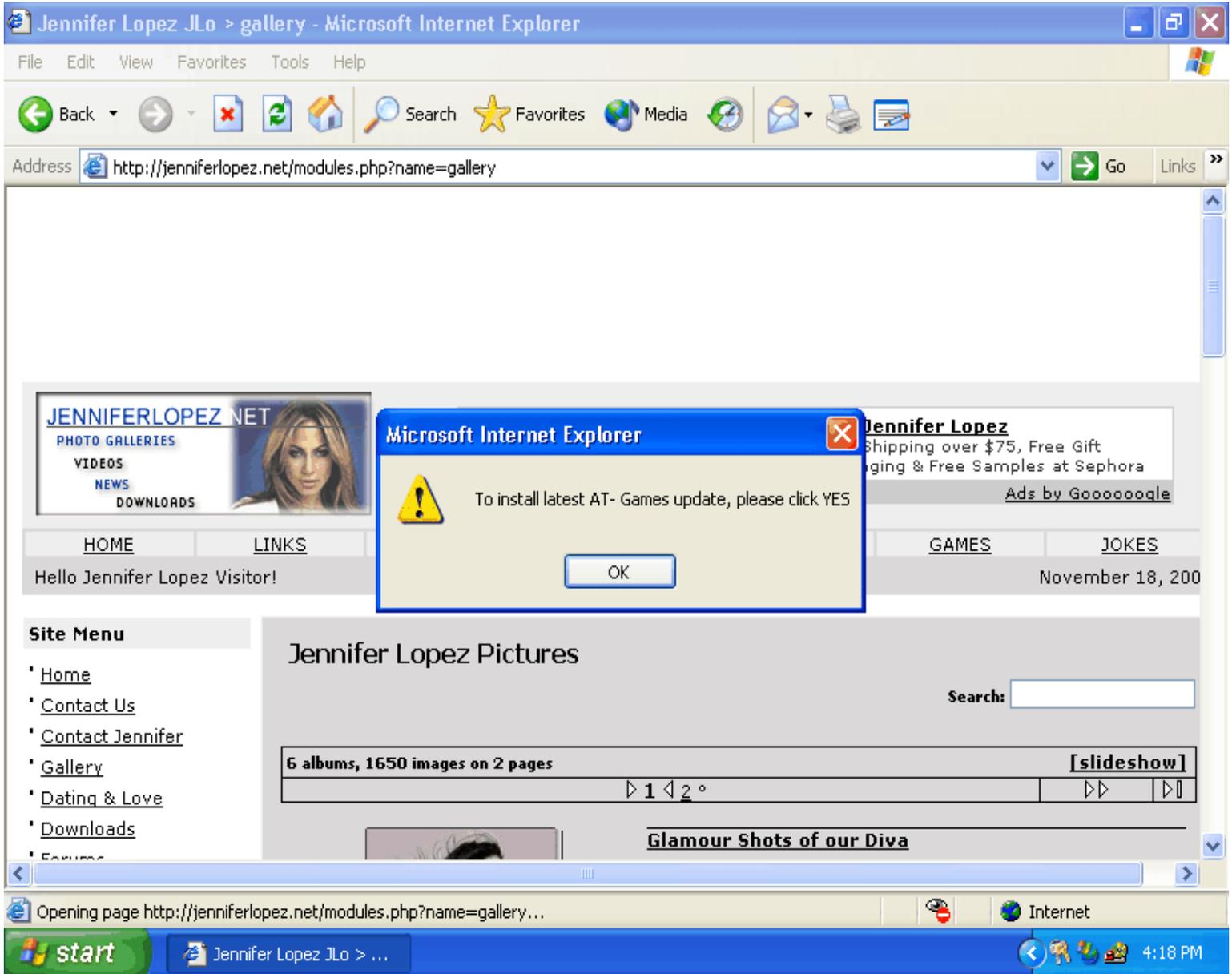
⁸ Before the latest version of Microsoft’s web browser (Internet Explorer 6.0), ActiveX programs would install and execute automatically on a user’s computer by default. See Exh. 13 (excerpt from *Malware: Fighting Malicious Code* by Ed Skoudis). Currently, because of abusive practices by spyware vendors, users who have Explorer 6.0 installed generally receive a “security” prompt before an ActiveX program executes. Consumers may nonetheless easily be duped by false descriptions, aggressive tactics and misleading statements.

SCREEN SHOT NO. 6



54. When Investigator Ip clicked “No” (i.e., do not install) to the prompt above, a Javascript program triggered another “pop-up” box reading “To install latest AT-Games update, please click YES.” See Ip. Aff ¶ 105. Again, as shown below in Screen Shot No. 7, there was no mention of any Intermix software. See id.

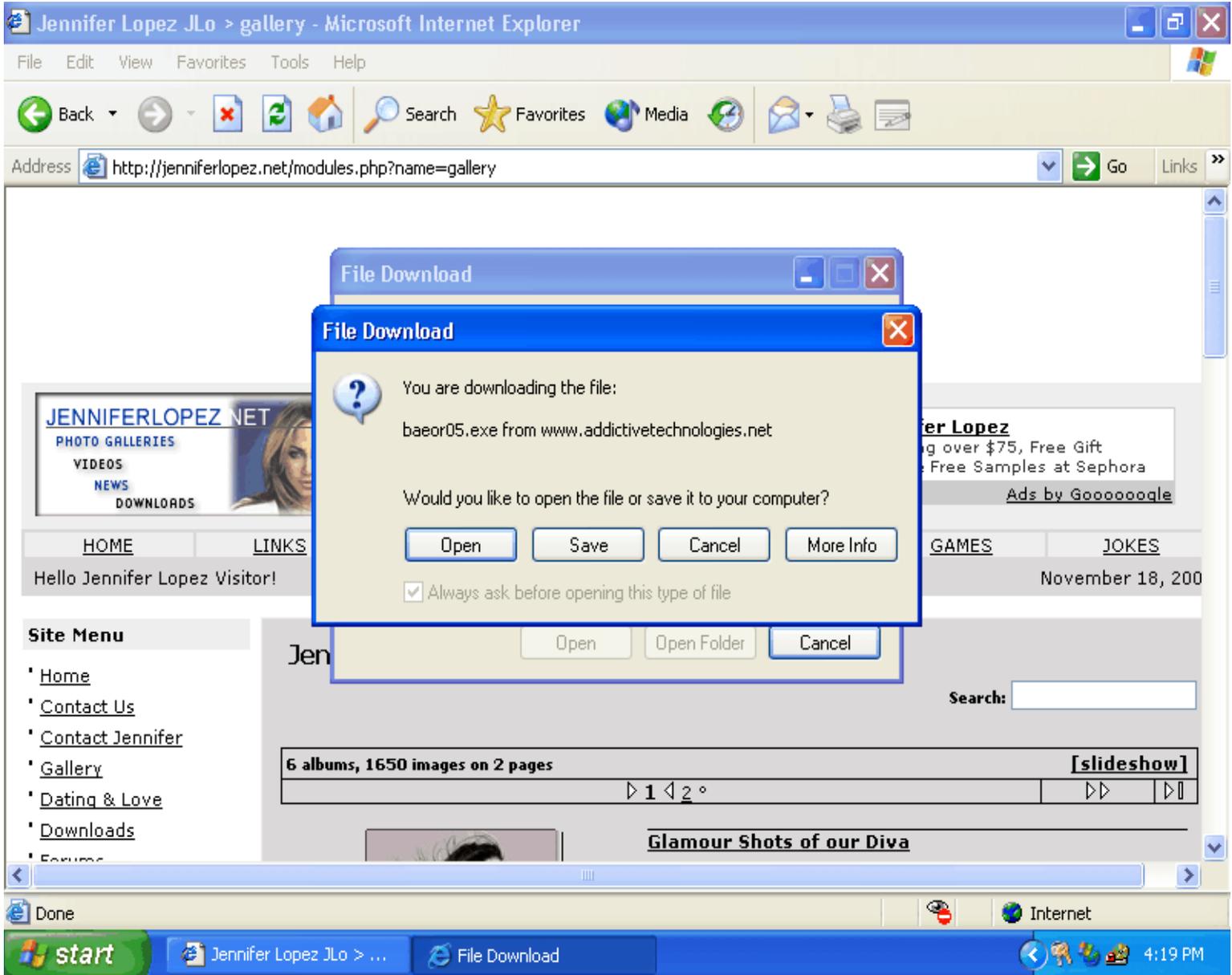
SCREEN SHOT NO. 7



55. When Investigator Ip next tried to close that pop-up box (offering installation of “AT-Games update”), the first ActiveX security box popped up again, offering “FREE on-line games and special offers from Addictive Technologies Partners.” See Ip. Aff. ¶ 106. Again, Investigator Ip clicked “No,” but this time a different Javascript box popped up, reading “This is a 1 time install, once you click Open it will never pop up this message again.” See id. ¶ 107.

56. After the investigator again closed the Javascript prompt, yet another pop-up box, shown below as Screen Shot No. 8, suddenly informed her that she was downloading a file identified as “baeor05.exe from addictivetechologies.net,” and asked “Would you like to open the file or save it to your computer.” See Ip Aff. ¶ 109. No description of Intermix software, or any other software, was provided. See id.

SCREEN SHOT NO. 8



57. Even though Investigator Ip clicked “Cancel” to try to stop the download and installation, the program began to silently download and install on our test computer. See Ip. Aff. ¶ 109. Several minutes later, Investigator Ip tested to see if any new programs had been installed on the computer. See id. ¶¶ 109-111. Instead of the “free games” promised by the ActiveX security box (and which Ip had never consented to install anyway), Mindset’s “FavoriteMan” spyware program was installed.⁹ FavoriteMan, in turn, had installed a number of other spyware programs on our test computer, including Intermix’s IncrediFind and another Intermix spyware program called “*Updater*,” which *allowed Intermix to “update” the software* it installed on our test computers. See id. ¶ 110.¹⁰

58. As described above, at no point before, during or after the installation process were these Intermix programs identified or described. See Ip Aff. ¶¶ 100-109. Indeed, in Investigator Ip’s tests, she had not consented to install any software on her computer. Documents produced by Intermix reveal that Intermix has paid Mindset’s parent corporation several hundred thousand dollars over the past two years to install Intermix’s spyware programs. See Exh. 14 (spreadsheet detailing periodic payments by Intermix).

⁹ “FavoriteMan” installs new icons on a user’s desktop and adds various links to the “Favorites” list in Internet Explorer; it also uploads and installs other spyware programs onto the computer’s hard drive.

¹⁰ Intermix uses this Updater program to install new versions of its spyware products on users’ computers, sometimes with added functionality. See Ip. Aff. ¶ 194. This is a particularly pernicious method of distribution, as there is no limit to the programs that Intermix may install on a user’s computer using the Updater function once Updater has been secretly installed. See id. ¶ 195. Updater is in constant communication with Intermix’s servers, determining whether newer versions of Intermix spyware are available to secretly install on users’ computers. See id. These updates occur silently, and the user is never notified that Intermix is “updating” its software on the user’s computer. See id.

D. Intermix's Deceptive Practices On Other Websites

59. The deceptive practices occurring at MyCoolScreen.com, CursorZone.com, Acez.com, and JenniferLopez.net are typical of the manner in which Intermix has spread its spyware from numerous websites, since at least 2003. Indeed, several Intermix installation methods are even worse, providing no hint – anywhere, in any form – that spyware is being bundled with the “free” software advertised.

60. For instance, as set forth in detail in the Ip Affidavit, Intermix distributes its spyware by bundling with animated desktop wallpaper programs offered at <http://www.ProgPlace.com>. See Ip Aff. ¶¶ 112-25. Nowhere on the ProgPlace.com website is there any mention whatsoever of Intermix or any bundled software. See id. ¶ 115. In Investigator Ip's test download of ProgPlace's “Winter Wonderland” wallpaper, the only reference to Intermix software was found in an End User License Agreement (or “EULA”) presented to users after download of the product. See id. ¶ 120. This EULA was contained on a small window that could not be expanded by the user and ran over twenty-two pages. See id. Although the EULA contained various legal provisions such as “Limitation of Liability,” “Ownership,” and “License Restrictions,” it provided no description of the Intermix software bundled with the screensaver. See id. Indeed, only a perceptive viewer would even have noticed that the EULA pertained not to the wallpaper program that the user had requested to download, but to an Intermix program instead. See id. After installing the “Winter Wonderland” wallpaper, Investigator Ip recorded that IncrediFind and Updater had been installed on the test computer without disclosure. See id. ¶¶ 122-25.

61. Intermix also secretly bundles its spyware with free software offered at <http://www.PCWeatherAlert.com>. See Ip. Aff. ¶¶ 137-57. This site allows users to download

small programs that provide constantly-updated weather information to the user on her desktop. During Investigator Ip's test of the PCWeatherAlert software, she received no notice whatsoever about Intermix or its bundled spyware programs. See id. ¶¶ 140-52. However, after downloading the free software, she discovered that several spyware programs, including IncrediFind and Updater from Intermix, had also been installed on her test computer. See id. ¶¶ 153-57.

62. [Http://www.TaskBuddy.com](http://www.TaskBuddy.com) is another site Intermix uses to distribute and install its spyware. See Ip Aff. ¶¶ 158-80. TaskBuddy.com offers free organizational software to help users organize their tasks and to-do lists. The TaskBuddy.com website does not mention Intermix or describe any Intermix spyware bundled with its free software programs. See id. ¶¶ 161-64. Nor does the TaskBuddy EULA mention or describe any Intermix bundled spyware. See id. ¶ 164. Nevertheless, after downloading and installing the TaskBuddy software, Investigator Ip recorded that Intermix's IncrediFind and Updater programs had also been installed without disclosure or notice. See id. ¶¶ 181-84.

63. These three websites – ProgPlace.com, PCWeatherAlert.com and TaskBuddy.com – have distributed Intermix spyware to more than 60,000 users in New York alone.¹¹ Each of these downloads are described in greater detail in the Ip Aff. ¶¶ 112-92.

¹¹ The websites PCWeatherAlert.com and TaskBuddy.com are owned by Intermix's agent Net Think Media (d/b/a Fabian Buys). See Exh. 15 (letter dated January 27, 2004, from W. Heberer to J. Brookman, p. 4). According to documentation provided by Intermix's counsel, New Yorkers have installed Intermix's spyware through this agent at least 60,037 times. See Exh. 16 (email dated March 7, 2004, from W. Heberer to J. Brookman, attachment).

**E. Intermix Obstructs User Efforts To
Detect and Remove Spyware Programs**

64. Further exacerbating the harm from its installation of hidden spyware programs, Intermix employs deceptive methods to prevent or impede user efforts to locate and remove its software.

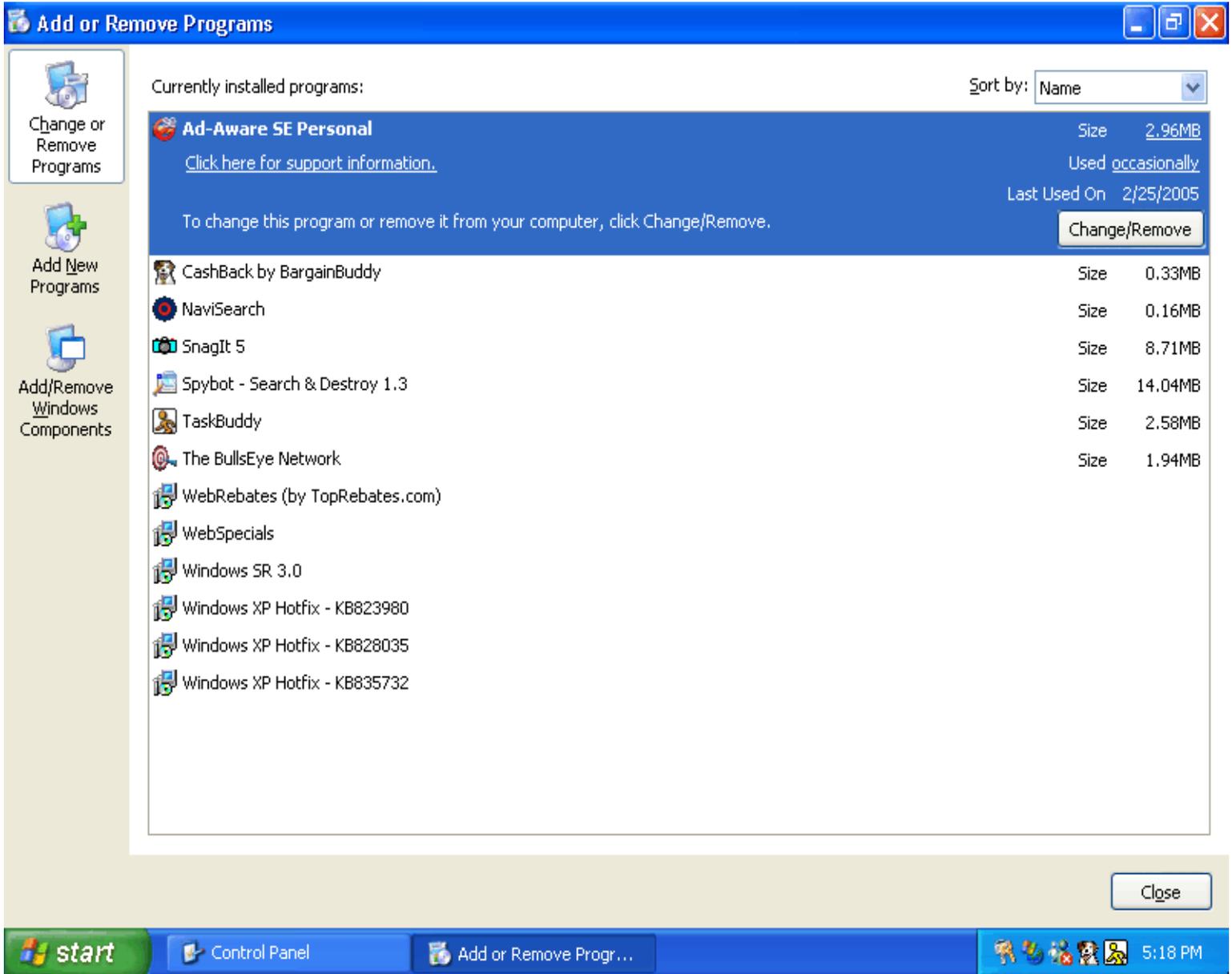
65. Plainly, as described in ¶¶ 7-63, supra, Intermix does not adequately inform consumers that its software has been installed on their computers. Thus, when users later receive annoying pop-up ads or redirected web page requests, they generally cannot identify and uninstall the offending programs.

66. Intermix goes even further to entrench the harm it causes through these deceptive spyware installations by making its programs extremely difficult for users to locate on a computer's hard drive, so that the programs can be removed. First, Intermix designs its spyware programs so that when the user uninstalls the program with which the spyware was bundled (e.g., a screensaver), Intermix's spyware programs remain behind, fully operational. In each of the tests our Investigator ran on Intermix's spyware programs, removing the original host program never resulted in the removal of Intermix's spyware programs. See, e.g., Ip. Aff. ¶¶ 17-21, 26-30.

67. Intermix also prevents its spyware programs from being listed in the "Add/Remove Programs" utility in the Microsoft Windows operating system. The "Add/Remove" feature is found in the Control Panel easily accessed from the Start Menu and is the most common mechanism by which consumers uninstall programs from their computers. See generally Exh. 17 (FTC Staff Report, Monitoring Software on Your PC: Spyware, Adware, and Other Software, March 2005, p. 7) ("FTC Spyware Report") (discussing problem of spyware programs that "cannot be removed using the Add/Remove Programs function and do not provide their own uninstaller," and citing testimony).

68. In our tests, after Intermix spyware installed itself on our computers, the spyware programs were rarely listed in “Add/Remove Programs.” See, e.g., Ip Aff. ¶¶ 18, 27, 82, 155, 185. Thus, for instance, as shown below in Screen Shot No. 9, when Intermix’s spyware programs were surreptitiously installed by the “TaskBuddy” program described supra ¶ 62, Intermix’s spyware programs did not appear in Microsoft’s “Add/Remove Programs” list. Underscoring the particularly egregious nature of Respondent’s conduct, the “TaskBuddy” application itself appeared in “Add/Remove,” as did other spyware programs that were also bundled with the TaskBuddy program. See Ip Aff. ¶ 185. In downloading Intermix’s spyware, Investigator Ip recorded at least seven instances in which the spyware was not listed in the computer’s “Add/Remove Programs.” In fact, in Ip’s tests, Intermix’s IncrediFind and Updater programs were never listed in “Add/Remove Programs.” See id. ¶¶ 18, 27, 82, 155, 185.

SCREEN SHOT NO. 9



69. Making the removal process yet more difficult, Intermix fails to provide its own “uninstall” utility within its spyware programs’ files or folders. See Ip Aff. ¶ 188. Such uninstall functions are common in the software industry, particularly when a given program cannot be uninstalled by the operating system’s Add/Remove feature. See Exh. 16, cited supra ¶ 67 (FTC Report p. 7). Indeed, during the TaskBuddy test cited above, Investigator Ip recorded

that several other spyware programs bundled with the TaskBuddy program (including TaskBuddy itself) provided their own uninstallers within their Program files; Intermix's IncrediFind and Updater programs, however, failed to do so. See Ip Aff. ¶ 188.

70. Even in the rare instance when Intermix does allow for the removal of its spyware programs, the uninstaller often does not work or leaves files and functionality behind. For example, in one test, Investigator Ip sought to uninstall IncrediFind using an uninstall program available at one of Intermix's websites. See Ip. Aff. ¶¶ 127-36. After a long and convoluted process, she received confirmation that the software had been removed. See id. ¶ 134. However, she was still unable to access the website <http://www.search.netscape.com>, and scans of her computer's hard drive indicated that no less than 17 Intermix files, folders and registry keys remained installed on her computer. See id. ¶¶ 134-36. Included in these files was the Updater program, which allows Intermix to install new versions of its spyware programs onto users' computers at its discretion. See supra ¶ 57, fn. 10.

71. Since many Intermix spyware programs cannot be uninstalled either through Microsoft Windows or through Intermix's own software, users must identify these programs, determine their names and locations, and then manually delete them – tasks involving both expertise and perseverance. Making this process more difficult, however, Intermix also hides its spyware programs in unlikely places on users' computers. In each test recorded by Investigator Ip, Intermix's spyware programs were never listed in the "All Programs" or "Programs" list accessed through the Start button on Microsoft Windows. See Ip. Aff. ¶ 189.

72. Even worse, Intermix's Updater spyware program was always placed in the unlikely "Common Files" folder within Windows. See Ip Aff. ¶¶ 14, 182. Downloaded programs commonly are stored in the appropriate and more commonly-accessed "Programs Folder"; the

“Common Files” folder, by contrast, typically houses small technical files that are shared by Microsoft programs. It is unlikely that even an experienced computer user would look in “Common Files” for a third-party spyware program.

73. Worst of all, Intermix thwarts savvy users who manage to find and delete their spyware programs by reinstalling its spyware after users have deleted it. During interviews with Intermix’s Chief Technology Officer Jeff Rajewski, Mr. Rajewski confirmed that Intermix’s “Updater” program has automatically reinstalled Intermix spyware programs onto users’ computers as newer versions became available – even when those same users had deliberately deleted the program previously. See Ip Aff. ¶ 196.

74. Thus, if a user deleted Intermix’s IncrediFind program from her computer (whether manually or through an anti-spyware program), Updater later would reinstall IncrediFind once a new version of the software became available. This “update” would occur without consent from or disclosure to the user. As noted supra, this Updater function is itself hidden in “Common Files,” and quite likely would escape the attention of a user seeking to remove unwanted spyware from her computer. See supra ¶ 72. Furthermore, even in the rare instance a user has the option to uninstall Intermix’s software, the Updater program is left behind to reinstall newer versions of Intermix’s spyware programs in the future. See Ip Aff. ¶¶ 127-36.

F. Pre-litigation Notice

75. Pre-litigation notice as provided for in New York General Business Law § 349 and § 350-c has been given, by certified mail delivered on five or more days notice to Respondent. See Exh. 18 (certified letters to Respondent and counsel containing Notice of Proposed Litigation).

76. Respondent repeatedly and persistently has engaged in fraudulent, deceptive and illegal acts in the course of distributing and installing its spyware programs. Respondent is responsible

for saddling unsuspecting consumers, including children, with untold amounts of spyware, hiding unwanted programs within apparently innocuous screensavers and games. Such practices not only harass, annoy, and intrude upon users, but damage the very integrity of e-commerce: such harassment and confusion repels consumers from using the Internet. Equally harmful, Respondent has deliberately made it exceedingly difficult for users to identify and uninstall these programs. Thus, consumers affected are generally not even provided a means to rid themselves of these unwanted programs or a party to whom to complain.¹²

77. Accordingly, Petitioners respectfully request that the court grant the relief requested in the accompanying Verified Petition, enjoining Respondent's deceptive business practices; requiring Respondent to issue an accounting; requiring Respondent to disgorge any unjust enrichment derived from its illegal activities; and awarding costs and penalties as authorized by statute, and such other relief as requested herein.

WHEREFORE, the Attorney General respectfully requests that the Court grant the relief sought in the accompanying Verified Petition.

Dated: April ___, 2005
New York, New York

Justin Brookman

¹² In response to the Attorney General's request for all email complaints received, Respondent has indicated that it has received approximately 27,000 user emails, an indeterminate number of which are complaints. Whatever the specific number of complaints Respondent has received, it plainly understates the number of deceived consumers, given how difficult it is for consumers to even identify when, why, how, and by whom their computers have been infected by spyware.