

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., 20<sup>th</sup> 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

15 IN RE PERSONALWEB TECHNOLOGIES,  
 16 LLC, ET AL., PATENT LITIGATION

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

**FIRST AMENDED COMPLAINT**

**DEMAND FOR JURY TRIAL**

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

**Case No.: 5:18-cv-05202-BLF**

22 Plaintiffs,

23 v.

24 SHAREFILE, LLC, a Delaware limited liability  
 company,

25 Defendant.  
 26  
 27  
 28

1 Plaintiff PersonalWeb Technologies, LLC (“Plaintiff” or “PersonalWeb”) files this First  
2 Amended Complaint (“Complaint”) for patent infringement against Defendants ShareFile, LLC.  
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.

**THE PARTIES**

1  
2 4. Plaintiff PersonalWeb Technologies, LLC is a limited liability company duly organized  
3 and existing under the laws of Texas with its principal place of business at 112 E. Line Street, Suite  
4 204, Tyler, TX 75702.

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

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

11 7. Defendant ShareFile LLC is, upon information and belief, a Delaware limited liability  
12 company having a principal place of business or regular and established place of business at 120 S.  
13 West Street, Raleigh, North Carolina 27603 or 851 West Cypress Creek Road, Fort Lauderdale,  
14 Florida 33309.

15 8. On information and belief, Defendant ShareFile LLC was acquired by Citrix Systems,  
16 Inc. in or around October 2011, and ShareFile LLC is a subsidiary of Citrix Systems, Inc. Citrix  
17 Systems, Inc. acquired RightSignature LLC in or around October 2014. On information and belief,  
18 RightSignature LLC merged into ShareFile LLC in or around October 2017. Prior to the  
19 aforementioned acquisitions and mergers, RightSignature LLC owned and/or operated the website  
20 rightsignature.com.

21  
22 **JURISDICTION AND VENUE**

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

25 10. Venue is proper in this federal district pursuant to 28 U.S.C. §§ 1391(b)–(c) and  
26 1400(b) because Defendant is incorporated in the State of Delaware and thus resides in such District  
27  
28

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

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

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

12  
13 **PERSONALWEB BACKGROUND**

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

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

22 16. Ronald Lachman and David Farber, the inventors of the Patents-in-Suit, recognized  
23 that the conventional approach for naming, locating, and accessing data in computer networks could  
24 not keep pace with ever-expanding, global data processing networks. New distributed storage systems  
25 use files that are stored across different devices in dispersed geographic locations. These different  
26 locations could use dissimilar conventions for identifying storage devices and data partitions.  
27 Likewise, different users could give identical names to different files or parts of files—or unknowingly  
28 give different names to identical files. No solution existed to ensure that identical file names referred

1 to the same data, and conversely, that different file names referred to different data. As a result,  
2 expanding networks could not only become clogged with duplicate data, they also made locating and  
3 controlling access to stored data more difficult.

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

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

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

24 20. Using a True Name, Lachman and Farber conceived various data structures and  
25 methods for managing data (each data item correlated with a single True Name) within a network—  
26 no matter the complexity of the data or the network. These data structures provide a key-map  
27 organization, allowing for a rapid identification of any particular data item anywhere in a network by  
28 comparing a True Name for the data item against other True Names for data items already in the

1 network. In operation, managing data using True Names allows a user to determine the location of  
2 any data in a network, determine whether access is authorized, and to selectively provide access to  
3 specific content not possible using the conventional naming arts.

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

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

### 13 14 **GENERAL BACKGROUND**

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

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

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

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

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

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

27          29.     Responses to HTTP requests may include header elements (control elements) and a  
28 body (the “object” that was requested). Under HTTP, web servers can include a “cache-control”

1 header with a response that includes a webpage or asset file. A “cache-control” header includes one  
2 or more directives that instruct browsers and intermediate server caches (“intermediate caches”) as to  
3 whether and for how long the file (object) included in the response may be cached or under what  
4 circumstances and under what conditions the cached content may be used. HTTP also provides for  
5 including other headers in responses that provide similar types of instructions to browsers and  
6 intermediate caches. Collectively, these other headers and directives in a “cache-control” header are  
7 referred to herein as “cache-control headers.”

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

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

### 19 20 **DEFENDANT’S BACKGROUND**

21 32. On information and belief, Defendant has operated a website located at  
22 **rightsignature.com**, and has done so since before expiration of the last to expire of the Patents-in-  
23 Suit, which has operated to provide authorized webpage content to its users in the manner herein  
24 described.<sup>1</sup>

25 33. On information and belief, Defendant’s web servers utilized a system of notifications  
26 and authorizations to control the distribution of content, *e.g.*, what webpage content may be served

27 \_\_\_\_\_  
28 <sup>1</sup> 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.



1 from web servers and intermediate caches and what cached webpage content a browser is re-authorized  
2 to use to render Defendant's webpage(s).

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

7 35. On information and belief, Defendant's system and its associated method of providing  
8 webpage content also inserted fingerprints generated based on the content of asset files into the  
9 filenames of asset files required to render various webpages of the Defendant.

10 36. On information and belief, Defendant's system and associated method used these  
11 ETags and fingerprints to instruct both the intermediate cache servers and the endpoint caches at  
12 browsers to verify whether they were still authorized to reuse the previously cached webpage base  
13 files of Defendant and to instruct them to obtain newly authorized content in rendering Defendant's  
14 webpage when that content had changed. In other words, whether the previously cached content was  
15 still considered valid for use by the Defendant website operator.

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

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

1           39.     On information and belief, Defendant's website used a web application framework to  
2 develop and compile various webpages of the Defendant, including asset files that were used in  
3 rendering the webpages, and to generate fingerprints of the contents of asset files. On information and  
4 belief, the fingerprints of individual asset files that were part of the webpage's content were included  
5 in the respective filenames of the individual asset files. On information and belief, the modified  
6 filenames were then used as part of the URI used to access the individual asset files over the Internet.  
7 On information and belief, when an asset file's content was changed, a new fingerprint was generated  
8 and included in the filename, its URI thus being changed accordingly.

9           40.     On information and belief, the asset file fingerprint was generated with a hash function  
10 and used to identify content changes. Furthermore, on information and belief, asset file URIs (with  
11 respective fingerprints) were included in webpage base files or other asset files contained references  
12 to other asset files. On information and belief, static webpage base files, if any, were recompiled when  
13 any URI of a referenced asset file was changed (due to the fingerprint of the referenced asset file  
14 changing). Thus, a content change in an asset file for a given webpage would result in a change to its  
15 fingerprint, its URI, and a subsequent change to the content of any static webpage base files  
16 referencing that changed asset file for that webpage.

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

23           42.     On information and belief, when an asset file's content was changed, a new fingerprint  
24 was generated and included in the filename, and its URI was thus changed accordingly, resulting in a  
25 content change to any webpage base file or other asset file that referenced that URI. This, in turn,  
26 caused a new and different ETag being generated for such webpage base file or other asset file that  
27 referenced that URI.

28

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

9           44.     On information and belief, Defendant contracted with Amazon to use Amazon’s S3  
10 system to store and serve at least some of Defendant’s CBI ETag files (“S3 asset files”) on its behalf.  
11 On information and belief, once Defendant’s S3 asset files were compiled and are complete, Defendant  
12 uploaded them to an Amazon S3 server as objects. On information and belief, such objects comprised  
13 a sequence of bits and, upon upload, an associated ETag value was generated by the S3 system on  
14 behalf of Defendant by applying a hash function to the sequence of bits, wherein any two S3 asset  
15 files comprising identical sequences of bits had identical associated ETag values. On information and  
16 belief, in this way, Defendant generated the associated ETag values for its CBI ETag asset files that  
17 were S3 asset files. On information and belief, the S3 server for each S3 asset file served the S3 asset  
18 file with the its associated ETag value to HTTP GET requests for the S3 asset file.

19           45.     On information and belief, when Defendant created a webpage base file for a webpage,  
20 whether dynamic or static, that webpage base file included a sequence of bits and an associated ETag  
21 value was generated by Defendant by applying a hash function to the sequence of bits; wherein any  
22 two webpage base files comprising identical sequences of bits had identical associated ETag values.  
23 Thus, on information and belief, when a webpage base file’s content was changed and a new associated  
24 ETag value was generated by Defendant, it thereafter instructed the respective service by intermediate  
25 cache servers or use by endpoint caches such as browser caches to no longer use the previous cached  
26 webpage base file’s content. Conversely, when the webpage base file content had not changed and  
27 thus its ETag was unchanged, the cached asset files with fingerprints in their URIs referenced in the  
28 webpage base file had not changed and were still valid to use.

1           46.     On information and belief, when an intermediate cache server or a browser requested  
2 a webpage from the Defendant for the first time, it sent an HTTP GET request with the webpage's  
3 URI and Defendant's origin server or an upstream cache server responded by sending an HTTP 200  
4 (OK) response message containing the webpage base file, along with its respective associated ETag.  
5 On information and belief, a browser then sent individual HTTP GET requests, each with an asset  
6 file's URI that was referenced in the webpage base file, and the asset files' origin servers or  
7 intermediate cache servers responded by sending individual HTTP 200 responses containing the  
8 requested asset files, along with, if available, their respective associated ETags. On information and  
9 belief, upon receipt of the HTTP 200 responses, the intermediate cache server or browser cached the  
10 webpage base file and asset files with their associated URI and associated ETag values and the browser  
11 used them in rendering the requested web page of the Defendant. On information and belief, the origin  
12 servers, intermediate cache servers, and browser caches were caused to maintain databases/tables  
13 which mapped the URIs of webpage base files and asset files to their respective responses and, if  
14 applicable, associated cache-control headers and ETags.

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

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

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

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

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

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

1           53.     On information and belief, if the webpage base file's or asset file's associated ETag  
2 sent by the browser in the conditional GET If-None-Match request did not match the associated ETag  
3 maintained at the responding server (or other intermediate cache servers further upstream or the origin  
4 server) for that URI, the responding server sent back an HTTP 200 response along with the new  
5 webpage base file or asset file and its new ETag value. The HTTP 200 response indicated to the  
6 browser that it was not authorized to use (or serve, in the case of an intermediate cache server receiving  
7 the HTTP 200 response) the previously cached webpage base file or asset file. In response to receiving  
8 the HTTP 200 response, the browser (or intermediate cache server) was instructed to update its  
9 respective cache with the new webpage base file or asset file and associated ETag. The browser  
10 subsequently used the new webpage base file (and the asset file URIs contained therein) or asset file  
11 to render the webpage.

12           54.     Exhibit 1 to the complaint lists specific examples of files that were, on information and  
13 belief, served by or on behalf of Defendant during the relevant time period. The examples in Exhibit  
14 1 include: a webpage base file served with a content-based ETag for the webpage base file; an asset  
15 file served by S3 with a content-based ETag generated by S3 for that asset file; and an asset file  
16 referenced by a URI with a fingerprint of the asset file contained into the URI.

17           55.     On information and belief, in this manner, Defendant used (1) ETag values and (2)  
18 asset files referenced by URIs with fingerprints based on the asset files' content to control the behavior  
19 of downstream intermediate cache servers and browser caches to assure that they only accessed and  
20 used Defendant's latest authorized webpage content to serve or to render its webpages.

21  
22                                   **FIRST CLAIM FOR RELIEF**

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

24           56.     PersonalWeb repeats and realleges paragraphs 1–55, as if the same were fully stated  
25 herein.

26           57.     On August 9, 2005, United States Patent No. 6,928,442 (the “'442 patent”) was duly  
27 and legally issued for an invention entitled “Enforcement and Policing of Licensed Content Using  
28 Content-Based Identifiers.” PersonalWeb has an ownership interest in the '442 patent by assignment,

1 including the exclusive right to enforce the '442 patent within the PersonalWeb Patent Field, and  
2 continues to hold that ownership interest in the '442 patent. A true and correct copy of the '442 patent  
3 is attached as Exhibit 2.

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

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

15 60. Claim 10 then recites the act of "obtaining a name for a data file, the name being based  
16 at least in part on a given function of the data, wherein the data used by the function comprises the  
17 contents of the particular file." As set forth above, on information and belief, Defendant generated or  
18 otherwise obtained ETags for its webpage base file and asset files used to render its webpages using a  
19 hash function, wherein the ETags were based on the contents of the particular files. Moreover,  
20 Defendant caused the intermediate caches servers and endpoint caches to obtain the ETags in HTTP  
21 200 responses sent from Defendant's origin servers. On information and belief, Defendant caused  
22 intermediate cache servers and its origin servers to obtain ETags in conditional GET messages from  
23 endpoint and intermediate caches, as described *supra*.

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

1 GET and to compare the ETag in the conditional GET to the ETag for that URI and determine whether  
2 a copy of the content having that ETag is present.

3 62. Claim 10 then recites the act of “determining whether a copy of the data file that is  
4 present on a at least one of said computers is an unauthorized copy or an unlicensed copy of the data  
5 file.” On information and belief, as set forth above, if there was a match, the origin or intermediate  
6 cache server determined that the copy of the file present at the downstream intermediate cache server  
7 and/or the endpoint cache was an authorized or licensed copy of the data file. Conversely, if there was  
8 no match, it determined that the copy of the file present at the downstream intermediate cache server  
9 and/or the endpoint cache was an unauthorized copy of the data file. Likewise, if the browser  
10 determined that it had a file with a matching URI, the browser determined that it was still authorized  
11 to use that file.

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

## 15 **SECOND CLAIM FOR RELIEF**

### 16 **INFRINGEMENT OF U.S. PATENT NO. 7,802,310**

17  
18 64. PersonalWeb repeats and realleges paragraphs 1–55, as if the same were fully stated  
19 herein.

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

26 66. Defendant has infringed at least claims 20 and 69 of the ’310 patent by its manufacture,  
27 use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution  
28 of its webpage content in the manner described herein. Defendant’s infringement is literal and/or



1 under the doctrine of equivalents and Defendant is liable for its infringement of the '310 patent  
2 pursuant to 35 U.S.C. § 271.

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

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

25         69. Claim 20 then recites “based at least in part on said content-dependent name of said  
26 particular data item, the first device (A) permitting the content to be provided to or accessed by the at  
27 least one other computer if it is not determined that the content is unauthorized or unlicensed,  
28 otherwise, (B) if it is determined that the content is unauthorized or unlicensed, not permitting the

1 content to be provided to or accessed by the at least one other computer.” On information and belief,  
2 the first computer, such as an upstream intermediate cache server or origin server, maintained a  
3 plurality of ETags associated with Defendant’s asset and webpage base files. On information and  
4 belief, the ETag in a request and the ETag maintained by the first computer for the particular data item  
5 sought by the request were compared to determine whether the associated content present at the  
6 downstream computer was still authorized to be used/served or whether new authorized content must  
7 be provided thereto. If it was determined that the data item corresponding to the received ETag was  
8 still authorized to be used, the first computer sent back an HTTP 304 response authorizing the  
9 downstream cache server or end-user cache to access the file content already present in order to serve  
10 it or to use it to render the webpage. On information and belief, if it had been determined that the data  
11 item corresponding to received E-tag was no longer authorized, the first computer sent back an HTTP  
12 200 response which indicated to the downstream cache server or end-user cache that was not  
13 authorized to access the old content and must access the new authorized file content contained in the  
14 HTTP 200 response to serve it or to use it to render the webpage.

15 70. For a further example, claim 69 covers a “system operable in a network of computers,  
16 the system comprising hardware including at least a processor, and software, in combination with said  
17 hardware.” On information and belief, Defendant has controlled the distribution of its website content  
18 across a system that included a network of computers, such as its production servers as well as origin  
19 servers, intermediate cache servers, and endpoint caches, all comprising hardware including a  
20 processor. On information and belief, Defendant has utilized software, in combination with such  
21 hardware, such as a web development framework, software utilized in implementing the HTTP web  
22 protocol, and software used on host servers that Defendant used to serve its content.

23 71. Claim 69 then recites the system “(a) to receive at a first computer, from a second  
24 computer, a request regarding a data item, said request including at least a content-dependent name  
25 for the data item, the content-dependent name being based at least in part on a function of the data in  
26 the data item, wherein the data used by the function to determine the content-dependent name  
27 comprises at least some of the contents of the data item, wherein the function that was used is a  
28 message digest function or a hash function, and wherein two identical data items will have the same

1 content-dependent name.” On information and belief, as set forth above, Defendant has caused  
2 downstream intermediate cache servers and endpoint caches to send conditional GET requests with  
3 URIs including fingerprints that are fielded by upstream cache or origin servers. On information and  
4 belief, the URIs including fingerprints were content-dependent names for a data item calculated by  
5 hashing the file’s contents; and when the file’s content changed a new content-dependent name was  
6 determined. On information and belief, in Defendant’s system, a first computer, such as the  
7 intermediate cache server or origin server, received such conditional GET requests from a second  
8 computer, such as a user browser, regarding data items, such as asset files, using content-dependent  
9 names such as URIs including fingerprints associated with the data items.

10 72. Claim 69 then recites “(b) in response to said request: (i) to cause the content-dependent  
11 name of the data item to be compared to a plurality of values; and (ii) to determine if access to the data  
12 item is authorized or unauthorized based on whether or not the content-dependent name corresponds  
13 to at least one of said plurality of values, and (iii) based on whether or not it is determined that access  
14 to the data item is authorized or unauthorized, to allow the data item to be provided to or accessed by  
15 the second computer if it is not determined that access to the data item is unauthorized.” On  
16 information and belief, the first computer, such as an upstream intermediate cache server or origin  
17 server, maintained a plurality of URI values associated with Defendant’s asset and webpage base files;  
18 compared the URI value received in a conditional GET request from the second (downstream)  
19 computer to that plurality of URI values; that comparison allowed the first computer to determine  
20 whether the content-dependent name in the request corresponded to one of the plurality of stored URI  
21 values and to determine whether access to the data item was still authorized or not. On information  
22 and belief, in particular when there was a match, the first computer determined the associated content  
23 present at the downstream computer was still authorized to be used/served or whether new authorized  
24 content must be provided thereto. If it was determined that the data item corresponding to the received  
25 URI including a fingerprint was still authorized to be used, the first computer has sent back an HTTP  
26 304 response authorizing the downstream cache server or end-user cache to access the file content  
27 already present in order to serve it or to use it to render the webpage.

28

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

4  
5 **THIRD CLAIM FOR RELIEF**

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

7 74. PersonalWeb repeats and realleges paragraphs 1–55, as if the same were fully stated  
8 herein.

9 75. On May 17, 2011, United States Patent No. 7,945,544 (the "'544 patent") was duly and  
10 legally issued for an invention entitled "Similarity-Based Access Control of Data in a Data Processing  
11 System." PersonalWeb has an ownership interest in the '544 patent by assignment, including the  
12 exclusive right to enforce the '544 patent within the PersonalWeb Patent Field, and continues to hold  
13 that ownership interest in the '544 patent. A true and correct copy of the '544 patent is attached as  
14 Exhibit 4.

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

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

24 78. Claim 46 then recites the act of "(A) for each particular file of a plurality of files:  
25 (a2) determining a particular digital key for the particular file, wherein the particular file comprises a  
26 first one or more parts." On information and belief, each of Defendant's webpages comprises one or  
27 more asset files and has an associated webpage base file, the webpage base file containing the URIs  
28 having fingerprints of a plurality of asset files comprising the webpage, and once the webpage base

1 files and asset files are compiled and complete, Defendant stores them on a host system. On  
2 information and belief, the webpage base file's associated ETag value is generated by applying a hash  
3 algorithm to the webpage base file's contents. On information and belief, whenever a new webpage  
4 base file is generated or the webpage base file's content changes, Defendant caused an ETag to be  
5 determined and associated to the webpage base file.

6 79. Claim 46 then recites "each part of said first one or more parts having a corresponding  
7 part value, the part value of each specific part of said first one or more parts being based on a first  
8 function of the contents of the specific part, wherein two identical parts will have the same part value  
9 as determined by the first function, and wherein the particular digital key for the particular file is  
10 determined using a second function of the one or more of part values of said first one or more parts."  
11 On information and belief, prior to various asset files being stored on a host system, a fingerprint is  
12 generated for each of these asset files by applying a hash function to the asset file's contents and the  
13 fingerprints are inserted into the URIs for the respective asset files. On information and belief, the  
14 webpage's ETag value is generated by applying a second hash function to the webpage base file's  
15 contents, which include the URIs of one or more of the asset files which comprise the webpage's  
16 contents. On information and belief, because the respective asset files' URIs include the fingerprints  
17 of their content, the webpage's ETag value will change and a new associated ETag value is generated  
18 to represent the webpage's content, when the content changes and two identical webpages having the  
19 identical content represented by their webpage base file will have the same ETag value.

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

26 81. Claim 46 then recites "(B) determining a search key based on search criteria, wherein  
27 the search criteria comprise a second one or more parts, each of said second one or more parts of said  
28 search criteria having a corresponding part value, the part value of each specific part of said second

1 one or more parts being based on the first function of the contents of the specific part, and wherein the  
2 search key is determined using the second function of the one or more of part values of said second  
3 one or more parts.” On information and belief, when a downstream intermediate cache server or a  
4 browser again requested a webpage of Defendant, Defendant caused it to send a conditional GET  
5 request with an If-None-Match header with the webpage’s associated ETag value. On information  
6 and belief, the received ETag value was determined using the second hash function of the webpage’s  
7 webpage base file, which included URIs including fingerprints for one or more of the asset files which  
8 comprised the webpage’s contents.

9 82. Claim 46 then recites “(C) attempting to match the search key with a digital key in the  
10 database.” On information and belief, when the responding server received the webpage’s ETag value  
11 in a conditional GET request with an If-None-Match header, it compared the received ETag with the  
12 ETag it has maintained in a database/table corresponding to the URI of the webpage’s webpage base  
13 file to determine if there is matching value for that webpage.

14 83. Claim 46 then recites “(D) if the search key matches a particular digital key in the  
15 database, providing information about the file corresponding to the particular digital key.” On  
16 information and belief, if the responding server had a matching ETag value for the webpage’s webpage  
17 base file, the responding server sent an HTTP 304 response, which included information about the  
18 corresponding webpage, such as, for example, information from cache-control headers for the  
19 webpage.

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

#### 23 **FOURTH CLAIM FOR RELIEF**

#### 24 **INFRINGEMENT OF U.S. PATENT NO. 8,099,420**

25 85. PersonalWeb repeats and realleges paragraphs 1–55, as if the same were fully stated  
26 herein.  
27  
28

1           86.     On January 17, 2012, United States Patent No. 8,099,420 (the “’420 patent”) was duly  
2 and legally issued for an invention entitled “Accessing Data in a Data Processing System.”  
3 PersonalWeb has an ownership interest in the ’420 patent by assignment, including the exclusive right  
4 to enforce the ’420 patent within the PersonalWeb Patent Field, and continues to hold that ownership  
5 interest in the ’420 patent. A true and correct copy of the ’420 patent is attached as Exhibit 5.

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

11           88.     For example, claim 166 covers a “system comprising hardware, including at least a  
12 processor, and software, in combination with said hardware.” On information and belief, Defendant  
13 has controlled the distribution of its website content across a system that included hardware including  
14 a processor, such as its production servers as well as origin servers, intermediate cache servers, and  
15 endpoint caches; and software, in combination with such hardware, such as a web development  
16 framework, software utilized in implementing the HTTP web protocol, and the software used on host  
17 servers that Defendant used to serve its webpages.

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

23           90.     Claim 166 then recites that for the particular data item to “(a1) determine one or more  
24 content-dependent digital identifiers for said particular data item, each said content-dependent digital  
25 identifier being based at least in part on a given function of at least some of the bits in the particular  
26 sequence of bits of the particular data item, wherein two identical data items will have the same digital  
27 identifiers as determined using said given function.” On information and belief, Defendant’s system  
28 has applied hash functions to each of various Defendant’s webpage base files to all of the bits of the

1 file's content to determine a fingerprint, an ETag, or both for the file's content; whereby two identical  
2 data items have the same ETag values and the same fingerprint values. On information and belief,  
3 fingerprints were included in files' URI and ETag values were associated with files' URIs.

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

13 92. On information and belief, Defendant's system has included one or more web servers  
14 with databases containing ETag values associated with the URIs for various of the webpage base files  
15 and asset files necessary to render its webpages; moreover, Defendant's system has used a system of  
16 conditional GET requests with If-None-Match headers and HTTP 304 and HTTP 200 responses  
17 containing the ETags, as described more particularly *supra*, to ensure that downstream caches only  
18 access authorized file content to either serve that file content further downstream or to use it to render  
19 Defendant's webpages. On information and belief, in particular, as more fully described *supra*, the  
20 system compared the ETag received in a given conditional GET request with the ETags contained in  
21 the database to selectively determine whether the requesting computer could access the file content it  
22 already had or must access newly received authorized content.

23 93. Defendant's acts of infringement have caused damage to PersonalWeb and  
24 PersonalWeb is entitled to recover from Defendant the damages sustained by PersonalWeb as a result  
25 of Defendant's wrongful acts in an amount subject to proof at trial.  
26  
27  
28



**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, 7,945,544, 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, 7,945,544, 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/ Sandeep Seth

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,

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

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/ Sandeep Seth

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