UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

HOME DEPOT U.S.A., INC.,
Petitioner

v.

RAVENWHITE SECURITY, INC.,
Patent Owner

Case IPR2024-01316
U.S. Patent No. 10,594,823

DECLARATION OF BERNARD J. JANSEN, PH.D.,
IN SUPPORT OF PATENT OWNER'S RESPONSE

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

RavenWhite EX2007
Home Depot v. RavenWhite
IPR2024-01316

TABLE OF CONTENTS

I. INTRODUCTION 1
II. MY BACKGROUND AND QUALIFICATIONS 2
III. LIST OF DOCUMENTS CONSIDERED 7
IV. LEGAL UNDERSTANDING 10
A. My Understanding of Claim Construction 10
B. My Understanding of Obviousness 11
C. My Understanding of a Person Having Ordinary Skill in the Art 13
V. PERSON OF ORDINARY SKILL IN THE ART 14
VI. THE '823 PATENT 14
A. Overview of the '823 Patent 14
B. Claim Construction 18
1. Browser Storage Area 18
VII. OVERVIEW OF THE GROUND REFERENCES 30
A. Hinton 30
B. Varghese 32
VIII. DR. WILLS' PROPOSED OBVIOUSNESS GROUNDS 35
A. Ground 1: Dr. Wills does not show that Hinton renders obvious any claim of the '823 patent. 35
1. Dr. Wills does not show that Hinton's e-community cookie is "caused to be stored at the client device during a second previous network session" (elements [1.b.iv] and [6.a.iv]). 35
2. Dr. Wills does not shown that storage of "a second cookie . . . during a second previous network session," as recited in elements [1.b.iv] and [6.a.iv], occurs prior to receiving the "network resource request" of elements [1.b.i] and [6.a.i]. 40
B. Grounds 2 and 3: Dr. Wills does not show that Varghese renders obvious any claim of the '823 patent. 44
1. Dr. Wills does not show that Varghese renders obvious "wherein the first cookie of the first type is stored in a first client device browser storage area and the second cookie of the second type is

stored in a second client device browser storage area different from the first client device browser storage area" (elements [1.b.v] and [6.a.v]). 44

2. Dr. Wills does not show that Varghese renders obvious "wherein a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session" (elements [1.b.iv] and [6.a.iv]). 48

IX. CONCLUSION 53

I, Bernard J. Jansen, hereby declare as follows.

I. INTRODUCTION

1. I have been retained as an expert witness on behalf of Patent Owner RavenWhite Security, Inc. ("Patent Owner") and RavenWhite Licensing LLC ("Exclusive Licensee") for the above-captioned *inter partes* review ("IPR"). I am being compensated for my time in connection with this IPR at my normal hourly rate. My compensation is not contingent on either my expert opinion or the outcome of this litigation. I have no other interest in this proceeding.

2. I understand that this declaration accompanies Patent Owner's Response filed in this IPR involving U.S. Patent No. 10,594,823 ("the '823 patent") (EX1001), which resulted from U.S. Patent Application No. 15/706,556 ("the '556 application"), filed September 15, 2017, which claims priority as a continuation application to U.S. Patent Appl. No. 11/590,083, filed October 31, 2006, and U.S. Provisional Appl. No. 60/732,025, filed November 1, 2005. I do not offer an opinion on whether the '823 patent is entitled to claim priority to U.S. Provisional Appl. No. 60/732,025. My opinions regarding the knowledge in the art at the time of the '823 patent are not dependent on the date to which the '823 patent is entitled to claim priority and would not materially differ with respect to either of the October 2006 and November 2005 dates. I refer to this general timeframe when I refer to the time of the '823 patent.

3. In preparing this declaration, I have reviewed the ’823 patent and each of the documents cited herein, in light of general knowledge in the art before the time of the ’823 patent. In formulating my opinions, I have relied upon my experience, education, and knowledge in the relevant art. In formulating my opinions, I have also considered the viewpoint of a person of ordinary skill in the art (“POSITA”) (as discussed further below in Section V) at the time of the ’823 patent.

II. MY BACKGROUND AND QUALIFICATIONS

4. My analysis is based on my experience, training, knowledge, and education, and it is formed through the application of that experience, training, knowledge, and education in the principles of search engines, Web search, keyword advertising, display advertising, online advertising, Web analytics, network communications, and related areas.

5. Since 2015, I have been a principal research scientist at the Qatar Computing Research Institute in Doha, Qatar. I was a tenure-track professor at Penn State from 2002 through 2016, departing as a tenured, full-time professor on January 1, 2017, to become a principal research scientist at the Qatar Computing Research Institute. I was a Senior Fellow at the Pew Internet & American Life Project, which is part of the Pew Research Center, from 2010 through 2012. I was a University Expert at the National Ground Intelligence Center from 2011 through

2014. Before my professorship at Penn State, I was a Lecturer in the Computer Science Program at the University of Maryland (Asian Division) for one year. Before that, I was an Assistant Professor in the Department of Electrical Engineering and Computer Science at the United States Military Academy, also known as West Point, for three years.

6. In addition to my academic credentials, my professional experience includes twenty years of practice in the U.S. military, serving in the Infantry as an enlisted soldier and then as a communications officer, upon commissioning, working primarily in a variety of information technology-related positions planning and establishing communication networks from portable ground radios to large satellite communication radios, and evaluating the performance of these networks. I also led a large multimedia team at a major U.S. Army educational facility, responsible for designing, providing, and assessing multimedia products, including the organizational website. I employed various software programs and databases for interactive products and website design for these tasks. I used these programs and others to develop interactive websites and multimedia applications, including employing analytics for the performance evaluation of these websites and applications. During this time, the team received several product awards and honors, including one award for website development, four for multimedia applications development, and one for software development.

7. I am the editor-in-chief of the international academic journal *Information Processing and Management*, a premier journal in computing science and information science, including computational science, online analytics, and social media computing. I am a former interim editor-in-chief of the *International Journal of Information Management*, a leading information systems and information management journal, and a former editor-in-chief of *Internet Research*, a top-ranked journal in the web science and business domains that examines the Internet's social, ethical, economic, and political implications.

8. I have authored more than 400 academic publications on Web searching, search engines, keyword advertising, online advertising, branding, Web analytics, social media, social networks, and related fields. My recent research focuses on online analytics, investigating the qualitative and quantitative attributes of digital content usage and social computing analytics, which investigates social behavior using algorithmic methods. I have authored, co-authored, or co-edited six books, including Web Search: Public Searching of the Web (2007), Understanding User – Web Interactions via Web Analytics (2009), Handbook of Research on Web Log Analysis (2009), Understanding Sponsored Search (2011), Data-Driven Personas (2021), and Understanding Audiences, Customers, and Users via Analytics – An Introduction to the Employment of Web, Social, and Other Types of Digital People Data (2023). In the 2024 edition of the Best Computer Science

Scientists in the World, my research was ranked 1369th worldwide. *See* EX2016.

9. My professional expertise includes search engine optimization, Web analytics, search engines, Web searching, social media, online advertising, online reputation management techniques, and related computer science and data science areas, including programming and computer networks. In my academic career, I have worked with various search engines and information searching applications to understand user information behavior on the Web and other environments. For example, as part of my Master's program in Computer Science, I designed and coded a text-based search engine, and my thesis involved the building of a tool for network performance monitoring. For my Doctorate program in Computer Science, I developed a program interface for Web search engines and implemented it on the Gigabyte search engine. I have been invited to present research at major search engine companies, including Google and Yandex, and many search marketing agencies.

10. As a computer scientist, I have engaged in and am experienced with classic computer science areas, such as programming, software development, algorithms, and networking, along with non-traditional areas, such as data analytics, keyword advertising, and online advertising. I have taught various computer science courses at the undergraduate and graduate levels, including topics such as micro-computing, programming (in various programming

languages), and the Web/Internet. I have taught a Web technology overview course (websites, mobile, social media, Web metrics, market analysis, etc.) and a graduate-level research course for professional masters students. Previously, I taught courses in keyword and display advertising where student teams engaged with small-medium-sized enterprises (SMEs) to implement online advertising campaigns. I have supervised students working with SMEs on various online advertising platforms, including Google Ads and Facebook Ads. I have experience with several online marketing platforms, including Google Ads, Facebook Ads, LinkedIn Ads, and Microsoft Advertising.

11. I have conducted research and teaching concerning search engines and websites, including search engine optimization, content creation, search engine keyword advertising, Web searching, and Web analytics. In the field of online searching, online advertising, and Web analytics, I have worked directly with real user searching data from several Web search engines. I have also analyzed Web data of traffic and other attributes from various websites and social media accounts. I have analyzed real user data of a multi-million dollar online advertising marketing campaign that spans multiple years, involving thousands of ads and key terms. I have also analyzed user referral traffic to websites and monetized this traffic via online advertising. I have developed Web analytics models and processes to analyze business goals and have used Web and online advertising

analytics data in my research and teaching.

12. I have advised government agencies and private companies in consulting and expert witness matters, including online searching, online advertising, search engines, locating relevant information, and disseminating defaming statements, among other related areas.

13. I have personal knowledge or have developed knowledge of the technologies discussed in this declaration based upon my education, training, or experience with the matters discussed herein.

14. I understand that a copy of my complete curriculum vitae has been submitted as Exhibit 2021, which includes a list of publications I have authored in the past ten years, a list of cases in which I have testified as an expert in deposition or trial in the past four years, and other details regarding my expertise and qualifications.

III. LIST OF DOCUMENTS CONSIDERED

15. I have considered the following documents listed below in addition to any other documents cited in this declaration. To the best of my knowledge, these documents are true and accurate copies of what they purport to be. An expert in the field would reasonably rely on them to formulate opinions such as those set forth in this declaration.

Paper No.	Description
1	Petition for *Inter Partes* Review of U.S. Patent No. 10,594,823
12	Institution Decision

Exhibit No.	Description
1001	U.S. Patent No. 10,594,823 ("the '823 Patent")
1002	Declaration of Dr. Craig Wills
1003	File history of U.S. Patent No. 10,594,823
1004	U.S. Patent No. 7,908,645 ("Varghese")
1005	U.S. Patent Publication No. 2003/0115267 ("Hinton")
1014	"Local Shared Objects—'Flash Cookies,'" Electronic Privacy Information Center (EPIC) (July 21, 2005) (available at https://archive.epic.org/privacy/cookies/flash.html).
1028	Adrian Ludwig, "Macromedia Flash Platform Security and Macromedia Enterprise Solutions" (Sept. 2005)
2005	Herrman, J., "What Are Flash Cookies and How Can You Stop Them?," Popular Mechanics, accessed at https://www.popularmechanics.com/technology/security/howto/a6134/what-are-flash-cookies-and-how-can-you-stop-them/ (Sept. 23, 2010)
2006	"What are Flash Cookies and how do they Work?," CookieScan, accessed at https://www.cookiescan.com/what-are-flash-cookies-how-do-they-work/
2008	"What are session cookies?," CookieYes, available at https://www.cookieyes.com/blog/session-cookies/
2010	Raymond Camden, Client-Side Data Storage, O'Reilly Media, Inc. (2016)

Exhibit No.	Description
2011	Hassan Djirdeh, "The Three Browser Storage Mechanisms," Progress Software, available at https://www.telerik.com/blogs/three-browser-storage-mechanisms
2012	Croft *et al*., "Complete Guide to Cookies and Where They're Stored," All About Cookies, available at https://allaboutcookies.org/what-is-a-cookie-file
2013	"In which location cookies are stored on the hard disk?," GeeksforGeeks, available at https://www.geeksforgeeks.org/javascript/in-which-location-cookies-are-stored-on-the-hard-disk/
2014	"How to delete cookies in Netscape," BlackRock, available at https://blackrock.tal.net/vx/lang-en-GB/mobile-1/brand-3/candidate/faq/how_to/local/8
2015	"Visual Design Evolution of Netscape Navigator," Version Museum, available at https://www.versionmuseum.com/history-of/netscape-browser
2016	"How to clean Infected Temporary Internet Files in Windows," Bitdefender, available at https://www.bitdefender.com/consumer/support/answer/2138/
2017	"Browser history logs," NXLog, available at https://docs.nxlog.co/integrate/browser-history.html
2018	"Adobe Flash Player 10 Administration Guide," Adobe Systems Incorporated (2008), available at https://web.archive.org/web/20081216032621/http://www.adobe.com/devnet/flashplayer/articles/flash_player_admin_guide.html
2019	"Flash Player Help – Local Storage settings," Adobe Systems Incorporated (2008), available at https://web.archive.org/web/20081025230757/http://www.macromedia.com/support/documentation/en/flashplayer/help/help02.html
2020	Deposition Transcript of Craig Ellis Wills, Ph.D., June 17, 2025

Exhibit No.	Description
2021	*Curriculum Vitae* of Bernard J. Jansen, Ph.D.
2022	"What Is the 127.0.0.1 IP Address?," Lifewire, available at https://www.lifewire.com/network-computer-special-ip-address-818385
2023	"Add pictures or attach files to emails in Outlook," Microsoft, available at https://support.microsoft.com/en-us/office/add-pictures-or-attach-files-to-emails-in-outlook-bdfafef5-792a-42b1-9a7b-84512d7de7fc
2024	"Send attachments with your Gmail message," Google, available at https://support.google.com/mail/answer/6584
2025	"Open & download attachments in Gmail," Google, available at https://support.google.com/mail/answer/30719
2026	"Adobe Flash Player 32.0 Administration Guide," Adobe Systems Incorporated (2020), available at https://developer.adobe.com/flash/devnet/flashplayer/articles/flash-player-admin-guide

IV. LEGAL UNDERSTANDING

A. My Understanding of Claim Construction

16. I understand that during an *inter partes* review proceeding, claims are to be construed in light of the specification as would be read by a person of ordinary skill in the relevant art at the time of the invention. I understand that claim terms are given their plain and ordinary meaning as would be understood by a person of ordinary skill in the relevant art in the context of the patent's specification and prosecution history. A claim term, however, will not receive its

ordinary meaning if the patentee acted as his or her own lexicographer and clearly set forth a definition of the claim term in the specification. In this case, the claim term will receive the definition set forth in the patent.

B. My Understanding of Obviousness

17. I understand that a patent claim is invalid if the claimed invention would have been obvious to a person of ordinary skill in the art at the time the application was filed. I understand that this means that even if all of the requirements of the claim cannot be found in a single prior-art reference that would anticipate the claim, the claim can still be invalid.

18. To obtain a patent, a claimed invention must have been, as of its priority date, nonobvious in view of the prior art in the field. I understand that a patent claim is obvious when the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art.

19. I understand that to prove that prior art or a combination of prior art renders a patent claim obvious, it is necessary to: (1) identify the particular references that, singly or in combination, render the patent claim obvious; (2) specifically identify which elements of the patent claim appear in each of the

asserted references; and (3) explain how the prior art references could have been combined in order to create the inventions claimed in the patent claim.

20. I also understand that when considering the obviousness of a patent claim, one should consider whether a teaching, suggestion, or motivation to combine the references exists so as to avoid impermissibly applying hindsight when considering the prior art. I understand this test should not be rigidly applied, but that the test can be important to avoiding such hindsight.

21. I understand that certain objective indicia can be important evidence as to whether a patent is obvious or nonobvious. Such indicia include: (1) commercial success of products covered by the patent claims; (2) a long-felt need for the invention; (3) failed attempts by others to make the invention; (4) copying of the invention by others in the field; (5) unexpected results achieved by the invention as compared to the closest prior art; (6) praise of the invention by the infringer or others in the field; (7) the taking of licenses under the patent by others; (8) expressions of surprise by experts and those skilled in the art at the making of the invention; and (9) the patentee proceeded contrary to the accepted wisdom of the prior art.

22. I also understand that "obviousness" is a legal conclusion based on the underlying factual issues of the scope and content of the prior art, the differences between the claimed invention and the prior art, the level of ordinary skill in the

pertinent art, and any objective indicia of non-obviousness. For that reason, I am not rendering a legal opinion on the ultimate legal question of obviousness. Rather, my testimony addresses the underlying facts and factual analysis that would support a legal conclusion of obviousness or non-obviousness, and when I use the term obvious, I am referring to the perspective of one of ordinary skill at the time of the ’823 patent.

C. My Understanding of a Person Having Ordinary Skill in the Art

23. I understand that a POSITA is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity.

24. I understand that the following should be considered when deciding the level of ordinary skill in the art that someone would have had at the time the claimed invention was made:

- the levels of education and experience of persons working in the field;
- the types of problems encountered in the field; and
- the sophistication of the technology.

25. My opinion below explains how a POSITA would have understood the technology described in the documents I have identified herein around the time of the ’823 patent.

26. Regardless of whether I use "I" or a "POSITA" during my technical analysis below, all of my statements and opinions are always to be understood to be based on how a POSITA would have understood or read a document at the time of the '823 patent.

V. PERSON OF ORDINARY SKILL IN THE ART

27. Based on my review of the '823 patent, it is my opinion that a POSITA at the time of the '823 patent would have had a bachelor's degree in computer science, computer engineering, electrical engineering, or a similar discipline, as well as two years of academic or industry experience in computer networking, or comparable industry experience.

VI. THE '823 PATENT

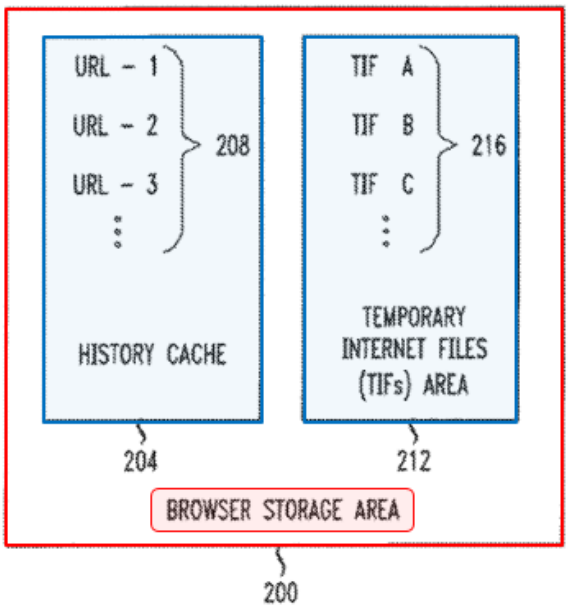
A. Overview of the '823 Patent

28. From my review of the '823 patent, the patent generally relates to "causing a browser to store information in a browser storage area of a client device" that can later be used for "identification of a user." EX1001, 1:31-34, 2:5-6. The '823 patent explains that "[a] Web page . . . may request user information from the user when the user first accesses the page, such as a user's name, password, address, interests, etc." EX1001, 1:39-42. "When the user accesses the same Web page at a later time, the server may use the information previously entered by the user to customize the Web page for the user." EX1001, 1:42-45.

29. The '823 patent further explains that "[t]his customization of a Web

page is typically the result of cookies," which are "message[s] transmitted to a browser by a server." EX1001, 1:46-48. "The message can include user-specific identifiers or personal information about the user," and "[t]he message (i.e., cookie) is then sent back to the server each time the browser requests a Web page from the server." EX1001, 1:48-52. However, "[d]espite the benefits associated with customizing a Web page, cookies also present drawbacks." EX1001, 2:11-13. "As a result, some people block or clear cookies," which results in organizations such as "banks [to] lose another technique to identify the user." EX1001, 2:24-40.

30. To circumvent issues associated with traditional cookies in the '823 patent, "one or more servers instead 'write' and 'read' a cache cookie to and from a browser storage area associated with a browser requesting a Web page from the server(s)." EX1001, 2:66-3:3. The patent describes exemplary embodiments in which "[t]he browser storage area may include a history cache and/or a Temporary Internet Files (TIFs) area." EX1001, 3:3-4. These two browser storage areas are illustrated in Figure 2.



EX1001, FIG. 2 (annotated).

31. As the '823 patent explains, the "history cache 204 [] contains Uniform Resource Locators (URLs) 208 recently visited by the browser (also called browser history)." EX1001, 6:4-8. "The first part of the URL indicates the protocol to use , and the second part specifies the IP address or the domain name (referred to below as domain) where the network resource is located." EX1001, 6:8-11.

32. "A server can 'write' any of a wide variety of cache cookies," e.g., URLs "recently visited by the browser," "in the history cache 204 to, for instance, facilitate the identification of a client device (or user)." EX1001, 6:4-8, 6:22-24. Then, "when the user revisits" a URL, "the server can 'read' the history cache 204

of the client device to determine what Web pages the browser has recently visited." EX1001, 6:42-45. "The server can use the pattern of URLs stored in the browser's history cache 204 to, e.g., identify the client device (or user)." EX1001, 6:47-49. And "[e]ven if the browser is blocking cookies (or has deleted its cookies . . .), the history cache 204 still contains the cache cookies that the server can use to identify the client device (or user)." EX1001, 6:49-53.

33. The '823 patent also explains that "[t]he browser storage area 200 can also include a Temporary Internet Files (TIFs) area 212 for storing TIFs 216," which "are files containing information embedded in Web pages." EX1001, 6:54-57. When a user returns to a URL, "[t]he server can use [a] determination (i.e., of which specific image files the browser retrieves from its local TIF area 212) to identify the browser." EX1001, 7:25-32. The patent explains that "[a]s a result, the TIFs stored in the TIF area 212 of a browser are an embodiment of cache cookies" that "persist indefinitely." EX1001, 6:64-67, 7:33-34.

34. By using "cache cookie[s]," the '823 patent addresses issues associated with traditional cookies, while still allowing websites to identify client devices. EX1001, 2:66-3:4. The cache cookies rely on native browser features, such as storage of temporary Internet files and browsing history, which obviates the need for a user to install additional applications (e.g., Flash software) on the client device. EX1001, 4:60-5:3, 6:4-8 (discussing cache cookie data that is stored

as part of the browser's native functionality).

B. Claim Construction

35. I have been informed that, absent a definition provided by the patentee, claim terms are given their plain and ordinary meaning as would have been understood by a POSITA in light of the specification and prosecution history. Therefore, I have accorded each claim term its plain and ordinary meaning, as would have been understood in the context of the '823 patent and its prosecution history, in my analysis. The plain and ordinary meaning of the claim term "*browser storage area*," in particular, is relevant to my analysis and discussed further below.

1. Browser Storage Area

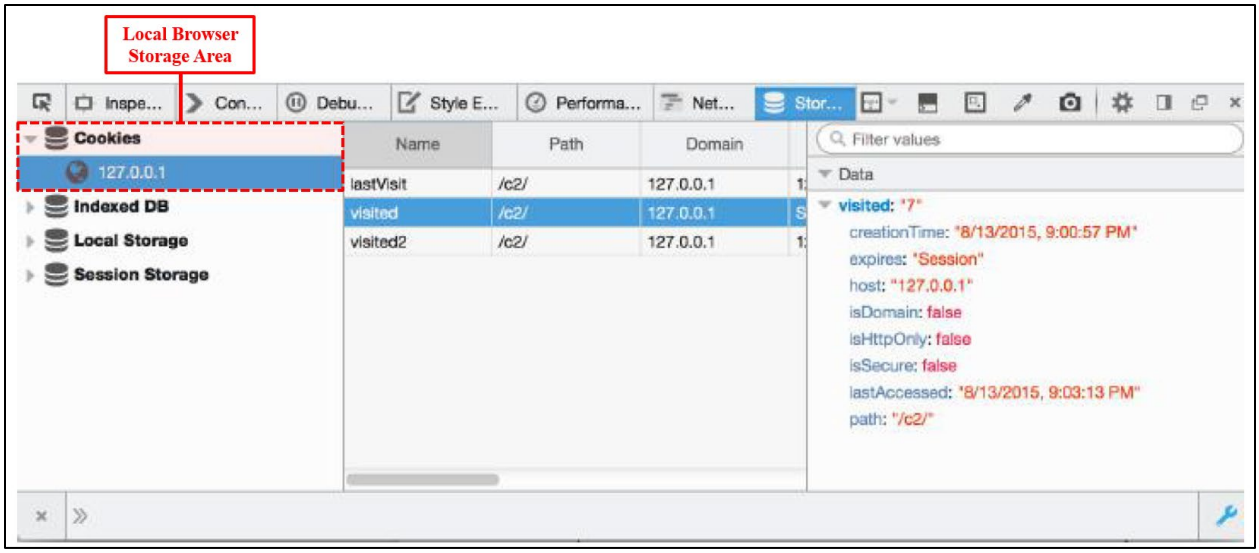
36. At the time of the '823 patent (and still today), a POSITA would have understood the term "*browser storage area*" to mean a storage area managed by and native to a browser application on the client device. As Camden explains in his book, browser applications have employed "client-side data storage" mechanisms for decades. citing EX2010, 1.[1] Rather than storing data at the server, browser applications offer "a powerful alternative—storing data on the browser itself."

[1] Citations to EX2010 reference original book page numbers (displayed at the bottom of each page).

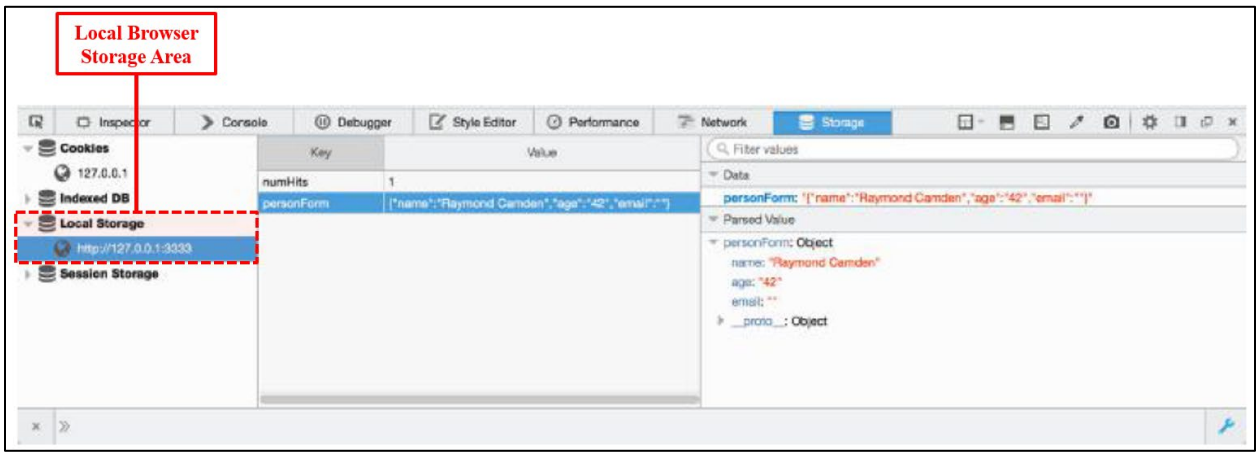
EX2010, 1. "This enables the browser to skip asking the server for information and to simply retrieve it locally from the user's machine," providing "[i]mmediate access to data." EX2010, 1.

37. Around the time of the '823 patent, one primary form of client-side data storage was cookies, which were first introduced in 1994 as part of the Netscape web browser application and are still used today. EX2010, 3. "Cookies are sent using HTTP headers, specifically the 'Cookie' HTTP header, and are sent by the browser to the server and sent to the browser from the server." EX2010, 3. Cookies can also be time constrained. For example, cookies can be set to "last for the current session," "last forever," or "expire after a particular time." EX2010, 4.

38. Cookies set by the browser application are stored in a storage area native to the browser on the user's local machine. For example, as Camden illustrates in its book, Mozilla Firefox designates storage areas on the local machine for storing cookies, as well as other local browser data, which can be viewed from within the browser application. EX2010, 10-11; *see also* EX2011 (discussing "different storage mechanisms of the web browser": "Cookies are another form of data that can be **stored in the browser**.") (emphasis added).



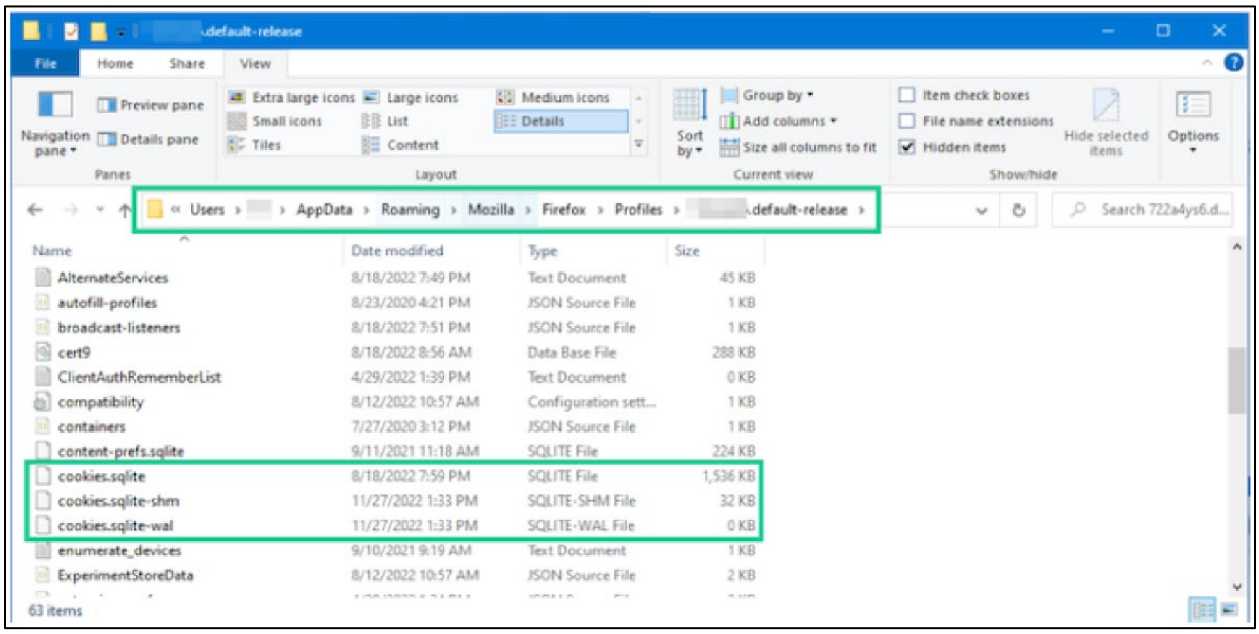
EX2010, 11 (FIG. 2-1, annotated).



EX2010, 23 (FIG. 3-6, annotated).

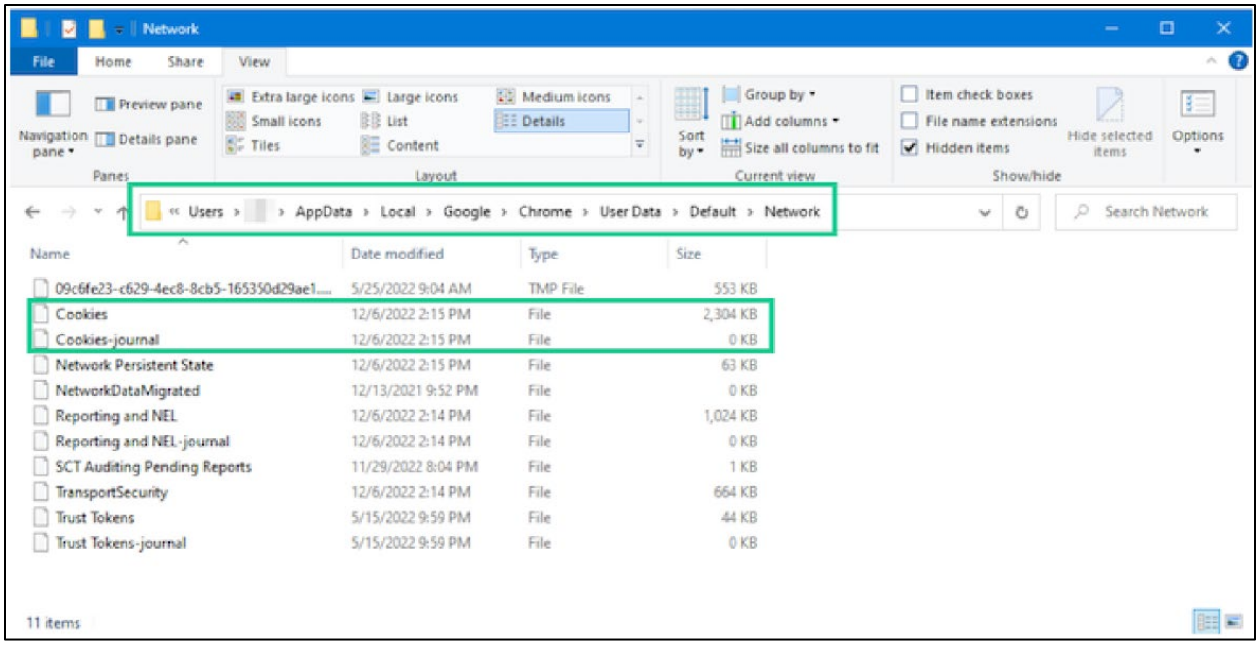
39. The storage location illustrated above corresponds to a file system folder on the user's local machine specific to the user's browser application (the IP address 127.0.0.1 is a special IP address that refers to the local computer, EX2022, 1). For example, on the Windows operating system, Mozilla Firefox typically stores this cookie data at

"C:\Users\Your_User_Name\AppData\Roaming\Mozilla\Firefox\Profiles"—a folder native to and dedicated for use by the Firefox browser application—as illustrated below. EX2012, 7. The exact Firefox file structure for the storage of the cookie data may have changed over time.



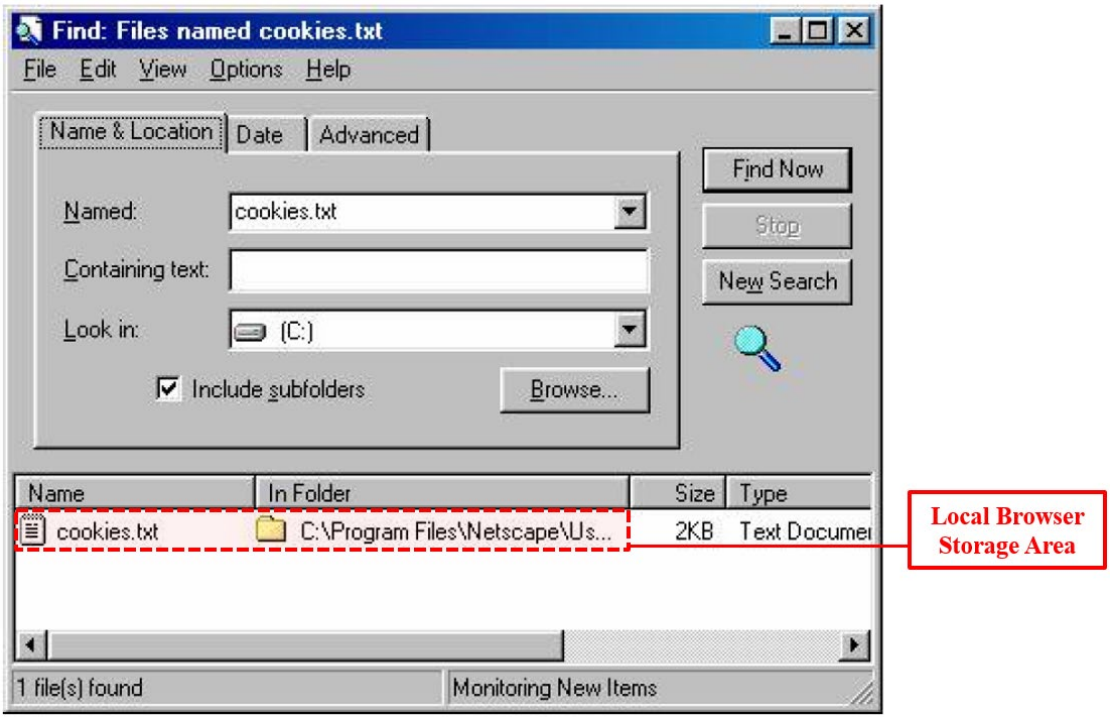
EX2012, 8.

40. Similarly, on Windows, Google Chrome typically stores cookie data at "C:\Users\Your_User_Name\AppData\Local\Google\Chrome\User Data\Default\Network"—again, a folder native to and dedicated for use by the Chrome browser application—as illustrated below. EX2012, 6; EX2013, 2. The exact Chrome file structure for the storage of the cookie data may have changed over time.



EX2012, 7.

41. This convention has remained the same since cookies were introduced as part of the Netscape Navigator browser application. For example, in Netscape Navigator version 4, introduced in 1997 (*see* EX2015, 25-26), browser cookie data was stored in a file named "cookies.txt" located within a folder native to and dedicated for use by Netscape Navigator, as illustrated below. EX2014, 3. The exact Netscape Navigator file structure for the storage of the cookie data may have changed over time.



EX2014, 3 (annotated).

42. A POSITA would have also understood that other browser data, such as Temporary Internet Files and browser history, are stored in storage areas native to the browser application. As the '823 patent explains, for example, "Temporary Internet Files (TIFs) . . . are files containing information embedded in Web pages," such as "graphics (e.g., one or more icons) (e.g., .JPG file) that are downloaded by a browser when the browser requests the Web page." EX1001, 6:54-60. "When you go to any website on the Internet, your web browser stores small pieces of data from that particular site so that pages load quicker during subsequent visits." EX2016, 2. These "files (e.g., images, text, style sheets, etc.)" are then stored in a "browser storage area (e.g., browser cache)" of the browser application. EX1001,

4:60-63; EX2016, 2 ("Windows PCs store this type of data in a cache file or a folder called 'Temporary Internet Files.'").

43. The "browser storage area (e.g., browser cache)," EX1001, 4:60-63, where TIFs are stored, corresponds to a folder on the user's local machine managed by and native to the browser application. For example, on Windows, Mozilla Firefox stores browser data such as TIFs in a browser-dedicated folder found at "C:\Users\[username]\AppData\Local\Mozilla\Firefox\Profiles\xxxxxx.default\cache," while Google Chrome stores this data in a browser-dedicated folder found at "C:\Users\[username]\AppData\Local\Google\Chrome\UserData\Default\Cache." EX2016, 1. The exact Firefox and Chrome file structures for the storage of the browser data may have changed over time.

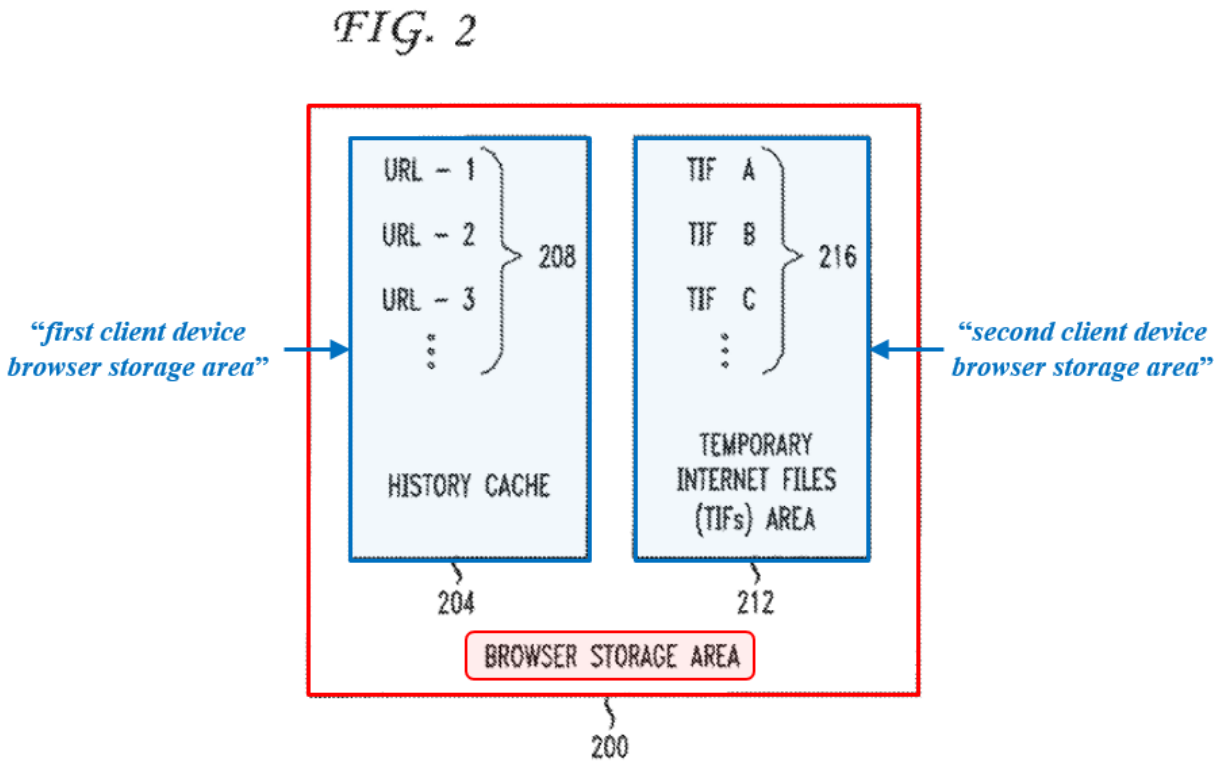
44. User browsing history also "is located in the user's profile folder" of the browser application "and the path depends on the browser and operating system." EX2017, 1. For example, on Windows, Mozilla Firefox stores browsing history in a browser-dedicated folder located at "C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<profile folder>," while Google Chrome stores this data in a browser-dedicated folder located at "C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default." EX2017, 1-2. The exact Firefox and Chrome file structures for the

storage of the browsing history data may have changed over time. A POSITA, therefore, would have understood client-side browser storage (e.g., storage areas used to store cookies, TIFs, browsing history, and other local browser data) to refer to storage areas managed by and native to a browser application, such as folders created for use by the browser application during installation.

45. The ’823 patent specification and file history are consistent with this understanding. In particular, the ’823 patent provides “a brief background of the **browser** storage area 170 and **how a browser typically uses its browser storage area** 170.” EX1001, 4:56-58 (emphasis added). As seen from this quote, the ’823 patent states that the “browser storage area” is part of (i.e., native to) the “browser” application—“how a **browser** typically uses **its browser storage area**.” EX1001, 4:56-58 (emphasis added). The ’823 patent also explains that “[w]hen a browser displays a Web page for the first time, the browser typically downloads one or more files (e.g., images, text, style sheets, etc.) to **its browser storage area (e.g., browser cache)**.” EX1001, 4:60-63 (emphasis added). “The next time the browser visits the same Web page, **the browser determines what is stored in its browser storage area** and displays the local copy of the files rather than downloading the same files again.” EX1001, 4:66-5:3 (emphasis added).

46. Example “*browser storage area[s]*” are described with respect to Figure 2 of the ’823 patent. Figure 2 illustrates “a browser storage area 200”

including "**a history cache 204** that contains Uniform Resource Locators (URLs) 208 recently visited by the browser (also called browser history)" and "**a Temporary Internet Files (TIFs) area 212** for storing TIFs 216." EX1001, 6:4-8, 6:54-56 (emphasis added); *see also* EX1001, 3:3-4 ("The browser storage area may include a history cache and/or a Temporary Internet Files (TIFs) area.").



EX1001, FIG. 2 (annotated).

47. The '823 patent explains that "the URLs written to the history cache 204 by the server" and "the TIFs stored in the TIF area 212 of a browser" are "embodiment[s] of cache cookies" stored in browser storage areas. EX1001, 6:39-41, 7:33-34. The '823 patent further explains that these browser storage areas are specifically associated with the user device's browser application: "[O]ne or more

servers [] 'write' and 'read' a cache cookie to and from **a browser storage area associated with a browser** requesting a Web page from the server(s)." EX1001, 2:66-3:3 (emphasis added).

48. From this description, it is my opinion that a POSITA would have understood that when the '823 patent refers to a "browser storage area (e.g., browser cache)," EX1001, 4:60-63, that term is referring to storage areas that are managed by and native to the browser application (in other words, storage areas that are created and dedicated for use by the browser), such as the file system folders discussed above. The '823 patent describes exactly the type of data stored in these browser application storage areas, such as "Temporary Internet Files (TIFs)" "(e.g., images, text, style sheets, etc.)" and user browsing history that act as "cache cookies" for the browser. EX1001, 4:60-63, 6:54-60, 7:33-34 ("As a result, the TIFs stored in the TIF area 212 of a browser are an embodiment of cache cookies.").

49. In my opinion, to interpret the term "*browser storage area*" to include file storage locations that are not associated with a browser application would conflict with the plain and ordinary meaning of the term. In particular, I understand that in its Institution Decision, the Board preliminarily found that "the claimed 'browser storage area' is broad in scope," and that as long as a storage area is "accessible by the user's browser," the storage area would be considered a

"*browser storage area*." DI, 51. This interpretation, however, would incorrectly encompass almost any storage area on a client device.

50. To take a simple example, web-based email programs illustrate the issue. For instance, Microsoft Outlook for the web allows users to insert attachments into emails. EX2023, 2. When a user chooses to attach a file, the browser provides the user to "[b]rowse th[e] computer" for files. EX2023, 3. The browser is then able to access any folder on the computer that the user chooses. EX2023, 3. Gmail operates similarly, allowing a user to "[c]hoose the files [they] want to upload," and allowing the browser to access files to upload as an attachment. EX2024, 1. A user can also download attachments to any folder on the user's computer, such as a download folder. EX2025, 1. If a "*browser storage area*" was simply a storage area accessible to the browser, any of the folders on a client device accessible to the browser for uploading or downloading attachments would be considered a "*browser storage area*," even though those folders are unrelated to the browser application.

51. From my review, the file history for the '823 patent is also consistent with how a POSITA would have understood the term "*browser storage area*" at the time of the '823 patent. I understand that during prosecution, the examiner relied on the publication *Local Shared Objects—"Flash Cookies*," EPIC, July 21, 2005 (EX1014 in this proceeding) "for its disclosure of flash specific cookies

stored in an area separate from traditional cookies." EX1003, 203. Quoting the Flash publication, the examiner observed that Flash cookies are (1) "set through a mechanism in Macromedia's Flash MX player" and (2) "stored in a special directory depending on the operating system on the client machine," which for Windows is "C:\Documents and Settings\[username]\Application Data\Macromedia\Flash Player," for Macintosh OSX is "/Users/[username]/Library/Preferences/Macromedia/Flash Player," and for GNU-Linux is "~/.macromedia)." EX1003, 217.

52. Those directories are not native to or managed by the browser. They do not exist until the Flash Player software is installed on the client device. *See* EX2018, 12 (showing storage locations of "[s]hared object files" in folders created as part of Flash Player software installation); EX2026, 6 (showing the same); EX1014, 2 (showing the same). Moreover, as Adobe's Flash Player Administration Guide explained around the time of the patent, those directories are given "a randomly generated name for security purposes," such that "users of other applications outside Flash Player, such as a web browser, cannot use those applications to access the data." EX2018, 12. To differentiate from these directories residing outside of browser storage, I understand that the applicant subsequently amended the independent claims to make clear that the claimed first and second storage areas are "*browser* storage areas." EX1003, 346, 348.

53. Therefore, consistent with the ’823 patent and file history, it is my opinion that a POSITA would have understood “*browser storage area*” to mean a storage area managed by and native to a browser application on the client device.

VII. OVERVIEW OF THE GROUND REFERENCES

54. I understand that Petitioner’s expert, Dr. Wills, relies on two references in his proposed obviousness grounds challenging the claims of the ’823 patent: Hinton (EX1005) and Varghese (EX1004). I provide brief overviews of these references below.

A. Hinton

55. Hinton is a U.S. patent application publication directed to “cross-domain log on technologies and technologies which create and manage virtual communities of online users.” EX1005, ¶7. Hinton explains that “[e]ach Internet user is served by a ‘home domain’, which is a domain in which a user is ‘registered.’” EX1005, ¶9. “[T]he home domain itself may have ‘long term’ relationships with other domains,” such as “e-community domains, where one domain (e.g. the home domain) is responsible for user registration issues.” EX1005, ¶10.

56. As Hinton explains, “[o]ften, a user will access resources in different (‘participating’) domains on behalf of their home domain,” and “the user will have to resubmit to a log in or authentication process as he or she moves from the home

domain to another domain." EX1005, ¶11. Moreover, in previous systems, a user could "only transfer to a participating domain directly from the user's home domain, and not across from one participating domain to another participating domain." EX1005, ¶13. Hinton sought to address these issues through "a cross-domain single-sign-on system and method which allows an Internet user to establish a long-term relationship with participating domains, and which gives the user the ability to go directly to participating domains, via bookmarks or direct URL's for example, without having to go through a home domain first." EX1005, ¶15.

57. Hinton's process requires users to enroll into an "e-community." EX1005, ¶70. "As a result of enrollment into the e-community, a user will have a 'domain identity cookie' ('DIDC') established by each of the participating e-community domains," which provides for "single-sign-on functionality." *Id.* After the DIDC has been established, "[i]f a user requests a protected resource in another domain, then authentication information must be transferred across the e-community." EX1005, ¶129. The DIDC allows the user's home domain to "vouch[] for a user's identity," and "[a]s a result of authentication, the SSO plug-in generates an 'e-Community Cookie' (an eCC or e-community cookie)." EX1005, ¶¶130, 136.

58. Hinton explains that "a user has one e-community cookie set for each

domain at which it has a current, authenticated (or vouched-for) session." EX1005, ¶132. In other words, the eCC is "a domain-wide e-community" that allows users to access resources across that particular domain. EX1005, ¶134. The eCC is a session cookie, meaning it "is valid for only for [sic] the duration of a browser session, and it is expired when a user invokes logout functionality." EX1005, ¶249. That is, Hinton's eCC is established and valid only within a user's current network session—it is never reused in a subsequent session. EX1005, ¶249.

B. Varghese

59. Varghese is a U.S. patent directed to "providing protection against identity theft over a computer network." EX1004, 1:16-18. Varghese's describes that its "invention includes secure cookies, flash objects and other technologies to recognize and to fingerprint [] from which device a user access an application, whether it is a computer, laptop, mobile device or any other." EX1004, 5:64-67. Varghese explains that "[t]hese user devices thus become additional authentication factors without requiring any change in user behavior" and "[i]nformation concerning these user devices is fingerprinted and stored into a device token or device id for one-time use." EX1004, 5:67-6:4.

60. Figure 4A of Varghese, produced below, illustrates "exemplary embodiments of the device fingerprinting process 400 of the system and method of the present invention." EX1004, 24:33-35.

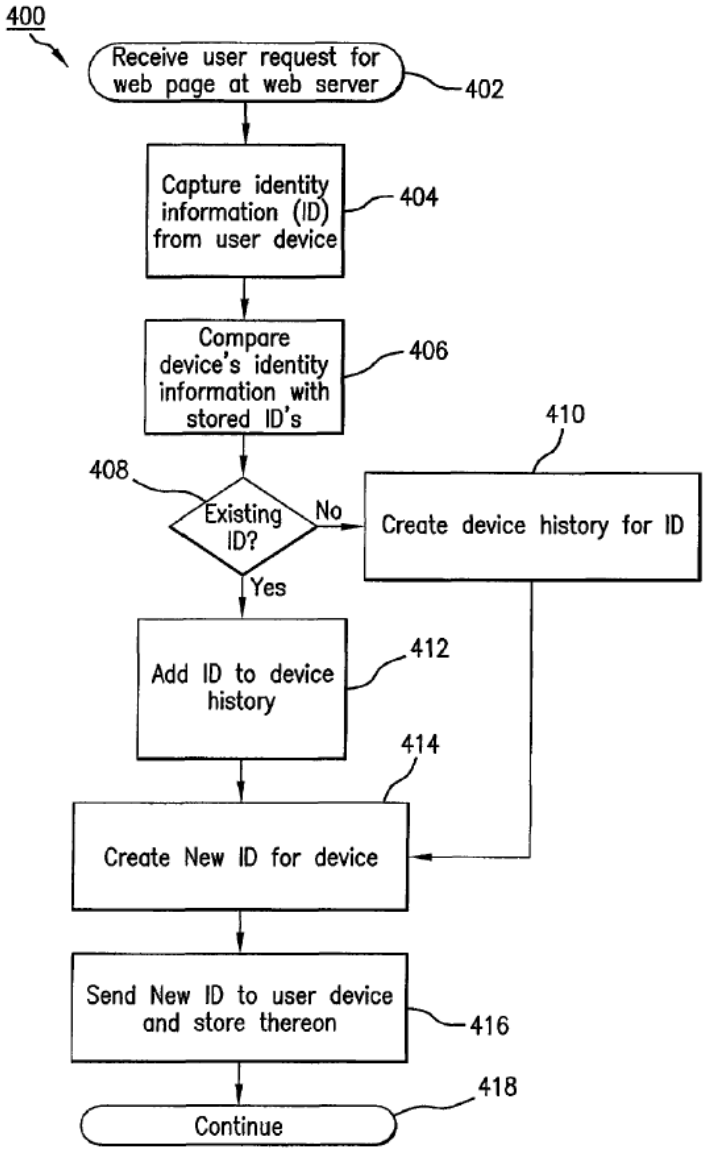


FIG.4A

EX1004, FIG. 4A.

61. Varghese describes that "[i]n Step 402, a request is received at a service provider server from a user device." EX1004, 24:40-42. "The fingerprinting process is invoked and information describing the request is transferred." EX1004, 24:42-44. Then, "[i]n Step 404, device identity information

for the user device is captured . . . by a client program already resident on the user device," such as "a web browser." EX1004, 24:50-53.

62. The device information captured in Varghese's process can be stored in the form of "cookies." EX1004, 25:7-42. "One such technique is known as 'secure cookies,'" which is "a data packet sent by a web server to a web browser for saving to a file on the host machine," and that "has been secured against modification or tampering." EX1004, 25:22-32. "Another such technique is known as 'flash cookies.'" EX1004, 25:33. Varghese explains that "Graphical software applications and/or plug-ins from Macromedia, and generally identified by the trade name 'Flash', are currently resident on many user devices." EX1004, 25:34-36. In the case of flash cookies, "Flash" "software can create local shared objects, known as 'flash cookies', for maintaining locally persistent data on a user's device akin to the standard 'cookies' stored by web browsers." EX1004, 25:34-43.

63. Because flash cookies are stored outside of browser storage in a "special directory" on the client device that is associated with "Flash" software, EX1014, 2, Varghese explains that they "have the advantage [of] not being as easily removed from the user's device as are standard cookies," EX1004, 25:40-43. One downside of flash cookies, however, is that the end-user is required to install and maintain additional software (Flash software) aside from the browser application on the host machine. *See* EX1004, 25:34-36 (requiring installation of

"software applications and/or plug-ins from Macromedia" for use of "flash cookies"); EX1014, 2 (installation of Macromedia "Flash Player" software required for use of flash cookies); EX2006, 3-4.

VIII. DR. WILLS' PROPOSED OBVIOUSNESS GROUNDS

64. I understand that Dr. Wills has provided a table of claims in his declaration with claim element labels. EX1002, pp. xiii-xv. I refer to these claim element labels in my analysis below. At times, I focus my analysis on the elements of independent claim 1, but my analysis applies equally to the corresponding elements of independent claim 6.

A. Ground 1: Dr. Wills does not show that Hinton renders obvious any claim of the '823 patent.

1. Dr. Wills does not show that Hinton's e-community cookie is "caused to be stored at the client device during a second previous network session" (elements [1.b.iv] and [6.a.iv]).

65. Each of independent claims 1 and 6 recites, "*a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session*." EX1001, 15:47-50, 16:41-44 (emphasis added). Dr. Wills asserts that Hinton's "domain identity cookie (DIDC)" is the recited "*first cookie*" of the independent claims, and that Hinton's e-community cookie ("eCC") is the recited "*second cookie*." EX1002, ¶¶84, 89.

66. In his analysis, Dr. Wills explains that "the eCC cookie is a session cookie type that is a different type of cookie from the DIDC cookie of the

persistent cookie type," and "[d]uring a session subsequent to the session that created the DIDC, when a user requests access to an affiliated domain, the affiliated domain generates an eCC for that domain and causes the eCC cookie to be stored at the user's device by sending the eCC cookie to the user." EX1002, ¶¶92-93. From this, Dr. Wills concludes that "Hinton's system discloses saving the eCC cookie in a different session than the DIDC cookie." Pet., 19 (emphasis added)." Dr. Wills, however, does not explain how establishment of the eCC occurs in a "***previous*** *network session*," as required by independent claims 1 and 6. EX1002, ¶¶89-93.

67. Dr. Wills' omission is for good reason. In my opinion, Hinton does not teach that the eCC is established in a "***previous*** *network session*" because Hinton's e-community cookie is a session cookie that is generated and valid only during a *current* network session—not a "*previous*" session. EX1005, ¶¶134, 249 ("An eCC is valid for only for the duration of a browser session, and it is expired when a user invokes logout functionality.").

68. Specifically, Hinton's system "allows an Internet user to transfer directly to a domain that is participating in the e-community, by means such as a Bookmark or a directly-typed URL, without the necessity of returning to a home domain prior to transferring to the participating domain." EX1005, ¶23. "As a result of enrollment into the e-community, a user will have a 'domain identity

cookie' ('DIDC') established by each of the participating e-community domains," which provides for "single-sign-on functionality." EX1005, ¶70.

69. After the DIDC is established for a user, "[i]f a user requests a protected resource in another domain, then authentication information must be transferred across the e-community." EX1005, ¶129. Dr. Wills alleges that "[d]uring a session subsequent to the session that created the DIDC, when a user requests access to an affiliated domain, the affiliated domain generates an eCC for that domain and causes the eCC cookie to be stored at the user's device by sending the eCC cookie to the user." EX1002, ¶93 (citing EX1005, ¶137). But Dr. Wills' analysis does not address the term "*previous*" in the claims.

70. As Dr. Wills acknowledges, "the eCC is a **session cookie**," EX1002, ¶92, which is valid only during the current network session, while the session is active. EX2008, 1 (explaining that "[s]ession cookies are cookies that last for a session," ending "when you leave the website or close your browser window."). As Hinton states, "a user has one e-community cookie set for each domain at which it has **a current, authenticated (or vouched-for) session**." EX1005, ¶132 (emphasis added). The "eCC is valid for only for [sic] the duration of a browser session, and **it is expired** when a user invokes logout functionality." EX1005, ¶249 (emphasis added). Because the eCC is valid only for the user's *current* network session and expires when the session is terminated (e.g., the user leaves the website or closes

the browser window), the eCC is not "*caused to be stored at the client device during a second **previous** network session*," as recited in the independent claims. EX1001, 15:47-50, 16:41-44 (emphasis added). That is, by definition, Hinton's eCC cannot be stored and used in subsequent sessions; it is merely used to provide access to different resources within a domain during the session in which the eCC is set.

71. Dr. Wills' analysis with respect to element [1.e], which addresses use of the eCC after it is established, still does not show that the eCC "*was caused to be stored at the client device during a second **previous** network session*," as the claims require. For example, Dr. Wills asserts, "When the user requests access to one of the servers in the domain that created the eCC, that server checks whether the user has an eCC to access the DNS domain," and "[i]f present, this would indicate that the user has a session with a different front-end within the associated domain (106)." EX1002, ¶106 (citing EX1005, ¶154). Hinton, however, does not create a *new* session when it checks for the eCC. Instead, Hinton explains that generation of the eCC for a domain establishes "**a single session**" for the domain, "such that the user can engage in e-community actions." EX1005, ¶126 (emphasis added). That is, a user is provided access to any server within the domain when it has a "current, authenticated (or vouched-for) session" for that domain. EX1005, ¶132 ("a user has one e-community cookie set **for each domain at which it has a**

current, authenticated (or vouched-for) session") (emphasis added).

72. This operation is illustrated in one of Hinton's examples in which a user is accessing the website "www.acme.com." EX1005, ¶134. Hinton explains:

> As an example, consider a hypothetical site "www.acme.com" that is partitioned so that there is a distinct security policy server set of replicas protecting each of the engineering, accounting, and human resource departments. In this situation, if a user authenticates (or is vouched for) first to engineering, **they will have a domain-wide e-community cookie set** by the engineering security policy server. **When this user then goes to the accounting server, this e-community cookie indicates that the user has a current, authenticated session, and that the accounting server need not re-authenticate the user**.

EX1005, ¶134 (emphasis added).

73. As seen in the example above, because the user already "has a current, authenticated session" with the domain (as indicated by the eCC) when it attempts to access the domain's accounting server, the user is given access without the need to re-authenticate or establish a new session. EX1005, ¶134. I understand that Dr. Wills confirmed this operation during his deposition, explaining that "by setting an E-community cookie for a domain," the user "has a current authenticated session" "[c]orresponding to the domain." EX2020, 110:3-11. In the "acme" example discussed above, Dr. Wills stated that "[t]he user has a domain-wide E-community cookie set," and "because the user already has an active session with the domain,

the user can use that session to access the accounting server." EX2020, 112:13-113:9.

74. I agree with Dr. Wills—in Hinton, a single session is used across a domain, e.g., the entire acme.com website, allowing access to resources (e.g., servers) within the domain as part of the same session. This understanding is consistent with the ordinary meaning of a session cookie, which corresponds to a session for a particular website and expires only when the user leaves the website or closes the browser window. EX2008, 1. Therefore, it is my opinion that Hinton's eCC is not "*caused to be stored at the client device during a second* ***previous*** *network session*" because subsequent access requests involving the eCC occur as part of the *same* session in which the eCC was established.

2. Dr. Wills does not shown that storage of "a second cookie . . . during a second previous network session," as recited in elements [1.b.iv] and [6.a.iv], occurs prior to receiving the "network resource request" of elements [1.b.i] and [6.a.i].

75. In my opinion, Dr. Wills' analysis with respect to Hinton fails for an additional reason. Specifically, independent claims 1 and 6 not only require that "*a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session*," as discussed above. They also require that the recited storage of the "*second cookie . . . during a second previous network session*," as recited in elements [1.b.iv] and [6.a.iv], have occurred before "*receiv[ing] a network resource request from a client device*," as

recited in elements [1.b.i] and [6.a.i]. EX1001, 15:35-54, 16:30-49.

76. First, independent claims 1 and 6 recite the step of "*receiv[ing] a network resource request from a client device, wherein the network resource request corresponds to a first cookie of a first type that* ***was caused to be stored*** *to the client device during a first previous network session*." EX1001, 15:35-39, 16:30-34 (emphasis added). I note that this element uses past tense to indicate that the "*first cookie*" was stored during the "*first … network session*." It also recites that the "*first … network session*" is "*previous*," indicating that the session occurred before receipt of the "*network resource request*." A skilled artisan, therefore, would have understood the claims to require that "*a first cookie of a first type [] was caused to be stored to the client device during a first previous network session*" before "*receiv[ing] a network resource request from a client device*." EX1001, 15:35-39, 16:30-34.

77. Within the same indented paragraph, the claims further recite (using past tense) "*wherein a second cookie of a second type different from the first type* ***was caused to be stored*** *at the client device during a second previous network session*." EX1001, 15:47-50, 16:41-44 (emphasis added). Following the same logic as above, a skilled artisan would have understood the claims to also require that "*a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session*" before "*receiv[ing]*

a network resource request from a client device." EX1001, 15:47-50, 16:41-44. I understand that Dr. Wills agreed with this interpretation of the claims. EX2020, 73:5-74:18. In my opinion, Dr. Wills has not shown that Hinton teaches these elements of independent claims 1 and 6.

78. For the recited "*network resource request*" of element [1.b.i], Dr. Wills asserts, "Hinton's **affiliated domain receives a 'vouch-for' request from user 100 to access contents of its domain**, which a POSITA would have understood to be a network resource request." EX1002, ¶84 (citing EX1005, ¶137) (emphasis added). As Hinton explains, that request "includ[ing] a domain identity cookie (DIDC) but not an e-community cookie," EX1005, ¶137, results in generation of an eCC for that domain: A "domain that authenticates the user or first receives an authentication 'vouch-for' message sets an e-community cookie at the user's browser." EX1005, ¶132. Dr. Wills then refers to this same request, citing the same paragraph of Hinton, to meet element [1.b.iv]: "During a session subsequent to the session that created the DIDC, when a user **requests access to an affiliated domain**, the affiliated domain generates an eCC for that domain and causes the eCC cookie to be stored at the user's device by sending the eCC cookie to the user." EX1002, ¶93 (citing EX1005, ¶137) (emphasis added).

79. In simple terms, Dr. Wills asserts that the same request (i.e., a request to access the affiliated domain before an eCC has been set for that domain)

satisfies both claim elements [1.b.i] and [1.b.iv]. Because Dr. Wills relies on the *same* request for each of these elements, however, he does not establish that Hinton teaches "*a second cookie of a second type different from the first type was caused to be stored at the client device during a second previous network session*" before "*receiv[ing] a network resource request from a client device*," as the independent claims require.

80. I understand that during deposition, Dr. Wills attempted to change his opinions, asserting that the request relied on for element [1.b.i] relates to a different affiliated domain than the affiliated domain relied on for element [1.b.iv]. Although I do not see this theory in Dr. Wills' declaration, that theory would still not satisfy the claim language, in my opinion. In particular, assuming a user proceeded to a second affiliated domain after an e-community cookie was set for a first affiliated domain, Hinton would simply repeat its process for that domain, issuing another e-community cookie corresponding to the second domain. That, however, does not affect the user's active "current, authenticated session" with the first affiliated domain, which is unrelated to the second affiliated domain. EX1005, ¶134 (discussing "domain-wide e-community cookie[s]").

81. As both sessions would be current, neither would have occurred prior to the other. This understanding is consistent with the description in the '823 patent, for example describing "**end[ing] the first network session**" before "a

second network session" can be initiated. EX1001, 5:10-32 (emphasis added). In other words, a session does not become a previous session until it is terminated—If both sessions were simultaneously active, neither would have occurred (i.e., began and ended) before the other. Therefore, it is my opinion that this theory still does not meet the claim requirements.

B. Grounds 2 and 3: Dr. Wills does not show that Varghese renders obvious any claim of the '823 patent.

1. Dr. Wills does not show that Varghese renders obvious "wherein the first cookie of the first type is stored in a first client device browser storage area and the second cookie of the second type is stored in a second client device browser storage area different from the first client device browser storage area" (elements [1.b.v] and [6.a.v]).

82. Each independent claim recites two storage areas that are specific to the client device browser: "*a first client device* ***browser storage area***" and "*a second client device* ***browser storage area***." EX1001, 15:50-54, 16:44-49. In my opinion, Dr. Wills does not establish that Varghese teaches this element because Varghese's "flash cookie"—which Dr. Wills relies on for the claimed "*second cookie*," EX1002, ¶165—is not stored in a "*browser storage area*."

83. Dr. Wills asserts that "Varghese discloses the use of two cookies – secure cookies and flash cookies." EX1002, ¶143. Petitioner equates Varghese's "secure cookie" to the recited "*first cookie*" and Varghese's "flash cookie" to the recited "*second cookie*." EX1002, ¶¶157, 165. Varghese's flash cookies, however,

are not stored in a "***browser*** *storage area*," as required by the independent claims.

84. As I discuss above, a POSITA would have understood the claimed "*browser storage area*" to refer to a storage area managed by and native to a browser application on the client device. *See* Section VI.B.1. Varghese's flash cookies are not stored in a storage area managed by and native to any browser application on the client device. As Dr. Wills notes, "[s]ecure cookies are standard cookies known to be saved by the Web browser in browser-maintained files," but, "**[i]n contrast, Flash cookies are stored in a separate storage area**." EX1002, ¶168 (emphasis added). Dr. Wills further explains that flash cookies not stored in local browser storage but instead "are stored on the client machine as Local Shared Objects: 'Windows C:\Documents and Settings\[username]\Application Data\Macromedia\Flash Player; Macintosh OSX /Users/[username]/Library/Preferences/Macromedia/Flash Player; GNU-Linux~/.macromedia.'" EX1002, ¶168 (citing EX1014, 2).

85. Indeed, Varghese's flash cookies are stored in a "special directory" on the user's hard disk that is associated with Macromedia Flash Player software—not with the user's Web browser. EX1014, 2; EX2005, 1 ("**Instead of using the browser's local storage system**, though, **it has its own**.") (emphasis added). The directory storing flash cookies is not managed by or native to the client's browser application. As Adobe's Flash Player Administration Guide explained around the

time of the patent, "[s]hared object files are used by Flash Player to store data locally. For example, a developer may create a game application that stores information on high scores." EX2018, 12. The document further explains that "[s]hared objects are stored in a directory with a randomly generated name for security purposes." EX2018, 12.

86. Importantly, the Flash Player Administration Guide explains that "Flash Player remembers how to direct a SWF file to the appropriate location, but **users of other applications outside Flash Player, such as a web browser, cannot use those applications to access the data**," which "ensures that the data is used only for its intended purpose." EX2018, 12; *see also* EX2019, 2 ("**[T]he information stored by Flash Player is not the same as a cookie; it is used only by the application that runs in Flash Player**, and has no relation to any other Internet privacy or security settings you may have set in your browser.") (emphasis added); EX1028 ("Flash Player runs content inside a virtual machine that implements a security sandbox. Within this sandbox, all Flash Player resources (applications, data, network URLs, and so on) are essentially isolated from the rest of the computing environment."). This limitation of access to Flash Player's shared objects has been present in versions the Flash Player software from the time of the '823 patent until its end of life. *See* EX2026, 6 (explaining the same limitation in the Adobe Flash Player 32.0 Administration Guide from 2020). Therefore, a

POSITA would have understood that not only are flash cookies stored in a folder not managed by the client's browser application, but they are also not even accessible to the browser application—only by the Flash software.

87. As Dr. Wills' own evidence confirms, this is why "Flash cookies are set through a mechanism in Macromedia's Flash MX player" and stored in a "special directory" defined by the Flash software's installation—*not* by the browser application. EX1014, 1. Therefore, it is my opinion that the folder where Flash cookies are stored is not a "*browser storage area*" because it is not managed by or native to a browser application. It is instead independently managed by and native to the Flash software installed on the client device. EX1014, 1-2.

88. Additionally, I do not see any reason why a POSITA would have sought to store Varghese's flash cookies in a "*browser storage area*," nor does Dr. Wills provide one. EX1002, ¶168. Varghese explains that because flash cookies are not stored in a "*browser storage area*," they "have the advantage [of] not being as easily removed from the user's device as are standard cookies." EX1004, 25:40-43. In other words, flash cookies are specifically designed to persist *outside* of browser storage. *See* EX2019, 2 ("[E]ven if you have specified in your browser settings that you do not want cookies placed on your computer, . . . the information stored by Flash Player is not the same as a cookie; **it is used only by the application that runs in Flash Player, and has no relation to any other**

Internet privacy or security settings you may have set in your browser.") (emphasis added); EX2006, 2 ("[**B]uilt-in browser controls** over standard cookies **don't apply to Flash cookies**.") (emphasis added), 3 ("**Because these cookies are stored outside the browser** you cannot protect yourself by using a different browser.") (emphasis added).

89. On the other hand, the '823 patent's use of browser storage areas provides an advantage over flash cookies by using native browser features. For example, the cache cookies provided by the '823 patent do not require end-users to separately install and maintain Flash software on their host machines. EX1004, 25:34-37; EX1014, 2; EX2006, 3-4. These cache cookies also do not rely on an additional third party to continue supporting Flash software in order to use flash cookies. EX1004, 25:34-37; EX1014, 2; EX2006, 3-4.

90. Therefore, a POSITA would have understood that storing Varghese's flash cookies in a "*browser storage area*" would not only conflict with Varghese's teaching but also with the purpose of flash cookies. For these reasons, it is my opinion that a POSITA would not have been motivated to store flash cookies in a "*browser storage area*."

2. Dr. Wills does not show that Varghese renders obvious "wherein a second cookie of a second type different from the first type was caused to be stored at the client device during

a second previous network session" (elements [1.b.iv] and [6.a.iv]).

91. Each of independent claims 1 and 6 also requires that the "*first cookie . . . was caused to be stored to the client device during a* ***first previous network session***," and the "*second cookie . . . was caused to be stored at the client device during a* ***second previous network session***." EX1001, 15:36-50, 16:31-44 (emphasis added). As I noted previously, Dr. Wills equates Varghese's "secure cookie" to the recited "*first cookie*" and Varghese's "flash cookie" to the recited "*second cookie*." EX1002, ¶¶157, 165. Dr Wills, however, does not show that Varghese teaches storing these cookies during two different "*previous network session[s]*," as recited in the independent claims.

92. To satisfy these claim elements, Dr. Wills asserts that Varghese "discloses that secure cookies can be removed from the browser's memory when the user clears the browser's cookies," and "that the cookies are routinely replaced with each login (*i.e.*, new network session)." EX1002, ¶166 (citing EX1004, 26:13-14). Dr. Wills then concludes, "[t]hus, in my opinion, a POSITA would have understood and found obvious that Varghese discloses a scenario in which the flash cookie was created and stored in a different (*i.e.*, second) previous network session than the secure cookie (e.g., the user cleared the browser's cookies)." EX1002, ¶166.

93. I do not see any support for Dr. Wills' assertions or hypothetical

scenario in Varghese. The passage of Varghese relied on by Dr. Wills actually indicates that *both* secure cookies and flash cookies would be replaced upon each login (not just one or the other), regardless of whether a user cleared the browser's secure cookies. EX1004, 26:12-28.

94. Specifically, as part of Varghese's "device fingerprinting process," Varghese explains that "a new Device ID token is created for the device," which is "sent to the user device and stored thereon, e.g., **as a standard cookie or as a flash cookie**." EX1004, 24:33-35, 26:4-11 (emphasis added). Varghese explains that both secure cookies and flash cookies are used for the same purpose of identifying a user device. EX1004, 24:23-27. Then, referring to these cookies, Varghese further explains that "[a] feature of the invention relates to the **replacement of the cookie on the user's machine upon each login**" so that "stolen fingerprints, tokens, or device ids cannot be fraudulently reused." *Id.*, 26:13-29 (emphasis added). In other words, Varghese discloses replacing cookies, including *both* secure cookies and flash cookies, upon each login.

95. Varghese further explains the purpose of replacing these cookies upon each login: "**This provides further security** so that even if a user's machine information is improperly acquired by a third party, **even including that embodied in a previous cookie, the authentication system can identify that the user is not authorized and deny access to the system**." EX1004, 26:14-19. That

is, regardless of the type of cookie (e.g., secure cookie or flash cookie), Varghese's techniques are designed to prevent unauthorized users by replacing the content of each cookie upon each login. If one of the previous cookies were not replaced, that would leave open a vulnerability in the case that the previous cookie was "improperly acquired by a third party." EX1004, 26:14-19.

96. Dr. Wills also points to Varghese's Table 8 as "showing various scenarios in which one of secure cookie present or flash cookie present." EX1002, ¶166. Although Varghese's Table 8 does provide an example scenario in which a flash cookie is present and a secure cookie is missing, Table 8 merely relates to how security decisions are made based on the existence of certain data, such as when a flash cookie exists but a secure cookie does not. EX1004, 19:55-20:10, Table 8. Nowhere does Varghese teach that a secure cookie or flash cookie is created upon performing a security check if it does not exist. EX1004, 19:55-20:10. Instead, Varghese explains, "[i]f the retrieved data tokens that were previously stored on a device by this invention, **e.g., a secure cookie, a Flash cookie, or Flash data, are not present, a further pattern check is performed**," which "examines the particulars of the pattern of the location and device criteria and assigns an appropriate score." EX1004, 19:62-67 (emphasis added). That is, when a cookie is missing (e.g., if a user were to clear the browser's cache), Varghese simply assesses other device characteristics to make a security decision.

EX1004, 19:62-67. As I note above, Varghese discloses replacing cookies upon login, so if one cookie is missing, it can be replaced at that time. EX1004, 26:12-28.

97. Therefore, it is my opinion that Dr. Wills does not show that Varghese renders obvious claim elements [1.b.iv] and [6.a.iv].

IX. CONCLUSION

In signing this declaration, I recognize that the declaration will be filed as evidence in an *inter partes* review before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required, I will appear for cross-examination within the United States during the time allotted.

I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed on this 27th day of June, 2025, in Srinagarindra, Phatthalung, Thailand.

Bernard J Jansen

Bernard J. Jansen