PUBLIC REDACTED VERSION

ABELSON | HERRON LLP
Michael Bruce Abelson (State Bar No. 130739)
Leslie A. Pereira (State Bar No. 180222)
333 South Grand Ave, Suite 650
Los Angeles, California 90071-1559
Telephone: (213) 402-1900
Facsimile: (213) 402-1901
mabelson@abelsonherron.com
lpereira@abelsonherron.com

BERGESON, LLP
Daniel J. Bergeson (State Bar No. 105439)
Hway-ling Hsu (State Bar No. 196178)
303 Almaden Boulevard, Suite 500
San Jose, California 95110-2712
Telephone: (408) 291-6200
Facsimile: (408) 297-6000
dbergeson@be-law.com
hhsu@be-law.com

Attorneys for Plaintiff
NETSCAPE COMMUNICATIONS CORP.
and AMERICA ONLINE, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA – SAN JOSE DIVISION

NETSCAPE COMMUNICATIONS CORPORATION, et al., Plaintiffs, v. FEDERAL INSURANCE COMPANY, et al., Defendants.	CASE NO. C-06-00198 JW (PVT) Case Filed: December 12, 2005 Assigned to: Hon. James Ware Courtroom: 8 **DECLARATION OF PATRICK J. CAROME IN SUPPORT OF PLAINTIFFS' CROSS-MOTION FOR PARTIAL SUMMARY JUDGMENT [WITH EXHIBITS H-J]** Date: March 26, 2007 Time: 9:00 a.m. Judge: Hon. James Ware Place: 8, 4th Floor, San Jose

DOCUMENT SUBMITTED UNDER SEAL
PUBLIC REDACTED VERSION

DECLARATION OF PATRICK J. CAROME

I, Patrick J. Carome, declare as follows:

1. I am a partner in the Washington, D. C. office of the law firm Wilmer Cutler Pickering Hale & Dorr LLP. I was lead counsel for Netscape Communications Corporation and America Online, Inc. in the following litigations: *Specht v. Netscape Communications Corp. and American Online, Inc.*, 00 CIV 4871 (S.D.N.Y.); *Weindorf v. Netscape Communications Corp. and America Online, Inc.*, No. 00 CIV 6219 (S.D.N.Y.); *Gruber v. Netscape Communications Corp. and America Online, Inc.*, No. 00 CIV 6249 (S.D.N.Y.); and *Mueller v. Netscape Communications Corp. and America Online, Inc.*, No. 00 CIV 01723 (D.D.C.)[1] (hereinafter, the "SmartDownload Actions"). I was also lead counsel for Netscape in connection with an investigation initiated by the New York Attorney General into consumer protection issues regarding its SmartDownload product (hereinafter, the "SmartDownload Investigation"). I have personal, first-hand knowledge of the matters stated herein and, if called to testify, could and would testify competently thereto.

The SmartDownload Actions

2. The SmartDownload Actions were nearly identical in their terms. All four actions alleged, among other things, that Netscape distributed a software program called SmartDownload, which allowed users to pause or resume downloads of .Zip or .Exe Files from the Internet. They alleged that Netscape and AOL violated the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*. ("ECPA"), because SmartDownload allegedly "intercepted" a user's communications by transmitting, during the course of a download and unbeknownst to the user, the URL address of the file the user was downloading, along with a string of characters called the "key," and a Netscape "cookie" (hereinafter, the "Behavioral Data").

[1] Mueller voluntarily dismissed his complaint on or about August 24, 2002.

3. The SmartDownload Actions also alleged that the same SmartDownload feature violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), by accessing a computer without or beyond the scope of authorization.

4. Throughout the course of the SmartDownload Actions, Plaintiffs pursued various legal theories, including whether the Behavioral Data allegedly intercepted by Netscape and AOL had been used for marketing purposes or had been shared with third parties. Specifically, Plaintiffs were keenly interested in whether the Behavioral Data was being collected by SmartDownload to create "profiles" of Internet users that defendants sold, shared with third parties, or otherwise used for financial advantage.

5. Plaintiffs actively touted and pursued a theory that Behavioral Data may have been directly sent by Netscape to a third-party advertising company named AdForce. To support their theory, Plaintiffs sought discovery from Netscape and repeatedly questioned Netscape regarding its dealings with AdForce. Netscape employee David Park was repeatedly questioned during deposition about whether the Behavioral Data had been sent to AdForce. Immediately following another deposition, Plaintiffs' counsel stated that he was still actively pursuing a theory that the Behavioral Data had, in fact, been shared with AdForce.

6. Plaintiffs' active pursuit of this disclosure theory was further borne-out by a Powerpoint presentation Plaintiffs made to Netscape and AOL in connection with their efforts to settle the SmartDownload Actions. Attached hereto as Exhibit H is a true and correct copy of the Plaintiffs' Powerpoint presentation. That presentation – aimed at summarizing Plaintiffs' liability case – contained an entire section entitled "Netscape Configured its Servers to Transmit SmartDownload Information to AdForce." See Ex. H at NET/SDL 00011318-24. In that section Plaintiffs' expressly stated that "SmartDownload was designed to send the Profiling information directly to AdForce, not to Netscape." Id. at NET/SDL 00011320. Moreover, the Powerpoint presentation references a document located during discovery that Plaintiffs claimed "shows direct communication between Netscape and its ad server." Id. at NET/SDL 00011321. Plaintiffs concluded this section of their presentation by stating that in early 1999, "Netscape and AdForce entered into a License Agreement that explicitly required Netscape to provide

demographic data about users of its products to AdForce in exchange for certain services from AdForce." Id. at NET/SDL 00011324.

7. Plaintiffs in the SmartDownload Actions prosecuted their claims substantially upon the basis of their theory that users' private information had been shared with advertisers. Despite Netscape's and AOL's denial (and evidence presented to the contrary), Plaintiffs doggedly pressed this theory until shortly before the actions ultimately settled.

The New York Attorney General Investigation

8. In mid-September, 2000, I was asked to assist Netscape in connection with an investigation by the New York Attorney General (NYAG) into consumer protection issues relating to its SmartDownload software. This investigation was initiated by a letter dated September 8, 2000, which detailed the subject matter of the NYAG's investigation (the "Initiation Letter"). Attached hereto as Exhibit I is a true and correct copy of the Initiation Letter.

9. The Initiation Letter stated that the NYAG's "interests" include Netscape's practices related to "data transmission, use, retention, and transfer." Ex. I at NET/SDL00010050. Indeed, the Initiation Letter expressly requested that Netscape provide, within 20 days, information that details the "[h]istory of transfers to third parties." Id. at NET/SDL00010051. Based on this, I was not surprised to learn that one of the NYAG's primary concerns was whether there had been third-party disclosure of users' information collected by SmartDownload. Although the NYAG's concern was ultimately determined to be unfounded, I spent substantial time and resources responding to the NYAG's disclosure inquiries and working to persuade him that no such disclosure had occurred.

10. Attached hereto as Exhibit J is a true and correct copy of a report prepared by @stake, the company our firm retained on behalf of Netscape to comply with the terms of the Assurance of Discontinuance executed by Netscape.

I declare under penalty of perjury of the laws of the United States of America that the foregoing is true and correct.

Executed this 11th day of January 2007 at Washington D.C.

Patrick J. Carome

EXHIBIT H

EXHIBIT FILED UNDER SEAL

EXHIBIT I

STATE OF NEW YORK
OFFICE OF THE ATTORNEY GENERAL
www.oag.state.ny.us

ELIOT SPITZER
Attorney General

DIETRICH L. SNELL
Deputy Attorney General
Division of Public Advocacy

DAVID A. STAMPLEY
Assistant Attorney General, Internet Bureau
Voice: 212-416-8332 Fax: 212-416-8369
david.stampley@oag.state.ny.us

CAITLIN J. HALLIGAN
Assistant Attorney General in Charge
Internet Bureau

Sept. 8, 2000

Paul T. Cappuccio, Esq.
Sr. Vice President and General Counsel
America Online, Inc.
22000 AOL Way
Dulles, VA 20166-9323

Re: Consumer software and background communications

Dear Mr. Cappuccio:

We are examining consumer protection issues related to background Internet communications software embedded in Netscape consumer software products and data collected by the communications software. With this letter, we are asking you to provide information relating to Netscape software, including SmartDownload.

Our interests include the availability and content of the company's notice to consumers about the communications software, the software's performance, and the company's practices relating to product installation and data transmission, use, retention, and transfer. Regarding any decisions you have made to modify or terminate use of the product, we want to learn about the availability to consumers of notice and deinstallation routines and any changes in the company's collection, use, retention, and transfer of the data.

In the requests contained in this letter:

- "Including" means "including but not limited to."
- "Communications software" means a software component residing at least in part on a consumer's PC, imbedded in or functionally linked to consumer software, and capable of transmitting data from a consumer's PC to a Web-based server.

SPM 0098

- "Consumer software" means a consumer PC software product that includes a communications software component.
- "Document" means a communication expressed in any medium, including hardcopy as well as machine-readable form such as a computer text file, pop-up message, email, digitized image, audio stream, or recorded telephone announcement. For purposes of this request, "document" does not include machine-language, object code, or source code forms computer program execution instructions.
- "Company" means the company owning or controlling the software at the time of a document's creation or receipt.

Unless otherwise indicated, the subject matter of the following requests is limited to the documents and information relating to the company's communications software.

We request that you provide all of the following within 20 days:

Documents:

1. Press releases
2. Litigation documents of record
3. Responses to non-litigation complaints received from outside the company
4. Consumer-directed documentation or notice, whether included in or separate from consumer software, and including:
   a. installation instructions
   b. descriptions of data collection, use, retention, and transfer
   c. deinstallation instructions
   d. privacy statements
5. Samples of all report types that include data communicated from any consumer's PC and reports derived from such data
6. Design, function, and implementation descriptions, whether for company or external distribution, and including those contained in manuals, marketing materials, and memoranda

Information, or reference to a provided document, that describes or identifies:

7. Past and pending legal actions
8. Past and pending government or regulatory actions and investigations
9. History of modifications to collection practices, including development and announcement of deinstallation routines and termination of data collection
10. Regarding data directly or indirectly derived from the communications software:
    a. Volume of existing data
    b. Volume of purged data
    c. Date range of collection

120 Broadway, New York, NY 10271-0332 • (212) 416-8433 • Fax (212) 416-8369

d. Form and content of data fields, including any data containing or derived from a global unique identifier (GUID) or relating to the age of the consumer
e. Form and content of metadata related to item 10(d)
f. History of analyses, reports, or other uses
g. History of data retention practices
h. History of transfers to third parties

We request that you provide all of the following within 30 days:

Documents:
11. Correspondence with state and federal entities
12. Non-litigation complaints received from outside the company controlling the software at the time
13. Correspondence with insurers
14. Correspondence with software developers and manufacturers from whom the company purchased or licensed the communications software

Information that describes or identifies:
15. History of modifications to functions that reside on user PCs
16. History of modifications to functions that do not reside on user PCs
17. History of data security practices

All documents that exist in a format interpretable by commonly available business word processing, spreadsheet, or database software should be provided in that format as well as in hardcopy format.

In addition, for all the above-requested documents and responses, please provide the documentation requested in the attachment to this letter, and in the format shown in the attachment. In transmitting this documentation to us, please send a hardcopy as well as a machine-readable table formatted for WordPerfect or Microsoft Word.

Feel free to contact me to discuss these matters.

Sincerely,

David A. Stampley
Assistant Attorney General

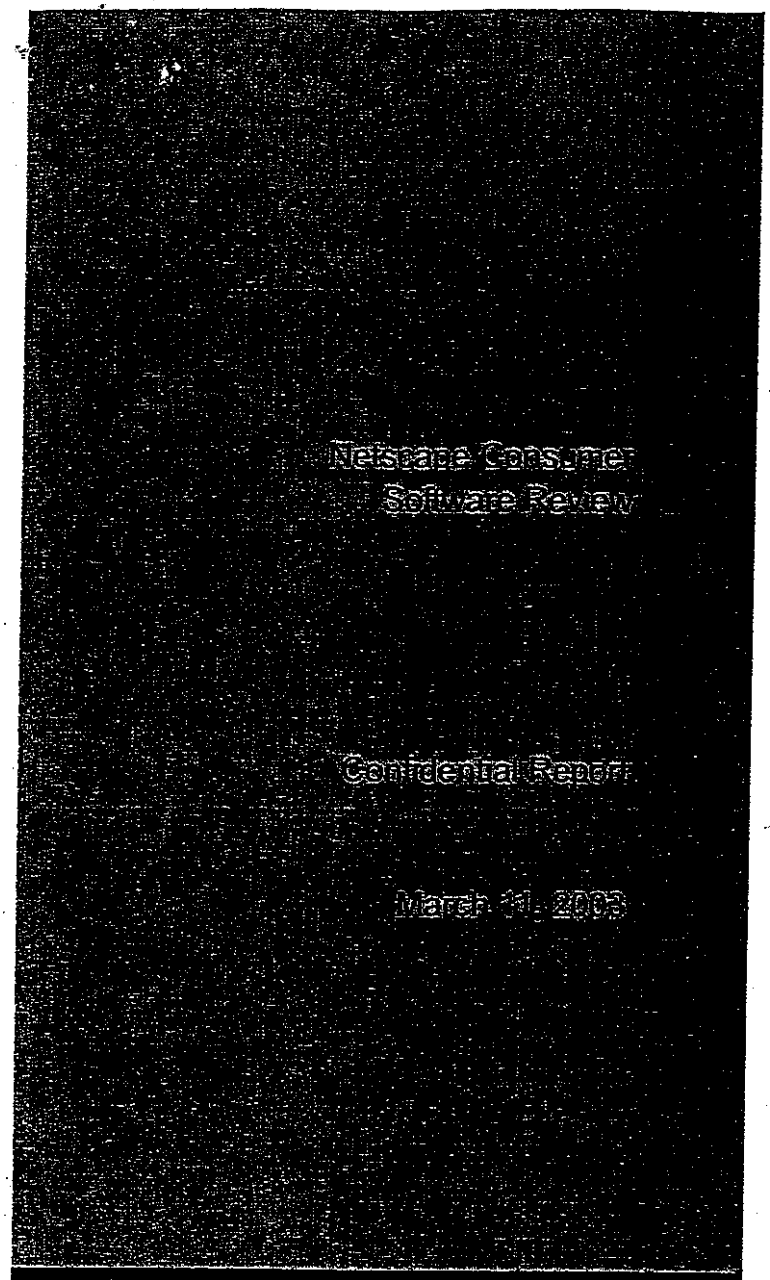
SPM 0100

Paul T. Cappuccio, Esq.
Sept. 8, 2000

Attachment

Request Number	Document ID	Document Date	Document Title	Document or Response Author	Document or Response Author's Business Unit	Document Recipient or Document Target Audience	Document or Response Effective Period	Document Means of Distribution
The item number of the requests stated above in this letter	*For a response in the form of a document, provide Bates-stamp or other unique ID, if applicable.*	*For a response in the form of a document, provide the document date.*	*For a response in the form of a document, provide the document title.*	*Identify the author of a company-created document.* *If known, identify the author of a document received from outside the company.* *For a written response to one of the requests in this letter, identify the author of the response.*	*For a document created by the company, identify the business unit of the author at the time of the document's creation.* *For a document created outside the company, identify the business unit of the company recipient at the time of the document's receipt.* *For a written response to one of the requests in this letter, identify the author's business unit.*	*For a document created by the company, identify the intended recipient or, for a document such as a user manual or Web site posting, the target audience.* *For a document created outside the company, identify the company recipient responsible for addressing the substance of the document.*	*For a document or response for which the content applies over a period of time, identify the time period. E.g., for a product warranty, identify the warranty period. For a Web site posting, identify the dates the posting appeared and the time period for the continuing validity of statements made in the posting.*	*E.g., U.S. mail, hardcopy installation instructions, email, etc.*

EXHIBIT J



mission

@stake offers comprehensive digital security consulting services for Global 2000 businesses whose success depends upon developing secure electronic relationships with customers, suppliers, partners and employees. With practice areas serving financial services, communications service providers and e-markets, @stake applies industry expertise and pioneering research to design and build strategic security solutions that enable long-term e-business objectives.

@stake

Where Security & Business Intersect℠

www.atstake.com

196 BROADWAY

CAMBRIDGE, MA 02139

MAIN: 617.621.3500

FAX: 617.621.1738

@stake

Contents

Introduction

@stake was engaged by Netscape Communications Corporation (Netscape) to perform a security assessment of Netscape's consumer software in accordance with the Assurance of Discontinuance Joint Agreement reached between Netscape and the New York Attorney General's Office dated June 16, 2003. The engagement took place between December 8, 2003 and February 13, 2004.

The scope of the assessment was broken down into two areas of investigation. The first area of investigation was an evaluation of the current Netscape product line to determine whether any of Netscape's consumer software products have any feature that transmits to Netscape uniquely identified user data reflecting user activity on web sites that are not affiliated with Netscape. In the event that @stake determined that a feature of any Netscape consumer software product or products transmits to Netscape uniquely identified user data reflecting user activity on web sites that are not affiliated with Netscape, @stake then would have determined whether any disclosures made to consumers describing the existence or operation of any such feature, or regarding Netscape's retention and/or use of any such user data, are accurate.

In the second area of investigation, @stake researched the current operation of the Netscape Network in regards to SmartDownload version 1.1 Profiling Data. In the agreement, Netscape states that profiling information is no longer recorded on Netscape servers, even if clients still send the data. Finally, the investigation attempted to identify the location and extent of any recorded profiling data that may have been obtained previous to the agreement.

Methodology and Evaluation Model

@stake downloaded the consumer software products and analyzed network traffic generated by the products to determine whether the products transmit to Netscape uniquely identified user data reflecting user activity on web sites that are not affiliated with Netscape.

@stake assessed the content and modification of local files, such as cookies, to determine whether such local files cause uniquely identified user data reflecting user activity on web sites that are not affiliated with Netscape to be transmitted to Netscape.

In order to determine how either Uniquely Identified User Data (UIUD) or data regarding Other Site Usage (OSU) may be collected by Netscape products, @stake observed the operation of the Netscape consumer suite of products and generated the following lists:

UIUD collected / created by Netscape products

1. Keycodes or other uniquely generated values based on computer configuration details that may be expected to be unique.
2. Screennames or other registration details from the Netscape Network. Cookies that are generated on Netscape servers and sent back to Netscape clients based on screennames or other registration details. User screennames can be attached to a Netscape profile.
3. Form Manager data in Navigator.
4. Password Manager data in Navigator.
5. User information in Communicator, such as e-mail address, name, and other data.

OSU collected / created by Netscape products

1. Navigator histories
2. Navigator caches
3. Cookies
4. Address books
5. Access to e-mail content
6. Links and other data stored in Netscape Composer-generated files
7. Navigator pre-fetch data
8. Registry data for non-Netscape or other products

During the evaluation of Netscape's Windows products, @stake used multiple Windows operating systems, including Windows 98, Windows 2000, and Windows XP. Mac OS 10.2 was used for the evaluation of Netscape's Macintosh products. Redhat Linux 9.0 was used for the evaluation of Netscape's Linux products. On all platforms, Netscape 7.1 software was downloaded from Netscape Network servers, and installation included both the "quick" version, where a bootstrapped installation and download took place, and a full download and installation. During installation, a user has the option to create a Netscape Network account. Test cases included the account creation as well as the rejection of account creation.

Software tested

- Netscape Navigator
- Netscape Composer
- Netscape Mail
- Instant Messenger
- Radio@Netscape
- Netscape Toolbar
- Netscape ISP (Windows only)

All of the above software, with the exception of the Netscape Toolbar and Netscape ISP (Windows only), was downloaded as part of the Netscape 7.1 package. Netscape 7.1, the Netscape Toolbar and Netscape ISP (Windows only) were downloaded from Netscape's website. The version strings submitted by the Netscape 7.1 product are as follows:

```
Windows: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4) Gecko/20030624 Netscape/7.1 (ax)

Macintosh: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.4) Gecko/20030624
Netscape/7.1

Linux: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.4) Gecko/20030624 Netscape/7.1
```

Netscape Products and Interaction with the Netscape Network

Due to the interdependency between Netscape software and the Netscape Network, it is difficult to constrain the scope of evaluation simply to Netscape products. For example, the "Search" button on the Netscape Navigator toolbar directs a user to the Netscape Network. The Netscape Network hosts user registration and maintenance, as well as search functionality, for the Netscape ISP service. Radio@Netscape and AIM are Netscape products that cannot function without the Netscape Network.

For the purposes of this evaluation, @stake evaluated network traffic between Netscape products and the Netscape Network for registration purposes, basic functionality (such as the search button on Navigator), and situations where Netscape was the exclusive provider of the service that the product utilized, such as Radio@Netscape and AIM. In these cases, network traffic between the Netscape Network and the Netscape product are considered part of the normal utilization of the Netscape product. Other interaction with the Netscape Network, such as clicking on a link or browsing content on the Netscape Network web pages, was considered to be user-initiated activity on the Netscape Network and was not evaluated.

Cookies set by the Netscape Network and affiliates were reviewed with Netscape staff to identify if any Netscape product sets the value of a cookie, rather than reflecting back cookies that were sent by the Netscape Network servers. Only one case exists where the cookie is set in order to initiate Netscape registration after installation of the Netscape Navigator software. The cookie does not contain UIUD or OSU.

Known Limitations

@stake has included a list of known or possible limitations for the sake of completeness.

Language Scope

The scope of the examination consisted of specifically the English language version of the Netscape 7.1 software for Windows, Macintosh, and Linux versions. Other localized versions of the Windows software in other versions were not tested.

SmartDownload version 1.5 Not Tested

@stake did not test SmartDownload version 1.5 as instructed by Netscape as it is not currently targeted at the U.S. mass consumer market. Only products within the Netscape 7.1 suite, the Netscape Toolbar and Netscape ISP (Windows only) were considered to be current Netscape consumer software.

Covert channels

While unlikely, it is necessary to state that it is technically possible that a covert channel could exist to collect OSU and transmit it to the Netscape Network that could not be detected without significant time and Netscape-specific knowledge of decoding personalization, cookie-formatting, session management, and other Netscape-network features and how they interact with Netscape software. Only overt stimulus to plain-text response mechanisms would be easily detected, where the stimulus is an action that generates OSU and the plain-text response is an immediate submission to Netscape. The time-bound nature of the test further decreases the likelihood of covert channel detection. @stake interviewed Netscape personnel on this issue and Netscape personnel provided no evidence that covert channels existed.

Results of Software Evaluation

While Netscape products handle data about other site usage and uniquely identified user data, the products' interaction with the Netscape Network or affiliates did not indicate transmission of either UIUD or OSU to the Netscape Network or affiliates, other than what would be expected during utilization of Netscape Network features. @stake found no transmission of UIUD combined with OSU to the Netscape Network by Netscape products during testing.

Retention of SmartDownload Profiling Data (Post-Agreement)

On January 12, 2004, an @stake consultant met with Netscape staff to review the mechanisms in place surrounding the receipt of SmartDownload version 1.1 Profiling data in current practice. Since there are active users of SmartDownload version 1.1, Netscape devised a mechanism to avoid logging the keycode and URL submissions.

The SmartDownload version 1.1 client, with profiling enabled, will send a keycode and the URL of the file being downloaded to cgi.netscape.com. The current server farm that hosts cgi.netscape.com is housed in a Netscape datacenter in Mountain View, California. It is load-balanced by a Foundry ServerIron which provides address translation and failover capability in case a single server fails. There are three servers behind the load balancer, all of which are configured in the same fashion.

Upon receipt of a web request, the Netscape server software, through a NSAPI plug-in, evaluates if the request is destined for sd_server.cgi, a CGI program that handles SmartDownload client data. The sd_server.cgi returns advertising and other application configuration parameters back to the client. A previous version of sd_server.cgi accepted the SmartDownload client data, including keycode and file downloaded, and logged it to a file. The current version, however, of the sd_server.cgi program does not contain this functionality. Default Netscape server logging would also capture the data. Netscape reported to @stake that, more than a year before it entered into the discontinuance agreement, Netscape devised and implemented the aforementioned NSAPI plug-in to programmatically remove the data from the client request before logging it to disk.

Results of Retention of SmartDownload version 1.1 Profiling Data (Post-Agreement) Evaluation

@stake reviewed the server configuration and logfiles on all three cgi.netscape.com servers to validate the configuration mentioned above. Through evaluation of the server logs, @stake was able to determine that there were SmartDownload version 1.1 users still using the system, and the keycode URL of the file downloaded were not logged to disk.

It should be noted that the review was performed during a visit with Netscape personnel, under review of Netscape's counsel. Since the hosts were in a production environment, the @stake consultant did not interact with the system, and accepted the representation by Netscape staff that the aforementioned systems were the cgi.netscape.com hosts in question. Nothing occurred during the review that would indicate that the systems in question were not the cgi.netscape.com webservers.

Storage and Retention of Previously Collected SmartDownload version 1.1 Profiling Data

@stake did not attempt to confirm the deletion of SmartDownload Profiling Data having been advised by Netscape that, in light of pending civil litigation, Netscape is subject to legal impediments regarding the deletion of such data as identified within paragraph 36 of the Assurance of Discontinuance. Additionally, in interviews Netscape staff reported that, since entering into the discontinuance agreement, Netscape has not associated the SmartDownload Profiling Data with any personally identifiable consumer data. @stake found no evidence that Netscape had either done so, or had the means to do so.

Conclusions of Review

1. With respect to paragraphs 38 (i) and (ii) of the Assurance of Discontinuance, @stake detected no feature of any Netscape Consumer Software Product that transmits to Netscape uniquely identified user data reflecting user activity on websites that are not affiliated with Netscape. Accordingly, it was unnecessary for @stake to assess the accuracy of any disclosures made by Netscape concerning the existence or operation of any such feature or the retention and/or use of any such user data.

2. With respect to paragraph 38 (iii) of the Assurance of Discontinuance:
   a. @stake confirmed that, as of the time of its review, Netscape is maintaining its server processes so as not to record URL or "keycode" parameter transmission profile data from SmartDownload version 1.1;
   b. Because @stake was informed by Netscape that Netscape is subject to legal impediments regarding the deletion of URL and "keycode" data it has received in the past, @stake did not attempt to confirm the deletion of SmartDownload profiling data;
   c. @stake detected no evidence indicating that, since entering into the Assurance of Discontinuance, Netscape had associated SmartDownload profiling data with any personally identifiable consumer data.