

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

10 **Attorneys for Plaintiffs**
 [Additional Attorneys listed
 11 below]

12 UNITED STATES DISTRICT COURT
 13 NORTHERN DISTRICT OF CALIFORNIA
 14 SAN JOSE DIVISION

16 IN RE: PERSONAL WEB TECHNOLOGIES,
 17 LLC ET AL., PATENT LITIGATION

CASE NO. 5:18-md-02834-BLF

FIRST AMENDED COMPLAINT

DEMAND FOR JURY TRIAL

20 _____
 21 PERSONALWEB TECHNOLOGIES, LLC, a
 22 Texas limited liability company, and
 LEVEL 3 COMMUNICATIONS, LLC,
 a Delaware limited liability company,

Case No. 5:18-cv-00183-BLF

23 Plaintiffs,

24 v.

25 SQUARE, INC., a Delaware corporation,

26 Defendant.

1 Plaintiff PersonalWeb Technologies, LLC (“Plaintiff” or “PersonalWeb”) files this First
2 Amended Complaint (“Complaint”) for patent infringement against Defendant Square, Inc.
3 (“Defendant”). Plaintiff PersonalWeb Technologies, LLC alleges:

4
5 **PRELIMINARY STATEMENT**

6 1. PersonalWeb and Level 3 Communications, LLC (“Level 3”) are parties to an
7 agreement between Kinetech, Inc. and Digital Island, Inc. dated September 1, 2000 (the “Agreement”).
8 Pursuant to the Agreement, PersonalWeb and Level 3 each own a fifty percent (50%) undivided
9 interest in and to the patents at issue in this action: U.S. Patent Nos. 6,928,442, 7,802,310, 7,945,544,
10 and 8,099,420 (“Patents-in-Suit”). Level 3 has joined in this Complaint pursuant to its contractual
11 obligations under the Agreement, at the request of PersonalWeb.

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

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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 Square, Inc. is, upon information and belief, a Delaware corporation having a principal place of business and regular and established place of business at 1455 Market Street, Suite 600, San Francisco CA 94103.

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, on information and belief, Defendant has a regular and established place of business in this District and has committed acts of infringement in this District.

10. 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, Defendant purposefully directed activities at residents of California, the claims herein arise out of and relate to those activities, and assertion of personal jurisdiction over Defendant would be fair.

PERSONALWEB BACKGROUND

1
2 11. The Patents-in-Suit cover fundamental aspects of cloud computing, including the
3 identification of files or data and the efficient retrieval thereof in a manner which reduces bandwidth
4 transmission and storage requirements.

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

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

20 14. Lachman and Farber developed a solution: replacing conventional naming and storing
21 conventions with system-wide “substantially unique,” content-based identifiers. Their approach
22 assigned substantially unique identifiers to “data items” of any type: “the contents of a file, a portion
23 of a file, a page in memory, an object in an object-oriented program, a digital message, a digital
24 scanned image, a part of a video or audio signal, or any other entity which can be represented by a
25 sequence of bits.” Applied system-wide, this invention would permit any data item to be stored,
26 located, managed, synchronized, and accessed using its content-based identifier.

27 15. To create a substantially unique, content-based identifier, Lachman and Farber turned
28 to cryptography. Cryptographic hash functions, including MD4, MD5, and SHA, had been used in

1 computer systems to verify the integrity of retrieved data—a so-called “checksum.” Lachman and
2 Farber recognized that these same hash functions could be devoted to a vital new purpose: if a
3 cryptographic hash function was applied to a sequence of bits (a “data item”), it would produce a
4 substantially unique result value, one that: (1) virtually guarantees a different result value if the data
5 item is changed; (2) is computationally difficult to reproduce with a different sequence of bits; and
6 (3) cannot be used to recreate the original sequence of bits.

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

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

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

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

GENERAL BACKGROUND

1
2 20. A webpage is a type of document that is typically retrieved over the World Wide Web,
3 made viewable and formatted (rendered) by a web browser, and displayed electronically. A “webpage”
4 often refers to what is visible in a browser, but sometimes also refers to a computer file (“webpage
5 base file”), usually written in Hypertext Markup Language (“HTML”) or a comparable markup
6 language. Such HTML webpage base files typically include text, formatting, and references
7 (hyperlinks) to other web content, such as style sheets, scripts, and images that make up part of the
8 webpage. Web content referenced in an HTML or similar file are also called “asset files” herein. The
9 web browser coordinates the retrieval of the various asset files of a webpage and renders the webpage
10 for display from the webpage base file and the asset files referenced in the webpage base file or
11 referenced in other asset files.

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

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

22 23. A static webpage is delivered exactly as stored, as web content in the web server’s file
23 system or memory. In contrast, a dynamic webpage is generated by a web server application, usually
24 driven by server-side software, upon receipt of a request from a browser (user). For example, a picture
25 of a building might be delivered as static content (a picture) whereas the latest traffic conditions may
26 be delivered dynamically based on real time traffic information.

27 24. The speed of a browser retrieving webpage base files and incorporated asset files can
28 be increased by the browser storing previously retrieved webpage base files and asset files in a browser

1 “cache” on the computer running the browser. If a browser’s user later requests a previously retrieved
2 webpage base file or requests a webpage that includes an asset file previously used by the browser in
3 rendering the same or a different webpage (for example, by reloading a webpage or visiting the same
4 webpage again), the browser may use the cached webpage base file or asset file rather than having to
5 download the same file repeatedly over the Internet again.

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

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

23 27. Given that webpage content changes, sometimes rather quickly and regularly, a
24 problem that website owners face is effectively instructing a browser that is re-rendering a previously
25 cached webpage that one or more of its cached files for that webpage are no longer the correct and
26 authorized content (the content of those files has changed) and similarly reauthorizing the use of those
27 cached files whose content has not changed.
28

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

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

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

17 36. On information and belief, Defendant's website used a web application framework to
18 develop and compile various webpages of the Defendant, including asset files that were used in
19 rendering the webpages, and to generate fingerprints of the contents of asset files. On information and
20 belief, the fingerprints of individual asset files that were part of the webpage's content were included
21 in the respective filenames of the individual asset files. On information and belief, the modified
22 filenames were then used as part of the URI used to access the individual asset files over the Internet.
23 On information and belief, when an asset file's content was changed, a new fingerprint was generated
24 and included in the filename, its URI thus being changed accordingly.

25 37. On information and belief, the asset file fingerprint was generated with a hash function
26 and used to identify content changes. Furthermore, on information and belief, asset file URIs (with
27 respective fingerprints) were included in webpage base files or other asset files contained references
28 to other asset files. On information and belief, static webpage base files, if any, were recompiled when

1 any URI of a referenced asset file was changed (due to the fingerprint of the referenced asset file
2 changing). Thus, a content change in an asset file for a given webpage would result in a change to its
3 fingerprint, its URI, and a subsequent change to the content of any static webpage base files
4 referencing that changed asset file for that webpage.

5 38. On information and belief, a dynamic webpage base file generated for a webpage of
6 Defendant webpages in response to one request from a user could be the same as it was when it was
7 generated in response to a prior request from that or another user. However, on information and belief,
8 this would not be the case if any of the asset files referenced in the webpage base file had changed
9 between the time of the two requests and the URIs of the changed asset files included fingerprints as
10 described above.

11 39. On information and belief, when an asset file's content was changed, a new fingerprint
12 was generated and included in the filename, and its URI was thus changed accordingly, resulting in a
13 content change to any webpage base file or other asset file that referenced that URI. This, in turn,
14 caused a new and different ETag being generated for such webpage base file or other asset file that
15 referenced that URI.

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

24 41. On information and belief, Defendant contracted with Amazon to use Amazon's S3
25 system to store and serve at least some of Defendant's CBI ETag files ("S3 asset files") on its behalf.
26 On information and belief, once Defendant's S3 asset files were compiled and are complete, Defendant
27 uploaded them to an Amazon S3 server as objects. On information and belief, such objects comprised
28 a sequence of bits and, upon upload, an associated ETag value was generated by the S3 system on

1 behalf of Defendant by applying a hash function to the sequence of bits, wherein any two S3 asset
2 files comprising identical sequences of bits had identical associated ETag values. On information and
3 belief, in this way, Defendant generated the associated ETag values for its CBI ETag asset files that
4 were S3 asset files. On information and belief, the S3 server for each S3 asset file served the S3 asset
5 file with the its associated ETag value to HTTP GET requests for the S3 asset file.

6 42. On information and belief, when Defendant created a webpage base file for a webpage,
7 whether dynamic or static, that webpage base file included a sequence of bits and an associated ETag
8 value was generated by Defendant by applying a hash function to the sequence of bits; wherein any
9 two webpage base files comprising identical sequences of bits had identical associated ETag values.
10 Thus, on information and belief, when a webpage base file's content was changed and a new associated
11 ETag value was generated by Defendant, it thereafter instructed the respective service by intermediate
12 cache servers or use by endpoint caches such as browser caches to no longer use the previous cached
13 webpage base file's content. Conversely, when the webpage base file content had not changed and
14 thus its ETag was unchanged, the cached asset files with fingerprints in their URIs referenced in the
15 webpage base file had not changed and were still valid to use.

16 43. On information and belief, when an intermediate cache server or a browser requested
17 a webpage from the Defendant for the first time, it sent an HTTP GET request with the webpage's
18 URI and Defendant's origin server or an upstream cache server responded by sending an HTTP 200
19 (OK) response message containing the webpage base file, along with its respective associated ETag.
20 On information and belief, a browser then sent individual HTTP GET requests, each with an asset
21 file's URI that was referenced in the webpage base file, and the asset files' origin servers or
22 intermediate cache servers responded by sending individual HTTP 200 responses containing the
23 requested asset files, along with, if available, their respective associated ETags. On information and
24 belief, upon receipt of the HTTP 200 responses, the intermediate cache server or browser cached the
25 webpage base file and asset files with their associated URI and associated ETag values and the browser
26 used them in rendering the requested web page of the Defendant. On information and belief, the origin
27 servers, intermediate cache servers, and browser caches were caused to maintain databases/tables
28

1 which mapped the URIs of webpage base files and asset files to their respective responses and, if
2 applicable, associated cache-control headers and ETags.

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

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

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

23 47. On information and belief, for a webpage base file or an asset file stored in the
24 browser’s cache with an ETag, and based on the cache-control headers received in the original
25 response, the browser sent a conditional GET request with an If-None-Match header using the
26 associated ETag value and the URI for the webpage base file or asset file so as to be notified whether
27 the browser still had Defendant’s authority to render the webpage with its locally cached webpage
28

1 base file or asset file. In other words, whether the cached content was still valid for use in rendering
2 Defendant's webpage.

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

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

18 50. On information and belief, if the webpage base file's or asset file's associated ETag
19 sent by the browser in the conditional GET If-None-Match request did not match the associated ETag
20 maintained at the responding server (or other intermediate cache servers further upstream or the origin
21 server) for that URI, the responding server sent back an HTTP 200 response along with the new
22 webpage base file or asset file and its new ETag value. The HTTP 200 response indicated to the
23 browser that it was not authorized to use (or serve, in the case of an intermediate cache server receiving
24 the HTTP 200 response) the previously cached webpage base file or asset file. In response to receiving
25 the HTTP 200 response, the browser (or intermediate cache server) was instructed to update its
26 respective cache with the new webpage base file or asset file and associated ETag. The browser
27 subsequently used the new webpage base file (and the asset file URIs contained therein) or asset file
28 to render the webpage.

1 origin servers, intermediate cache servers and endpoint caches used by browsers rendering
2 Defendant's webpages.

3 57. Claim 10 then recites the act of "obtaining a name for a data file, the name being based
4 at least in part on a given function of the data, wherein the data used by the function comprises the
5 contents of the particular file." As set forth above, on information and belief, Defendant generated or
6 otherwise obtained ETags for its webpage base file and asset files used to render its webpages using a
7 hash function, wherein the ETags were based on the contents of the particular files. Moreover,
8 Defendant caused the intermediate caches servers and endpoint caches to obtain the ETags in HTTP
9 200 responses sent from Defendant's origin servers. On information and belief, Defendant caused
10 intermediate cache servers and its origin servers to obtain ETags in conditional GET messages from
11 endpoint and intermediate caches, as described *supra*.

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

19 59. Claim 10 then recites the act of "determining whether a copy of the data file that is
20 present on a at least one of said computers is an unauthorized copy or an unlicensed copy of the data
21 file." On information and belief, as set forth above, if there was a match, the origin or intermediate
22 cache server determined that the copy of the file present at the downstream intermediate cache server
23 and/or the endpoint cache was an authorized or licensed copy of the data file. Conversely, if there was
24 no match, it determined that the copy of the file present at the downstream intermediate cache server
25 and/or the endpoint cache was an unauthorized copy of the data file. Likewise, if the browser
26 determined that it had a file with a matching URI, the browser determined that it was still authorized
27 to use that file.

28

1 being based at least in part on a function of at least some of the data comprising the particular data
2 item, wherein the function comprises a message digest function or a hash function, and wherein two
3 identical data items will have the same content-dependent name.” On information and belief, as set
4 forth above, Defendant has caused downstream intermediate cache servers and endpoint caches to
5 send conditional GET requests with If-None-Match headers containing ETags that are fielded by
6 upstream cache or origin servers. On information and belief, the ETags were content-dependent names
7 for a data item based on hashing the data item’s contents; and when the file’s content changed a new
8 content-dependent name was determined. On information and belief, in Defendant’s method, a first
9 computer, such as the intermediate cache server or origin server, received such conditional GET
10 requests from a second computer, such as a user browser or other intermediate cache server, regarding
11 data items, such as webpage or asset files, the requests including ETags associated with the respective
12 data items.

13 66. Claim 20 then recites “based at least in part on said content-dependent name of said
14 particular data item, the first device (A) permitting the content to be provided to or accessed by the at
15 least one other computer if it is not determined that the content is unauthorized or unlicensed,
16 otherwise, (B) if it is determined that the content is unauthorized or unlicensed, not permitting the
17 content to be provided to or accessed by the at least one other computer.” On information and belief,
18 the first computer, such as an upstream intermediate cache server or origin server, maintained a
19 plurality of ETags associated with Defendant’s asset and webpage base files. On information and
20 belief, the ETag in a request and the ETag maintained by the first computer for the particular data item
21 sought by the request were compared to determine whether the associated content present at the
22 downstream computer was still authorized to be used/served or whether new authorized content must
23 be provided thereto. If it was determined that the data item corresponding to the received ETag was
24 still authorized to be used, the first computer sent back an HTTP 304 response authorizing the
25 downstream cache server or end-user cache to access the file content already present in order to serve
26 it or to use it to render the webpage. On information and belief, if it had been determined that the data
27 item corresponding to received E-tag was no longer authorized, the first computer sent back an HTTP
28 200 response which indicated to the downstream cache server or end-user cache that was not

1 authorized to access the old content and must access the new authorized file content contained in the
2 HTTP 200 response to serve it or to use it to render the webpage.

3 67. For a further example, claim 69 covers a “system operable in a network of computers,
4 the system comprising hardware including at least a processor, and software, in combination with said
5 hardware.” On information and belief, Defendant has controlled the distribution of its website content
6 across a system that included a network of computers, such as its production servers as well as origin
7 servers, intermediate cache servers, and endpoint caches, all comprising hardware including a
8 processor. On information and belief, Defendant has utilized software, in combination with such
9 hardware, such as a web development framework, software utilized in implementing the HTTP web
10 protocol, and software used on host servers that Defendant used to serve its content.

11 68. Claim 69 then recites the system “(a) to receive at a first computer, from a second
12 computer, a request regarding a data item, said request including at least a content-dependent name
13 for the data item, the content-dependent name being based at least in part on a function of the data in
14 the data item, wherein the data used by the function to determine the content-dependent name
15 comprises at least some of the contents of the data item, wherein the function that was used is a
16 message digest function or a hash function, and wherein two identical data items will have the same
17 content-dependent name.” On information and belief, as set forth above, Defendant has caused
18 downstream intermediate cache servers and endpoint caches to send conditional GET requests with
19 URIs including fingerprints that are fielded by upstream cache or origin servers. On information and
20 belief, the URIs including fingerprints were content-dependent names for a data item calculated by
21 hashing the file’s contents; and when the file’s content changed a new content-dependent name was
22 determined. On information and belief, in Defendant’s system, a first computer, such as the
23 intermediate cache server or origin server, received such conditional GET requests from a second
24 computer, such as a user browser, regarding data items, such as asset files, using content-dependent
25 names such as URIs including fingerprints associated with the data items.

26 69. Claim 69 then recites “(b) in response to said request: (i) to cause the content-dependent
27 name of the data item to be compared to a plurality of values; and (ii) to determine if access to the data
28 item is authorized or unauthorized based on whether or not the content-dependent name corresponds

1 to at least one of said plurality of values, and (iii) based on whether or not it is determined that access
2 to the data item is authorized or unauthorized, to allow the data item to be provided to or accessed by
3 the second computer if it is not determined that access to the data item is unauthorized.” On
4 information and belief, the first computer, such as an upstream intermediate cache server or origin
5 server, maintained a plurality of URI values associated with Defendant’s asset and webpage base files;
6 compared the URI value received in a conditional GET request from the second (downstream)
7 computer to that plurality of URI values; that comparison allowed the first computer to determine
8 whether the content-dependent name in the request corresponded to one of the plurality of stored URI
9 values and to determine whether access to the data item was still authorized or not. On information
10 and belief, in particular when there was a match, the first computer determined the associated content
11 present at the downstream computer was still authorized to be used/served or whether new authorized
12 content must be provided thereto. If it was determined that the data item corresponding to the received
13 URI including a fingerprint was still authorized to be used, the first computer has sent back an HTTP
14 304 response authorizing the downstream cache server or end-user cache to access the file content
15 already present in order to serve it or to use it to render the webpage.

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

19
20 **THIRD CLAIM FOR RELIEF**

21 **INFRINGEMENT OF U.S. PATENT NO. 7,945,544**

22 71. PersonalWeb repeats and realleges paragraphs 1–52, as if the same were fully stated
23 herein.

24 72. On May 17, 2011, United States Patent No. 7,945,544 (the “’544 patent”) was duly and
25 legally issued for an invention entitled “Similarity-Based Access Control of Data in a Data Processing
26 System.” PersonalWeb has an ownership interest in the ’544 patent by assignment, including the
27 exclusive right to enforce the ’544 patent within the PersonalWeb Patent Field, and continues to hold
28 that ownership interest in the ’544 patent.

1 73. Defendant has infringed at least claims 46, 48, 52, and 55 of the '544 patent by its
2 manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the
3 distribution of its webpage content in the manner described herein. Defendant's infringement is literal
4 and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '544 patent
5 pursuant to 35 U.S.C. § 271.

6 74. For example, claim 46 covers a claimed "computer-implemented method." On
7 information and belief, Defendant uses the claimed computer implemented method by using a system
8 of notifications and authorizations to locate and control the distribution of data items, such as various
9 webpage base files and asset files, necessary to render its webpages.

10 75. Claim 46 then recites the act of "(A) for each particular file of a plurality of files:
11 (a2) determining a particular digital key for the particular file, wherein the particular file comprises a
12 first one or more parts." On information and belief, each of Defendant's webpages comprises one or
13 more asset files and has an associated webpage base file, the webpage base file containing the URIs
14 having fingerprints of a plurality of asset files comprising the webpage, and once the webpage base
15 files and asset files are compiled and complete, Defendant stores them on a host system. On
16 information and belief, the webpage base file's associated ETag value is generated by applying a hash
17 algorithm to the webpage base file's contents. On information and belief, whenever a new webpage
18 base file is generated or the webpage base file's content changes, Defendant caused an ETag to be
19 determined and associated to the webpage base file.

20 76. Claim 46 then recites "each part of said first one or more parts having a corresponding
21 part value, the part value of each specific part of said first one or more parts being based on a first
22 function of the contents of the specific part, wherein two identical parts will have the same part value
23 as determined by the first function, and wherein the particular digital key for the particular file is
24 determined using a second function of the one or more of part values of said first one or more parts."
25 On information and belief, prior to various asset files being stored on a host system, a fingerprint is
26 generated for each of these asset files by applying a hash function to the asset file's contents and the
27 fingerprints are inserted into the URIs for the respective asset files. On information and belief, the
28 webpage's ETag value is generated by applying a second hash function to the webpage base file's

1 contents, which include the URIs of one or more of the asset files which comprise the webpage's
2 contents. On information and belief, because the respective asset files' URIs include the fingerprints
3 of their content, the webpage's ETag value will change and a new associated ETag value is generated
4 to represent the webpage's content, when the content changes and two identical webpages having the
5 identical content represented by their webpage base file will have the same ETag value.

6 77. Claim 46 then recites the act of "(a2) adding the particular digital key of the particular
7 file to a database, the database including a mapping from digital keys of files to information about the
8 corresponding files." On information and belief, Defendant caused the origin server, intermediate
9 caches and endpoint caches to maintain databases/tables which mapped the ETag of each webpage's
10 webpage base file to its URI, and information about the corresponding webpage, such as, for example,
11 information from cache-control headers for the webpage.

12 78. Claim 46 then recites "(B) determining a search key based on search criteria, wherein
13 the search criteria comprise a second one or more parts, each of said second one or more parts of said
14 search criteria having a corresponding part value, the part value of each specific part of said second
15 one or more parts being based on the first function of the contents of the specific part, and wherein the
16 search key is determined using the second function of the one or more of part values of said second
17 one or more parts." On information and belief, when a downstream intermediate cache server or a
18 browser again requested a webpage of Defendant, Defendant caused it to send a conditional GET
19 request with an If-None-Match header with the webpage's associated ETag value. On information
20 and belief, the received ETag value was determined using the second hash function of the webpage's
21 webpage base file, which included URIs including fingerprints for one or more of the asset files which
22 comprised the webpage's contents.

23 79. Claim 46 then recites "(C) attempting to match the search key with a digital key in the
24 database." On information and belief, when the responding server received the webpage's ETag value
25 in a conditional GET request with an If-None-Match header, it compared the received ETag with the
26 ETag it has maintained in a database/table corresponding to the URI of the webpage's webpage base
27 file to determine if there is matching value for that webpage.
28

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

4 86. Claim 166 then recites “(A) for a particular data item in a set of data items, said
5 particular data item comprising a corresponding particular sequence of bits.” On information and
6 belief, Defendant’s system has controlled the distribution of webpage base files and asset files
7 necessary to render its webpages which represent particular data items, and each of these files comprise
8 a corresponding sequence of bits.

9 87. Claim 166 then recites that for the particular data item to “(a1) determine one or more
10 content-dependent digital identifiers for said particular data item, each said content-dependent digital
11 identifier being based at least in part on a given function of at least some of the bits in the particular
12 sequence of bits of the particular data item, wherein two identical data items will have the same digital
13 identifiers as determined using said given function.” On information and belief, Defendant’s system
14 has applied hash functions to each of various Defendant’s webpage base files to all of the bits of the
15 file’s content to determine a fingerprint, an ETag, or both for the file’s content; whereby two identical
16 data items have the same ETag values and the same fingerprint values. On information and belief,
17 fingerprints were included in files’ URI and ETag values were associated with files’ URIs.

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

27 89. On information and belief, Defendant’s system has included one or more web servers
28 with databases containing ETag values associated with the URIs for various of the webpage base files

1 and asset files necessary to render its webpages; moreover, Defendant’s system has used a system of
2 conditional GET requests with If-None-Match headers and HTTP 304 and HTTP 200 responses
3 containing the ETags, as described more particularly *supra*, to ensure that downstream caches only
4 access authorized file content to either serve that file content further downstream or to use it to render
5 Defendant’s webpages. On information and belief, in particular, as more fully described *supra*, the
6 system compared the ETag received in a given conditional GET request with the ETags contained in
7 the database to selectively determine whether the requesting computer could access the file content it
8 already had or must access newly received authorized content.

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

12
13 **PRAYER FOR RELIEF**

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

16 a) Declaration that Defendant has infringed U.S. Patent Nos. 6,928,442, 7,802,310,
17 7,945,544, and 8,099,420 as described in this action;

18 b) Awarding the damages arising out of Defendant’s infringement of U.S. Patent Nos.
19 6,928,442, 7,802,310, 7,945,544, and 8,099,420, together with pre-judgment and post-judgment
20 interest, in an amount according to proof;

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

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

25
26
27
28

1 Respectfully submitted,

2 Dated: October 3, 2018

STUBBS, ALDERTON & MARKILES, LLP

3

4

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

5

6

7

8

9

Dated: October 3, 2018

MACEIKO IP

10

11

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,

12

13

14

15

16

Dated: October 3, 2018

DAVID D. WIER

17

18

19

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

20

21

22

23

24

25

26

27

28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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 3, 2018

STUBBS, ALDERTON & MARKILES, LLP

By: /s/ Michael A. Sherman

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

Dated: October 3, 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 3, 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