Michael A. Sherman (SBN 94783)
masherman@stubbsalderton.com
Jeffrey F. Gersh (SBN 87124)
jgersh@stubbsalderton.com
Sandeep Seth (SBN 195914)
sseth@stubbsalderton.com
Wesley W. Monroe (SBN 149211)
wmonroe@stubbsalderton.com
Stanley H. Thompson, Jr. (SBN 198825)
sthompson@stubbsalderton.com
Viviana Boero Hedrick (SBN 239359)
vhedrick@stubbsalderton.com
STUBBS, ALDERTON & MARKILES, LLP
15260 Ventura Blvd., 20th Floor
Sherman Oaks, CA 91403
Telephone: (818) 444-4500
Facsimile: (818) 444-4520

Attorneys for Plaintiffs
[Additional Attorneys listed below]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE PERSONALWEB TECHNOLOGIES, LLC, ET AL., PATENT LITIGATION	**CASE NO.: 5:18-md-02834-BLF** **FIRST AMENDED COMPLAINT** **DEMAND FOR JURY TRIAL**
PERSONALWEB TECHNOLOGIES, LLC, a Texas limited liability company, and LEVEL 3 COMMUNICATIONS, LLC, a Delaware limited liability company, Plaintiffs, v. TRIPADVISOR LLC, a Delaware limited liability company, Defendant.	**Case No.: 5:18-cv-05967-BLF**

Plaintiff PersonalWeb Technologies, LLC ("Plaintiff" or "PersonalWeb") files this First Amended Complaint ("Complaint") for patent infringement against Defendant TripAdvisor LLC ("Defendant"). Plaintiff PersonalWeb Technologies, LLC alleges:

PRELIMINARY STATEMENT

1. PersonalWeb and Level 3 Communications, LLC ("Level 3") are parties to an agreement between Kinetech, Inc. and Digital Island, Inc. dated September 1, 2000 (the "Agreement"). Pursuant to the Agreement, PersonalWeb and Level 3 each own a fifty percent (50%) undivided interest in and to the patents at issue in this action: U.S. Patent Nos. 6,928,442, 7,802,310, and 8,099,420 ("Patents-in-Suit"). Level 3 has joined in this Complaint pursuant to its contractual obligations under the Agreement, at the request of PersonalWeb.

2. Pursuant to the Agreement, Level 3 has, among other rights, certain defined rights to use, practice, license, sublicense and enforce and/or litigate the Patents-in-Suit in connection with a particular field of use ("Level 3 Exclusive Field"). Pursuant to the Agreement PersonalWeb has, among other rights, certain defined rights to use, practice, license, sublicense, enforce and/or litigate the Patents-in-Suit in fields other than the Level 3 Exclusive Field (the "PersonalWeb Patent Field").

3. All infringement allegations, statements describing PersonalWeb, statements describing any Defendant (or any Defendant's products) and any statements made regarding jurisdiction and venue are made by PersonalWeb alone, and not by Level 3. PersonalWeb alleges that the infringements at issue in this case all occur within, and are limited to, the PersonalWeb Patent Field. Accordingly, PersonalWeb has not provided notice to Level 3—under Section 6.4.1 of the Agreement or otherwise—that PersonalWeb desires to bring suit in the Level 3 Exclusive Field in its own name on its own behalf or that PersonalWeb knows or suspects that Defendant is infringing or has infringed any of Level 3's rights in the patents.

THE PARTIES

4. Plaintiff PersonalWeb Technologies, LLC is a limited liability company duly organized and existing under the laws of Texas with its principal place of business at 112 E. Line Street, Suite 204, Tyler, TX 75702.

5. Plaintiff Level 3 Communications, LLC is a limited liability company organized under the laws of Delaware with its principal place of business at 100 CenturyLink Drive, Monroe, Louisiana, 71203.

6. PersonalWeb's infringement claims asserted in this case are asserted by PersonalWeb and all fall outside the Level 3 Exclusive Field. Level 3 is currently not asserting patent infringement in this case in the Level 3 Exclusive Field against any Defendant.

7. Defendant TripAdvisor LLC is, upon information and belief, a Delaware limited liability company having a principal place of business and regular and established place of business at 400 1st Avenue, Needham, Massachusetts 02494.

JURISDICTION AND VENUE

8. The court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq.*

9. Venue is proper in this federal district pursuant to 28 U.S.C. §§ 1391(b)–(c) and 1400(b) because Defendant is incorporated in the State of Delaware.

10. Venue is also proper in this Court because this action has been transferred to this District by the Judicial Panel on Multidistrict Litigation for consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407.

11. This court has personal jurisdiction over Defendant because, in addition to the allegations in above paragraphs, on information and belief, Defendant is domiciled in this District. Further, on information and belief, Defendant purposefully directed activities at residents of Delaware, the claims herein arise out of and relate to those activities, and assertion of personal jurisdiction over Defendant would be fair.

12. On information and belief, Defendant is subject to this Court's jurisdiction because this action has been transferred to this District by the Judicial Panel on Multidistrict Litigation for consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407.

PERSONALWEB BACKGROUND

13. The Patents-in-Suit cover fundamental aspects of cloud computing, including the identification of files or data and the efficient retrieval thereof in a manner which reduces bandwidth transmission and storage requirements.

14. The ability to reliably identify and access specific data is essential to any computer system or network. On a single computer or within a small network, the task is relatively easy: simply name the file, identify it by that name and its stored location on the computer or within the network, and access it by name and location. Early operating systems facilitated this approach with standardized naming conventions, storage device identifiers, and folder structures.

15. Ronald Lachman and David Farber, the inventors of the Patents-in-Suit, recognized that the conventional approach for naming, locating, and accessing data in computer networks could not keep pace with ever-expanding, global data processing networks. New distributed storage systems use files that are stored across different devices in dispersed geographic locations. These different locations could use dissimilar conventions for identifying storage devices and data partitions. Likewise, different users could give identical names to different files or parts of files—or unknowingly give different names to identical files. No solution existed to ensure that identical file names referred to the same data, and conversely, that different file names referred to different data. As a result, expanding networks could not only become clogged with duplicate data, they also made locating and controlling access to stored data more difficult.

16. Lachman and Farber developed a solution: replacing conventional naming and storing conventions with system-wide "substantially unique," content-based identifiers. Their approach assigned substantially unique identifiers to "data items" of any type: "the contents of a file, a portion of a file, a page in memory, an object in an object-oriented program, a digital message, a digital scanned image, a part of a video or audio signal, or any other entity which can be represented by a

sequence of bits." Applied system-wide, this invention would permit any data item to be stored, located, managed, synchronized, and accessed using its content-based identifier.

17. To create a substantially unique, content-based identifier, Lachman and Farber turned to cryptography. Cryptographic hash functions, including MD4, MD5, and SHA, had been used in computer systems to verify the integrity of retrieved data—a so-called "checksum." Lachman and Farber recognized that these same hash functions could be devoted to a vital new purpose: if a cryptographic hash function was applied to a sequence of bits (a "data item"), it would produce a substantially unique result value, one that: (1) virtually guarantees a different result value if the data item is changed; (2) is computationally difficult to reproduce with a different sequence of bits; and (3) cannot be used to recreate the original sequence of bits.

18. These cryptographic hash functions would thus assign any sequence of bits, based on content alone, with a substantially unique identifier. Lachman and Farber estimated that the odds of these hash functions producing the same identifier for two different sequences of bits (i.e., the "probability of collision") would be about 1 in 2 to the 29th power. Lachman and Farber dubbed their content-based identifier a "True Name."

19. Using a True Name, Lachman and Farber conceived various data structures and methods for managing data (each data item correlated with a single True Name) within a network—no matter the complexity of the data or the network. These data structures provide a key-map organization, allowing for a rapid identification of any particular data item anywhere in a network by comparing a True Name for the data item against other True Names for data items already in the network. In operation, managing data using True Names allows a user to determine the location of any data in a network, determine whether access is authorized, and to selectively provide access to specific content not possible using the conventional naming arts.

20. On April 11, 1995, Lachman and Farber filed their patent application, describing these and other ways in which content-based "True Names" elevated data-processing systems over conventional file-naming systems. The first True Name patent issued on November 2, 1999. The last of the Patents-in-Suit has expired, and the allegations herein are directed to the time period before expiration of the last of the Patents-in-Suit.

21. PersonalWeb has successfully enforced its intellectual property rights against third party infringers, and its enforcement of the Patents-In Suit is ongoing. This enforcement has resulted in PersonalWeb obtaining settlements and granting non-exclusive licenses regarding the Patents-in-Suit.

GENERAL BACKGROUND

22. A webpage is a type of document that is typically retrieved over the World Wide Web, made viewable and formatted (rendered) by a web browser, and displayed electronically. A "webpage" often refers to what is visible in a browser, but sometimes also refers to a computer file ("webpage base file"), usually written in Hypertext Markup Language ("HTML") or a comparable markup language. Such HTML webpage base files typically include text, formatting, and references (hyperlinks) to other web content, such as style sheets, scripts, and images that make up part of the webpage. Web content referenced in an HTML or similar file are also called "asset files" herein. The web browser coordinates the retrieval of the various asset files of a webpage and renders the webpage for display from the webpage base file and the asset files referenced in the webpage base file or referenced in other asset files.

23. On the World Wide Web, hyperlinks generally include Uniform Resource Identifiers ("URIs"), which each typically include an address of a server ("host") from which the asset file is to be retrieved (*e.g.*, "www.website.com"), a "path" to the location of that asset file on the host server (*e.g.*, "/directory/"), and a filename (*e.g.*, "filename.ext").

24. On the Internet, a web browser typically retrieves a webpage base file from a remote web server and retrieves referenced asset files from the same or different servers. The web browser retrieves a webpage base file or an asset file by making a GET "request" to a web server using the Hypertext Transfer Protocol ("HTTP"), an industry standard. The web server may respond to such an HTTP request with a HTTP "response" that includes the requested web content and may include other information or instructions.

25. A static webpage is delivered exactly as stored, as web content in the web server's file system or memory. In contrast, a dynamic webpage is generated by a web server application, usually

driven by server-side software, upon receipt of a request from a browser (user). For example, a picture of a building might be delivered as static content (a picture) whereas the latest traffic conditions may be delivered dynamically based on real time traffic information.

26. The speed of a browser retrieving webpage base files and incorporated asset files can be increased by the browser storing previously retrieved webpage base files and asset files in a browser "cache" on the computer running the browser. If a browser's user later requests a previously retrieved webpage base file or requests a webpage that includes an asset file previously used by the browser in rendering the same or a different webpage (for example, by reloading a webpage or visiting the same webpage again), the browser may use the cached webpage base file or asset file rather than having to download the same file repeatedly over the Internet again.

27. Two computers communicating over the Internet usually are not directly connected to each other but rather interact via chains of network appliances and other computers (*e.g.*, "switches" and "intermediate" servers). Many intermediate servers have caches similar to and complementing the browser cache that store webpage base files and assets that pass through that intermediate server. If a browser or server requests a file from the intermediate server that is present in that intermediate server's cache, the intermediate server can use the content in its cache to respond to the request rather than send the request upstream towards the web server from which the file initially originated (also called the "origin server").

28. Responses to HTTP requests may include header elements (control elements) and a body (the "object" that was requested). Under HTTP, web servers can include a "cache-control" header with a response that includes a webpage or asset file. A "cache-control" header includes one or more directives that instruct browsers and intermediate server caches ("intermediate caches") as to whether and for how long the file (object) included in the response may be cached or under what circumstances and under what conditions the cached content may be used. HTTP also provides for including other headers in responses that provide similar types of instructions to browsers and intermediate caches. Collectively, these other headers and directives in a "cache-control" header are referred to herein as "cache-control headers."

29. Given that webpage content changes, sometimes rather quickly and regularly, a problem that website owners face is effectively instructing a browser that is re-rendering a previously cached webpage that one or more of its cached files for that webpage are no longer the correct and authorized content (the content of those files has changed) and similarly reauthorizing the use of those cached files whose content has not changed.

30. On one hand, website owners want to encourage the browsers that render their web pages to use cached files thereby reducing the number of requests for these files that are being made to their webpage servers. Therefore, they frequently will set cache-control headers that authorize the browser to cache their webpage base files and asset files so the files are on hand when the browser needs to render that webpage again. On the other hand, website owners want the browsers to use the latest authorized files so that their users do not see the wrong content when viewing their webpage.

DEFENDANT'S BACKGROUND

31. On information and belief, Defendant has operated a website located at **tripadvisor.com**, and has done so since before expiration of the last to expire of the Patents-in-Suit, which has operated to provide authorized webpage content to its users in the manner herein described.[1]

32. On information and belief, Defendant's web servers utilized a system of notifications and authorizations to control the distribution of content, *e.g.*, what webpage content may be served from web servers and intermediate caches and what cached webpage content a browser is re-authorized to use to render Defendant's webpage(s).

33. On information and belief, Defendant's system and its associated method of providing webpage content used "conditional" HTTP GET requests with If-None-Match headers and associated content-based ETag values for various asset files required to render various webpages of the Defendant.

34. On information and belief, Defendant's system and associated method used these ETags to instruct both the intermediate cache servers and the endpoint caches at browsers to verify

[1] While the complaint is sometimes written in the present or present perfect tense, all specific allegations are directed to the system's operations and the method's performance in the relevant time period.

whether they were still authorized to reuse the previously cached webpage base files of Defendant and to instruct them to obtain newly authorized content in rendering Defendant's webpage when that content had changed. In other words, whether the previously cached content was still considered valid for use by the Defendant website operator.

35. On information and belief, Defendant thereby reduced the bandwidth and computation required by its origin servers and any intermediate cache servers to field user requests to render Defendant's webpages as those servers only need to serve files whose content has changed. On information and belief, this has allowed for the efficient update of cached information only when such content has changed, thereby reducing transaction overhead and bandwidth and allowing the authorized content to be served from the nearest cache.

36. More particularly, on information and belief, each of Defendant's webpages included a webpage base file (*e.g.*, a main or initial HTML file) and one or more asset files referenced in the webpage base file (or referenced in other asset files that contained references to other asset files). On information and belief, the references in the webpage base file to the asset files needed to render the webpage were typically Uniform Resource Identifiers ("URIs"), which each typically included a filename, the address of a host server from which the asset file could be retrieved, and a "path" to the location of that asset file on that server.

37. On information and belief, for at least one of the asset files ("CBI ETag asset files"), the asset file comprised a sequence of bits and an associated ETag value was generated by Defendant by applying a hash function to the sequence of bits; wherein any two CBI ETag asset files comprising identical sequences of bits had identical associated ETag values. Thus, on information and belief, when a CBI ETag asset file's content was changed a new associated ETag value was generated by Defendant. On information and belief, Defendant caused the origin server for each CBI ETag asset file to serve such CBI ETag asset file with its associated Etag value in response to HTTP GET requests for the CBI ETag asset file.

38. On information and belief, when an intermediate cache server or a browser requested a webpage from the Defendant for the first time, it sent an HTTP GET request with the webpage's URI and Defendant's origin server or an upstream cache server responded by sending an HTTP 200

(OK) response message containing the webpage base file. On information and belief, a browser then sent individual HTTP GET requests, each with an asset file's URI that was referenced in the webpage base file, and the asset files' origin servers or intermediate cache servers responded by sending individual HTTP 200 responses containing the requested asset files, along with, if available, their respective associated ETags. On information and belief, upon receipt of the HTTP 200 responses, the intermediate cache server or browser cached the webpage base file and asset files with their associated URI and associated ETag values and the browser used them in rendering the requested web page of the Defendant. On information and belief, the origin servers, intermediate cache servers, and browser caches were caused to maintain databases/tables which mapped the URIs of webpage base files and asset files to their respective responses and, if applicable, associated cache-control headers and ETags.

39. On information and belief, by responding to an HTTP GET request for a given webpage by transmitting content of a asset file with an associated ETag, Defendant instructed the browser cache and all intermediate cache servers, to use an HTTP conditional GET request the next time that asset file is requested. More specifically, on information and belief, the browser or intermediate cache is instructed to include the ETag in the HTTP conditional GET request with an "If-None-Match" header to re-verify that they are still authorized to serve or use that content or determine that they are no longer authorized to use that content and therefore must use new content.

40. On information and belief, Defendant did this, for example, by causing cache-control headers to be included in HTTP responses containing its asset files. On information and belief, Defendant benefits from using the ETags to control the distribution of its webpage content by communicating to a downstream cache and to a browser which of Defendant's cached webpage base files it is reauthorized to serve/use and what newly authorized files it must first obtain in serving/rendering Defendant's webpages.

41. More particularly, on information and belief, when a browser again requested the Defendant's webpage, the browser either used a cached copy, if allowed by the cache-control headers, or retrieved a new copy of the webpage base file for Defendant's webpage. Similarly, on information and belief, for asset files referenced in the new or cached webpage base file, the browser either used a

cached copy or retrieved a new copy, if allowed by the cache-control headers, of the asset files for Defendant's webpage.

42. On information and belief, for an asset file stored in the browser's cache with an ETag, and based on the cache-control headers received in the original response, the browser sent a conditional GET request with an If-None-Match header using the associated ETag value and the URI for the asset file so as to be notified whether the browser still had Defendant's authority to render the webpage with its locally cached asset file. In other words, whether the cached content was still valid for use in rendering Defendant's webpage.

43. On information and belief, under most circumstances, a responding intermediate cache server having content cached for the URI in the conditional GET request and having an ETag for that URI responded to the request by determining whether it had the same associated ETag value for that URI. If it had no ETag value for that URI, on information and belief, the request was passed up to an upstream intermediate cache server capable of responding or, if none, to the URI's origin server, which responded to the request. On information and belief, if the intermediate cache server did not have content cached for the URI in the conditional GET request, the request was similarly passed up to an upstream intermediate cache server capable of responding or, if none, to the URI's origin server.

44. On information and belief, if the responding server had the webpage content for that URI and there was a match between the ETag it received in the request with the ETag it currently had associated for that URI, it sent back an HTTP 304 (Not Modified) response message; this message notifying the browser that the same webpage content was present at the responding server and that the browser was still authorized to use that previously cached asset file to render the webpage. On information and belief, upon receipt of the HTTP 304 response, the browser accessed the locally cached asset file in rendering the webpage.

45. On information and belief, if the asset file's associated ETag sent by the browser in the conditional GET If-None-Match request did not match the associated ETag maintained at the responding server (or other intermediate cache servers further upstream or the origin server) for that URI, the responding server sent back an HTTP 200 response along with the new asset file and its new ETag value. The HTTP 200 response indicated to the browser that it was not authorized to use (or

serve, in the case of an intermediate cache server receiving the HTTP 200 response) the previously cached asset file. In response to receiving the HTTP 200 response, the browser (or intermediate cache server) was instructed to update its respective cache with the new asset file and associated ETag. The browser subsequently used the new asset file to render the webpage.

46. Exhibit 1 to the complaint lists specific examples of files that were, on information and belief, served by or on behalf of Defendant during the relevant time period. The examples in Exhibit 1 include: an asset file with a content-based ETag for that asset file.

47. On information and belief, in this manner, Defendant used ETag values based on the asset files' content to control the behavior of downstream intermediate cache servers and browser caches to assure that they only accessed and used Defendant's latest authorized webpage content to serve or to render its webpages.

FIRST CLAIM FOR RELIEF

INFRINGEMENT OF U.S. PATENT NO. 6,928,442

48. PersonalWeb repeats and realleges paragraphs 1–47, as if the same were fully stated herein.

49. On August 9, 2005, United States Patent No. 6,928,442 (the "'442 patent") was duly and legally issued for an invention entitled "Enforcement and Policing of Licensed Content Using Content-Based Identifiers." PersonalWeb has an ownership interest in the '442 patent by assignment, including the exclusive right to enforce the '442 patent within the PersonalWeb Patent Field, and continues to hold that ownership interest in the '442 patent. A true and correct copy of the '442 patent is attached as Exhibit 2.

50. Defendant has infringed at least claims 10 and 11 of the '442 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Defendant's infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '442 patent pursuant to 35 U.S.C. § 271.

51. For example, claim 10 covers "a method, in a system in which a plurality of files are distributed across a plurality of computers." On information and belief, Defendant has used a system of notifications and authorizations to distribute a plurality of files, *e.g.*, Defendant's files containing content necessary to render its webpages, across a plurality of computers such as production servers, origin servers, intermediate cache servers and endpoint caches used by browsers rendering Defendant's webpages.

52. Claim 10 then recites the act of "obtaining a name for a data file, the name being based at least in part on a given function of the data, wherein the data used by the function comprises the contents of the particular file." As set forth above, on information and belief, Defendant generated or otherwise obtained ETags for its asset files used to render its webpages using a hash function, wherein the ETags were based on the contents of the particular files. Moreover, Defendant caused the intermediate caches servers and endpoint caches to obtain the ETags in HTTP 200 responses sent from Defendant's origin servers. On information and belief, Defendant caused intermediate cache servers and its origin servers to obtain ETags in conditional GET messages from endpoint and intermediate caches, as described *supra*.

53. Claim 10 then recites the act of "determining, using at least the name, whether a copy of the data file is present on at least one of said computers." On information and belief, as set forth above, Defendant has caused its origin severs and the intermediate cache servers between an endpoint cache and one of its origin servers to, in response to receiving a conditional GET request with an If-None-Match header, determine whether it has a file present that matches the URI in the conditional GET and to compare the ETag in the conditional GET to the ETag for that URI and determine whether a copy of the content having that ETag is present.

54. Claim 10 then recites the act of "determining whether a copy of the data file that is present on a at least one of said computers is an unauthorized copy or an unlicensed copy of the data file." On information and belief, as set forth above, if there was a match, the origin or intermediate cache server determined that the copy of the file present at the downstream intermediate cache server and/or the endpoint cache was an authorized or licensed copy of the data file. Conversely, if there was no match, it determined that the copy of the file present at the downstream intermediate cache server

and/or the endpoint cache was an unauthorized copy of the data file. Likewise, if the browser determined that it had a file with a matching URI, the browser determined that it was still authorized to use that file.

55. Defendant’s acts of infringement caused damage to PersonalWeb and PersonalWeb is entitled to recover from Defendant the damages sustained by PersonalWeb as a result of Defendant’s wrongful acts in an amount subject to proof at trial.

SECOND CLAIM FOR RELIEF

INFRINGEMENT OF U.S. PATENT NO. 7,802,310

56. PersonalWeb repeats and realleges paragraphs 1–47, as if the same were fully stated herein.

57. On September 21, 2010, United States Patent No. 7,802,310 (the “’310 patent”) was duly and legally issued for an invention entitled “Controlling Access to Data in a Data Processing System.” PersonalWeb has an ownership interest in the ’310 patent by assignment, including the exclusive right to enforce the ’310 patent within the PersonalWeb Patent Field, and continues to hold that ownership interest in the ’310 patent. A true and correct copy of the ’310 patent is attached as Exhibit 3.

58. Defendant has infringed at least claim 20 of the ’310 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Defendant’s infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the ’310 patent pursuant to 35 U.S.C. § 271.

59. For example, claim 20 covers a “computer-implemented method operable in a system which includes a plurality of computers.” On information and belief, Defendant used the claimed computer implemented method by using a system of notifications and authorizations to control the distribution of data items, such as various asset files, necessary to render its webpages, across a plurality of computers such as production servers, origin servers, intermediate cache servers, and endpoint caches.

60. Claim 20 then recites "controlling distribution of content from a first computer to at least one other computer, in response to a request obtained by a first device in the system from a second device in the system, the first device comprising hardware including at least one processor, the request including at least a content-dependent name of a particular data item, the content-dependent name being based at least in part on a function of at least some of the data comprising the particular data item, wherein the function comprises a message digest function or a hash function, and wherein two identical data items will have the same content-dependent name." On information and belief, as set forth above, Defendant has caused downstream intermediate cache servers and endpoint caches to send conditional GET requests with If-None-Match headers containing ETags that are fielded by upstream cache or origin servers. On information and belief, the ETags were content-dependent names for a data item based on hashing the data item's contents; and when the file's content changed a new content-dependent name was determined. On information and belief, in Defendant's method, a first computer, such as the intermediate cache server or origin server, received such conditional GET requests from a second computer, such as a user browser or other intermediate cache server, regarding data items, such as webpage or asset files, the requests including ETags associated with the respective data items.

61. Claim 20 then recites "based at least in part on said content-dependent name of said particular data item, the first device (A) permitting the content to be provided to or accessed by the at least one other computer if it is not determined that the content is unauthorized or unlicensed, otherwise, (B) if it is determined that the content is unauthorized or unlicensed, not permitting the content to be provided to or accessed by the at least one other computer." On information and belief, the first computer, such as an upstream intermediate cache server or origin server, maintained a plurality of ETags associated with Defendant's asset and webpage base files On information and belief, the ETag in a request and the ETag maintained by the first computer for the particular data item sought by the request were compared to determine whether the associated content present at the downstream computer was still authorized to be used/served or whether new authorized content must be provided thereto. If it was determined that the data item corresponding to the received ETag was still authorized to be used, the first computer sent back an HTTP 304 response authorizing the

downstream cache server or end-user cache to access the file content already present in order to serve it or to use it to render the webpage. On information and belief, if it had been determined that the data item corresponding to received E-tag was no longer authorized, the first computer sent back an HTTP 200 response which indicated to the downstream cache server or end-user cache that was not authorized to access the old content and must access the new authorized file content contained in the HTTP 200 response to serve it or to use it to render the webpage.

62. Defendant's acts of infringement have caused damage to PersonalWeb and PersonalWeb is entitled to recover from Defendant the damages sustained by PersonalWeb as a result of Defendant's wrongful acts in an amount subject to proof at trial.

THIRD CLAIM FOR RELIEF

INFRINGEMENT OF U.S. PATENT NO. 8,099,420

63. PersonalWeb repeats and realleges paragraphs 1–47, as if the same were fully stated herein.

64. On January 17, 2012, United States Patent No. 8,099,420 (the "'420 patent") was duly and legally issued for an invention entitled "Accessing Data in a Data Processing System." PersonalWeb has an ownership interest in the '420 patent by assignment, including the exclusive right to enforce the '420 patent within the PersonalWeb Patent Field, and continues to hold that ownership interest in the '420 patent. A true and correct copy of the '420 patent is attached as Exhibit 4.

65. Defendant has infringed claims 25, 26, 27, 29, 30, 32, 34–36, and 166 of the '420 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner recited herein. Defendant's infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '420 patent pursuant to 35 U.S.C. § 271.

66. For example, claim 166 covers a "system comprising hardware, including at least a processor, and software, in combination with said hardware." On information and belief, Defendant has controlled the distribution of its website content across a system that included hardware including a processor, such as its production servers as well as origin servers, intermediate cache servers, and

endpoint caches; and software, in combination with such hardware, such as a web development framework, software utilized in implementing the HTTP web protocol, and the software used on host servers that Defendant used to serve its webpages.

67. Claim 166 then recites "(A) for a particular data item in a set of data items, said particular data item comprising a corresponding particular sequence of bits." On information and belief, Defendant's system has controlled the distribution of asset files necessary to render its webpages which represent particular data items, and each of these files comprise a corresponding sequence of bits.

68. Claim 166 then recites that for the particular data item to "(a1) determine one or more content-dependent digital identifiers for said particular data item, each said content-dependent digital identifier being based at least in part on a given function of at least some of the bits in the particular sequence of bits of the particular data item, wherein two identical data items will have the same digital identifiers as determined using said given function." On information and belief, Defendant's system has applied hash functions to each of various Defendant's webpage base files to all of the bits of the file's content to determine an ETag, for the file's content; whereby two identical data items have the same ETag values. On information and belief, ETag values were associated with files' URIs.

69. Claim 166 then recites that for the particular data item "(a2) selectively permits the particular data item to be made available for access and to be provided to or accessed by or from at least some of the computers in a network of computers, wherein the data item is not to be made available for access or provided without authorization, as resolved based, at least in part, on whether or not at least one of said one or more content-dependent digital identifiers for said particular data item corresponds to an entry in one or more databases, each of said one or more databases comprising a plurality of identifiers, each of said identifiers in each said database corresponding to at least one data item of a plurality of data items, and each of said identifiers in each said database being based, at least in part, on at least some of the data in a corresponding data item."

70. On information and belief, Defendant's system has included one or more web servers with databases containing ETag values associated with the URIs for various of the asset files necessary to render its webpages; moreover, Defendant's system has used a system of conditional GET requests

with If-None-Match headers and HTTP 304 and HTTP 200 responses containing the ETags, as described more particularly *supra*, to ensure that downstream caches only access authorized file content to either serve that file content further downstream or to use it to render Defendant's webpages. On information and belief, in particular, as more fully described *supra*, the system compared the ETag received in a given conditional GET request with the ETags contained in the database to selectively determine whether the requesting computer could access the file content it already had or must access newly received authorized content.

71. Defendant's acts of infringement have caused damage to PersonalWeb and PersonalWeb is entitled to recover from Defendant the damages sustained by PersonalWeb as a result of Defendant's wrongful acts in an amount subject to proof at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff PersonalWeb requests entry of judgment in its favor and against Defendant as follows:

a) Declaration that Defendant has infringed U.S. Patent Nos. 6,928,442, 7,802,310, and 8,099,420 as described in this action;

b) Awarding the damages arising out of Defendant's infringement of U.S. Patent Nos. 6,928,442, 7,802,310, and 8,099,420, together with pre-judgment and post-judgment interest, in an amount according to proof;

c) An award of attorneys' fees pursuant to 35 U.S.C. § 285 or as otherwise permitted by law; and

d) For costs incurred and such other and further relief as the Court may deem just and proper.

Respectfully submitted,

Dated: October 4, 2018

STUBBS, ALDERTON & MARKILES, LLP

By: */s/ Stanley H. Thompson, Jr.*
Michael A. Sherman
Jeffrey F. Gersh
Sandeep Seth
Wesley W. Monroe
Stanley H. Thompson, Jr.
Viviana Boero Hedrick
Attorneys for Plaintiffs

Dated: October 4, 2018

MACEIKO IP

By: */s/ Theodore S. Maceiko*
Theodore S. Maceiko (SBN 150211)
ted@maceikoip.com
MACEIKO IP
420 2nd Street
Manhattan Beach, California 90266
Telephone: (310) 545-3311
Facsimile: (310) 545-3344
Attorneys for Plaintiff
PERSONALWEB TECHNOLOGIES, LLC,

Dated: October 4, 2018

DAVID D. WIER

By: */s/ David D. Wier*
David D. Wier
david.wier@level3.com
Vice President and Assistant General Counsel
Level 3 Communications, LLC
1025 Eldorado Boulevard
Broomfield, CO 80021
Telephone: (720) 888-3539
Attorneys for Plaintiff
LEVEL 3 COMMUNICATIONS, LLC

DEMAND FOR JURY TRIAL

Pursuant to Fed. R. Civ. P. 38(b) and Local Rule 3–6, Plaintiff PersonalWeb Technologies, LLC hereby demands a trial by jury on all issues triable in this action.

Respectfully submitted,

Dated: October 4, 2018

STUBBS, ALDERTON & MARKILES, LLP

By: */s/ Stanley H. Thompson, Jr.*
Michael A. Sherman
Jeffrey F. Gersh
Sandeep Seth
Wesley W. Monroe
Stanley H. Thompson, Jr.
Viviana Boero Hedrick
Attorneys for Plaintiffs

Dated: October 4, 2018

MACEIKO IP

By: */s/ Theodore S. Maceiko*
Theodore S. Maceiko (SBN 150211)
ted@maceikoip.com
MACEIKO IP
420 2nd Street
Manhattan Beach, California 90266
Telephone: (310) 545-3311
Facsimile: (310) 545-3344
Attorneys for Plaintiff
PERSONALWEB TECHNOLOGIES, LLC,

Dated: October 4, 2018

DAVID D. WIER

By: */s/ David D. Wier*
David D. Wier
david.wier@level3.com
Vice President and Assistant General Counsel
Level 3 Communications, LLC
1025 Eldorado Boulevard
Broomfield, CO 80021
Telephone: (720) 888-3539
Attorneys for Plaintiff
LEVEL 3 COMMUNICATIONS, LLC