APPENDIX C

Appendix C

The first set of tables in this appendix compares PersonalWeb's infringement allegations asserted in PersonalWeb's current counterclaims against Amazon (*Amazon.com Inc. v. PersonalWeb Techs., LLC*, No. 5:18-cv-00767-BLF, Dkt. No. 62) with PersonalWeb's infringement allegations in one of its latest-filed complaints that PersonalWeb does not intend to amend. (*PersonalWeb Techs., LLC v. Strava, Inc.*, No. 5:18-cv-04627-BLF, Dkt. No. 1).

The second set of tables compares PersonalWeb's infringement allegations in its proposed amended counterclaims against Amazon in the DJ Action (No. 5:18-cv-00767-BLF) with its infringement allegations from a sample second amended complaint that PersonalWeb proposes filing in many of the website defendant cases.

I. Comparison of Infringement Allegations in Filed Counterclaims against Amazon and Filed Complaints

Filed Counterclaims Against Amazon[1]	Filed Complaint PersonalWeb Does Not Intend to Amend[2]
Alleged "INFRINGEMENT OF U.S. PATENT NO. 6,928,442"	
Amazon has infringed at least claims 10 and 11 of the '442 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Amazon's infringement is literal and/or under the doctrine of equivalents and Amazon is liable for its infringement of the '442 patent pursuant to 35 U.S.C. § 271.	Defendant has infringed at least claims 10 and 11 of the '442 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Defendant's infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '442 patent pursuant to 35 U.S.C. § 271.
For example, claim 10 covers "a method, in a system in which a plurality of files are distributed across a plurality of computers." On information and belief, Amazon has used a system of notifications and authorizations to distribute a plurality of files, *e.g.*,	For example, claim 10 covers "a method, in a system in which a plurality of files are distributed across a plurality of computers." On information and belief, Defendant has used a system of notifications and authorizations to distribute a plurality of files, *e.g.*,

[1] *Amazon.com Inc. v. PersonalWeb Techs., LLC*, No. 5:18-cv-00767-BLF, Dkt. No. 62 ¶¶ 46–50.
[2] *PersonalWeb Techs., LLC v. Strava, Inc.*, No. 5:18-cv-04627-BLF, Dkt. No. 1 ¶¶ 52–56.

the web server customers' files containing content necessary to render the web server customers' webpages, across a plurality of computers such as S3 web host servers, intermediate cache servers, and endpoint caches used by browsers rendering the web server customers' webpages.	Defendant's files containing content necessary to render its webpages, across a plurality of computers such as production servers, origin servers, intermediate cache servers and endpoint caches used by browsers rendering Defendant's webpages.
Claim 10 then recites the act of "obtaining a name for a data file, the name being based at least in part on a given function of the data, wherein the data used by the function comprises the contents of the particular file." As set forth above, on information and belief, Amazon generated ETags for the index and asset files used to render web server customers' webpages using a hash function, wherein the ETag were based on the contents of the particular file. Moreover, Amazon caused the intermediate caches servers and endpoint caches to obtain the ETags and URIs in HTTP 200 messages sent from the S3 web host servers. On information and belief, Amazon caused intermediate cache servers to obtain ETags and URIs in conditional GET messages from endpoint and intermediate caches, as described *supra*.	Claim 10 then recites the act of "obtaining a name for a data file, the name being based at least in part on a given function of the data, wherein the data used by the function comprises the contents of the particular file." As set forth above, on information and belief, Defendant generated or otherwise obtained ETags for its webpage and asset files used to render its webpages using a hash function, wherein the ETags were based on the contents of the particular files. Moreover, Defendant caused the intermediate caches servers and endpoint caches to obtain the ETags in HTTP 200 responses sent from Defendant's origin servers. On information and belief, Defendant caused intermediate cache servers and its origin servers to obtain ETags in conditional GET messages from endpoint and intermediate caches, as described *supra*.
Claim 10 then recites the act of "determining, using at least the name, whether a copy of the data file is present on at least one of said computers." On information and belief, as set forth above, S3 web host servers have, and Amazon has caused the intermediate cache servers between an endpoint cache and one of the S3 web host servers to, in response to receiving a conditional GET request with an If-None-Match header, determine whether it has a file present that matches the URI in the conditional GET and to compare the ETag in the conditional GET to the Etag for that URI and determine whether a copy of the content having that ETag is present.	Claim 10 then recites the act of "determining, using at least the name, whether a copy of the data file is present on at least one of said computers." On information and belief, as set forth above, Defendant has caused its origin severs and the intermediate cache servers between and endpoint cache and one of its origin servers to, in response to receiving a conditional GET request with an If-None-Match header, determine whether it has a file present that matches the URI in the conditional GET and to compare the ETag in the conditional GET to the ETag for that URI and determine whether a copy of the content having that ETag is present.
Claim 10 then recites the act of "determining whether a copy of the data file that is present on a at least one of said computers is	Claim 10 then recites the act of "determining whether a copy of the data file that is present on a at least one of said computers is

an unauthorized copy or an unlicensed copy of the data file." On information and belief, as set forth above, if there was a match, and it was determined that the max-age value was unexpired and/or after any further reauthorization check required by other directives set by the web server customer via "cache-control" headers, the origin or intermediate cache server determined that the copy of the file present at the downstream intermediate cache server and/or the endpoint cache was an authorized or licensed copy of the data file. Conversely, if there was no match, it determined that the copy of the file present at the downstream intermediate cache server and/or the endpoint cache was an unauthorized or unlicensed copy of the data file. Likewise, if the browser determined that it had a file with a matching URI, and its max-age value was unexpired and/or after any further reauthorization check required by the web server customer via other directives in "cache-control" headers, the browser determined that it was still authorized to use that file.	an unauthorized copy or an unlicensed copy of the data file." On information and belief, as set forth above, if there was a match, the origin or intermediate cache server determined that the copy of the file present at the downstream intermediate cache server and/or the endpoint cache was an authorized or licensed copy of the data file. Conversely, if there was no match, it determined that the copy of the file present at the downstream intermediate cache server and/or the endpoint cache was an unauthorized copy of the data file. Likewise, if the browser determined that it had a file with a matching URI, the browser determined that it was still authorized to use that file.

Counterclaims Against Amazon[3]	**Filed Complaint PersonalWeb Does Not Intend to Amend[4]**
Alleged "INFRINGEMENT OF U.S. PATENT NO. 7,945,544"	
Amazon has infringed at least claims 46, 48, 52, and 55 of the '544 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Amazon's infringement is literal and/or under the doctrine of	Defendant has infringed at least claims 46, 48, 52, and 55 of the '544 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Defendant's infringement is literal and/or under the doctrine of

[3] *Amazon.com Inc. v. PersonalWeb Techs., LLC*, No. 5:18-cv-00767-BLF, Dkt. No. 62 ¶¶ 61–68.
[4] *PersonalWeb Techs., LLC v. Strava, Inc.*, No. 5:18-cv-04627-BLF, Dkt. No. 1 ¶¶ 70–77.

equivalents and Amazon is liable for its infringement of the '544 patent pursuant to 35 U.S.C. § 271.	equivalents and Defendant is liable for its infringement of the '544 patent pursuant to 35 U.S.C. § 271.
For example, claim 46 covers a claimed "computer-implemented method." On information and belief, Amazon uses the claimed computer implemented method by using a system of notifications and authorizations to locate and control the distribution of data items, such as various index and asset files, necessary to render its web server customers' webpages.	For example, claim 46 covers a claimed "computer-implemented method." On information and belief, Defendant uses the claimed computer implemented method by using a system of notifications and authorizations to locate and control the distribution of data items, such as various webpage and asset files, necessary to render its webpages.
Claim 46 then recites the act of "(A) for each particular file of a plurality of files: (a2) determining a particular digital key for the particular file, wherein the particular file comprises a first one or more parts." On information and belief, for some of Amazon's web server customers ("URI fingerprint customers"), each of the URI fingerprint customers' webpages comprises one or more asset files and has an associated index file. The index file contained URIs having fingerprints of a plurality of asset files comprising that webpage. On information and belief, once the index and asset files are compiled and complete and the files have been uploaded to the S3 host system by the URI fingerprint customers, the index file's associated ETag value is generated by applying a hash algorithm to the index file's contents, wherein any two index files comprising the identical content will have identical associated ETag values. On information and belief, whenever a new index file is uploaded to an S3 server or the index file's content changes, Amazon determines and associates an ETag for the index file at the time of upload.	Claim 46 then recites the act of "(A) for each particular file of a plurality of files: (a2) determining a particular digital key for the particular file, wherein the particular file comprises a first one or more parts." On information and belief, each of Defendant's webpages comprises one or more asset files and has an associated webpage file, the webpage file containing the URIs having fingerprints of a plurality of asset files comprising the webpage, and once the webpage and asset files are compiled and complete, Defendant stores them on a host system. On information and belief, the webpage file's associated ETag value is generated by applying a hash algorithm to the webpage file's contents. On information and belief, whenever a new webpage file is generated or the webpage file's content changes, Defendant caused an ETag to be determined and associated to the webpage file.
Claim 46 then recites "each part of said first one or more parts having a corresponding part value, the part value of each specific part of said first one or more parts being based on a first function of the contents of the specific part, wherein two identical parts will have the same part value as determined by the first function,	Claim 46 then recites "each part of said first one or more parts having a corresponding part value, the part value of each specific part of said first one or more parts being based on a first function of the contents of the specific part, wherein two identical parts will have the same part value as determined by the first function,

and wherein the particular digital key for the particular file is determined using a second function of the one or more of part values of said first one or more parts." On information and belief, prior to an asset file being uploaded to the S3 host system, a fingerprint is generated for that asset file by applying a hash function to its contents. On information and belief, the fingerprint is inserted into the URI for that asset file. On information and belief, the webpage's ETag value is generated by applying a second hash function to its index file's contents, which consist of the URIs of one or more of the asset files which comprise the webpage's contents. On information and belief, because the respective asset file's URIs include the fingerprints of their content, the webpage's ETag value will change and a new associated ETag value is generated to represent the webpage's content, when the content changes and two identical webpages having the identical content represented by their index file will have the same ETag value.	and wherein the particular digital key for the particular file is determined using a second function of the one or more of part values of said first one or more parts." On information and belief, prior to various asset files being stored on a host system, a fingerprint is generated for each of these asset files by applying a hash function to the asset file's contents and the fingerprints are inserted into the URIs for the respective asset files. On information and belief, the webpage's ETag value is generated by applying a second hash function to the webpage file's contents, which include the URIs of one or more of the asset files which comprise the webpage's contents. On information and belief, because the respective asset files' URIs include the fingerprints of their content, the webpage's ETag value will change and a new associated ETag value is generated to represent the webpage's content, when the content changes and two identical webpages having the identical content represented by their webpage file will have the same ETag value.
Claim 46 then recites the act of "(a2) adding the particular digital key of the particular file to a database, the database including a mapping from digital keys of files to information about the corresponding files." On information and belief, the S3 host system, intermediate caches, and browser caches are caused to maintain database/tables which map the ETag of each webpage's index file to its URI, and information about the corresponding webpage, such as, for example, cache control information for the webpage.	Claim 46 then recites the act of "(a2) adding the particular digital key of the particular file to a database, the database including a mapping from digital keys of files to information about the corresponding files." On information and belief, Defendant caused the origin server, intermediate caches and browser caches to maintain databases/tables which mapped the ETag of each webpage's webpage file to its URI, and information about the corresponding webpage, such as, for example, information from cache-control headers for the webpage.
Claim 46 then recites "(B) determining a search key based on search criteria, wherein the search criteria comprise a second one or more parts, each of said second one or more parts of said search criteria having a corresponding part value, the part value of each specific part of said second one or more parts being based on the first function of the contents of the specific part,	Claim 46 then recites "(B) determining a search key based on search criteria, wherein the search criteria comprise a second one or more parts, each of said second one or more parts of said search criteria having a corresponding part value, the part value of each specific part of said second one or more parts being based on the first function of the contents of the specific part,

and wherein the search key is determined using the second function of the one or more of part values of said second one or more parts." On information and belief, when a downstream intermediate cache server or a browser again requests a webpage of a URI fingerprint customer, it sends a conditional GET request with an If-None-Match header with the webpage's associated ETag value. On information and belief, the received ETag value was determined using the second hash function of the webpage's index file, which includes URIs including fingerprints for one or more of the asset files which comprise the webpage's contents.	and wherein the search key is determined using the second function of the one or more of part values of said second one or more parts." On information and belief, when a downstream intermediate cache server or a browser again requested a webpage of Defendant, Defendant caused it to send a conditional GET request with an If-None-Match header with the webpage's associated ETag value. On information and belief, the received ETag value was determined using the second hash function of the webpage's webpage file, which included URIs including fingerprints for one or more of the asset files which comprised the webpage's contents.
Claim 46 then recites "(C) attempting to match the search key with a digital key in the database." On information and belief, when the responding server receives the webpage's ETag value in a conditional GET request with an If-None-Match header, it compares the received ETag with the ETags it has maintained in a database/table corresponding to the URI of the webpage's index file to determine if there is matching value for that webpage.	Claim 46 then recites "(C) attempting to match the search key with a digital key in the database." On information and belief, when the responding server received the webpage's ETag value in a conditional GET request with an If-None-Match header, it compared the received ETag with the ETag it has maintained in a database/table corresponding to the URI of the webpage's webpage file to determine if there is matching value for that webpage.
Claim 46 then recites "(D) if the search key matches a particular digital key in the database, providing information about the file corresponding to the particular digital key." On information and belief, if the responding server has a matching ETag value for the webpage's index file, the responding server sends an HTTP 304 message, which includes information about the corresponding webpage, such as, for example, cache control information for the webpage	Claim 46 then recites "(D) if the search key matches a particular digital key in the database, providing information about the file corresponding to the particular digital key." On information and belief, if the responding server had a matching ETag value for the webpage's webpage file, the responding server sent an HTTP 304 response, which included information about the corresponding webpage, such as, for example, information from cache-control headers for the webpage.

Counterclaims Against Amazon[5]	Filed Complaint PersonalWeb Does Not Intend to Amend[6]
Alleged "INFRINGEMENT OF U.S. PATENT No. 8,099,420"	
Amazon has infringed claims 25, 26, 27, 29, 30, 32, 34-36, and 166 of the '420 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner recited herein. Amazon's infringement is literal and/or under the doctrine of equivalents and Amazon is liable for its infringement of the '420 patent pursuant to 35 U.S.C. § 271.	Defendant has infringed claims 25, 26, 27, 29, 30, 32, 34–36, and 166 of the '420 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner recited herein. Defendant's infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '420 patent pursuant to 35 U.S.C. § 271.
For example, claim 166 covers a "system comprising hardware, including at least a processor, and software, in combination with said hardware." On information and belief, Amazon's system has comprised hardware including a processor, such as its S3 web host servers and the associated Amazon S3 software system which has been used in combination with its hardware.	For example, claim 166 covers a "system comprising hardware, including at least a processor, and software, in combination with said hardware." On information and belief, Defendant has controlled the distribution of its website content across a system that included hardware including a processor, such as its production servers as well as origin servers, intermediate cache servers, and endpoint caches; and software, in combination with such hardware, such as a web development framework, software utilized in implementing the HTTP web protocol, and the software used on host servers that Defendant used to serve its webpages.
Claim 166 then recites "(A) for a particular data item in a set of data items, said particular data item comprising a corresponding particular sequence of bits." On information and belief, Amazon's system has been used to control the distribution of asset files and index files necessary to render the web host customers' webpages which represent particular data items, and each of these files comprise a corresponding sequence of bits.	Claim 166 then recites "(A) for a particular data item in a set of data items, said particular data item comprising a corresponding particular sequence of bits." On information and belief, Defendant's system has controlled the distribution of asset files and webpage files necessary to render its webpages which represent particular data items, and each of these files comprise a corresponding sequence of bits.
Claim 166 then recites that for the particular data item to "(a1) determine one or more content-dependent digital identifiers for	Claim 166 then recites that for the particular data item to "(a1) determine one or more content-dependent digital identifiers for

[5] *Amazon.com Inc. v. PersonalWeb Techs., LLC*, No. 5:18-cv-00767-BLF, Dkt. No. 62 ¶¶ 72–77.
[6] *PersonalWeb Techs., LLC v. Strava, Inc.*, No. 5:18-cv-04627-BLF, Dkt. No. 1 ¶¶ 81–86.

said particular data item, each said content-dependent digital identifier being based at least in part on a given function of at least some of the bits in the particular sequence of bits of the particular data item, wherein two identical data items will have the same digital identifiers as determined using said given function." On information and belief, Amazon's system has, for particular files of the web server customers' webpage files, applied a hash function to all of the bits of each of the files' content to determine an ETag for the file's content; whereby two identical files have the same ETag. On information and belief, the ETag value was associated with the file's URI.	said particular data item, each said content-dependent digital identifier being based at least in part on a given function of at least some of the bits in the particular sequence of bits of the particular data item, wherein two identical data items will have the same digital identifiers as determined using said given function." On information and belief, Defendant's system has applied hash functions to each of various Defendant's webpage files to all of the bits of the file's content to determine a fingerprint, an ETag, or both for the file's content; whereby two identical data items have the same ETag values and the same fingerprint values. On information and belief, fingerprints were included in files' URI and ETag values were associated with files' URIs.
Claim 166 then recites that for the particular data item "(a2) selectively permits the particular data item to be made available for access and to be provided to or accessed by or from at least some of the computers in a network of computers, wherein the data item is not to be made available for access or provided without authorization, as resolved based, at least in part, on whether or not at least one of said one or more content-dependent digital identifiers for said particular data item corresponds to an entry in one or more databases, each of said one or more databases comprising a plurality of identifiers, each of said identifiers in each said database corresponding to at least one data item of a plurality of data items, and each of said identifiers in each said database being based, at least in part, on at least some of the data in a corresponding data item." On information and belief, Amazon's S3 web host servers included databases containing ETag values associated with the various URIs for asset and manifest/index files necessary to render web host customers' webpages; moreover, Amazon's system has used a system of conditional GET requests with If-None-	Claim 166 then recites that for the particular data item "(a2) selectively permits the particular data item to be made available for access and to be provided to or accessed by or from at least some of the computers in a network of computers, wherein the data item is not to be made available for access or provided without authorization, as resolved based, at least in part, on whether or not at least one of said one or more content-dependent digital identifiers for said particular data item corresponds to an entry in one or more databases, each of said one or more databases comprising a plurality of identifiers, each of said identifiers in each said database corresponding to at least one data item of a plurality of data items, and each of said identifiers in each said database being based, at least in part, on at least some of the data in a corresponding data item." On information and belief, Defendant's system has included one or more web servers with databases containing ETag values associated with the URIs for various of the asset and webpage files necessary to render its webpages; moreover, Defendant's system has used a system of conditional GET requests with If-None-

Match headers and HTTP 304 and HTTP 200 messages containing the ETags, as described more particularly supra, to ensure that downstream caches only access authorized file content to either serve that file content further downstream or to use it to render the web server customers' webpages. On information and belief, in particular, as more fully described supra, the system compared the ETag received in a given conditional GET request with the ETags contained in the database to selectively determine whether the requesting computer could access the file content it already had or must access newly received authorized content.	Match headers and HTTP 304 and HTTP 200 responses containing the ETags, as described more particularly supra, to ensure that downstream caches only access authorized file content to either serve that file content further downstream or to use it to render Defendant's webpages. On information and belief, in particular, as more fully described supra, the system compared the ETag received in a given conditional GET request with the ETags contained in the database to selectively determine whether the requesting computer could access the file content it already had or must access newly received authorized content.

Counterclaims Against Amazon[7]	**Filed Complaint PersonalWeb Does Not Intend to Amend**[8]
Alleged "INFRINGEMENT OF U.S. PATENT NO. 7,802,310"	
Amazon has infringed at least claim 20 of the '310 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Amazon's infringement is literal and/or under the doctrine of equivalents and Amazon is liable for its infringement of the '310 patent pursuant to 35 U.S.C. § 271.	Defendant has infringed at least claims 20 and 69 of the '310 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Defendant's infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '310 patent pursuant to 35 U.S.C. § 271.
For example, claim 20 covers a "computer-implemented method operable in a system which includes a plurality of computers." On information and belief, Amazon used the claimed computer implemented method by using a system of notifications and authorizations to control the distribution of data items, such as various index and asset files, necessary to render the web host customers' webpages, across a plurality of computers such as S3	For example, claim 20 covers a "computer-implemented method operable in a system which includes a plurality of computers." On information and belief, Defendant used the claimed computer implemented method by using a system of notifications and authorizations to control the distribution of data items, such as various webpage and asset files, necessary to render its webpages,

[7] *Amazon.com Inc. v. PersonalWeb Techs., LLC*, No. 5:18-cv-00767-BLF, Dkt. No. 62 ¶¶ 54–57.
[8] *PersonalWeb Techs., LLC v. Strava, Inc.*, No. 5:18-cv-04627-BLF, Dkt. No. 1 ¶¶ 60–63.

web host servers, intermediate cache servers, and endpoint caches.	across a plurality of computers such as production servers, origin servers, intermediate cache servers, and endpoint caches.
Claim 20 then recites "controlling distribution of content from a first computer to at least one other computer, in response to a request obtained by a first device in the system from a second device in the system, the first device comprising hardware including at least one processor, the request including at least a content-dependent name of a particular data item, the content-dependent name being based at least in part on a function of at least some of the data comprising the particular data item, wherein the function comprises a message digest function or a hash function, and wherein two identical data items will have the same content-dependent name." On information and belief, as set forth above, Amazon has caused downstream intermediate cache servers and endpoint caches to send conditional GET requests with If-None-Match headers containing ETags that are fielded by upstream cache or S3 web host servers. On information and belief, the ETags were content-dependent names for a data item based on hashing the data item's contents; and when the file's content changed a new content-dependent name was determined. On information and belief, in Amazon's method, a first computer, such as the intermediate cache server or S3 web host server, received such conditional GET requests from a second computer, such as a user browser or other intermediate cache server, regarding data items, such as index or asset files, the requests including ETags associated with the respective data items.	Claim 20 then recites "controlling distribution of content from a first computer to at least one other computer, in response to a request obtained by a first device in the system from a second device in the system, the first device comprising hardware including at least one processor, the request including at least a content-dependent name of a particular data item, the content-dependent name being based at least in part on a function of at least some of the data comprising the particular data item, wherein the function comprises a message digest function or a hash function, and wherein two identical data items will have the same content-dependent name." On information and belief, as set forth above, Defendant has caused downstream intermediate cache servers and endpoint caches to send conditional GET requests with If-None-Match headers containing ETags that are fielded by upstream cache or origin servers. On information and belief, the ETags were content-dependent names for a data item based on hashing the data item's contents; and when the file's content changed a new content-dependent name was determined. On information and belief, in Defendant's method, a first computer, such as the intermediate cache server or origin server, received such conditional GET requests from a second computer, such as a user browser or other intermediate cache server, regarding data items, such as webpage or asset files, the requests including ETags associated with the respective data items.
Claim 20 then recites "based at least in part on said content-dependent name of said particular data item, the first device (A) permitting the content to be provided to or accessed by the at least one other computer if it is not determined that the content is unauthorized or unlicensed, otherwise, (B) if it is determined	Claim 20 then recites "based at least in part on said content-dependent name of said particular data item, the first device (A) permitting the content to be provided to or accessed by the at least one other computer if it is not determined that the content is unauthorized or unlicensed, otherwise, (B) if it is determined

that the content is unauthorized or unlicensed, not permitting the content to be provided to or accessed by the at least one other computer." On information and belief, the first computer, such as an upstream intermediate cache server or S3 web host server, maintained a plurality of ETags associated with a web server customer's asset and index files On information and belief, the ETag in a request and the ETag maintained by the first computer for the particular data item sought by the request were compared to determine whether the associated content present at the downstream computer was still authorized to be used/served or whether new authorized content must be provided thereto. If it was determined that the data item corresponding to the received ETag was still authorized to be used, the first computer sent back an HTTP 304 message authorizing the downstream cache server or end-user cache to access the file content already present in order to serve it or to use it to render the webpage. On information and belief, if it had been determined that the data item corresponding to received E-tag was no longer authorized, the first computer sent back an HTTP 200 message which indicated to the downstream cache server or end-user cache that it was not authorized to access the old content and must access the new authorized file content contained in the HTTP 200 message to serve it or to use it to render the webpage.	that the content is unauthorized or unlicensed, not permitting the content to be provided to or accessed by the at least one other computer." On information and belief, the first computer, such as an upstream intermediate cache server or origin server, maintained a plurality of ETags associated with Defendant's asset and webpage files On information and belief, the ETag in a request and the ETag maintained by the first computer for the particular data item sought by the request were compared to determine whether the associated content present at the downstream computer was still authorized to be used/served or whether new authorized content must be provided thereto. If it was determined that the data item corresponding to the received ETag was still authorized to be used, the first computer sent back an HTTP 304 response authorizing the downstream cache server or end-user cache to access the file content already present in order to serve it or to use it to render the webpage. On information and belief, if it had been determined that the data item corresponding to received E-tag was no longer authorized, the first computer sent back an HTTP 200 response which indicated to the downstream cache server or end-user cache that was not authorized to access the old content and must access the new authorized file content contained in the HTTP 200 response to serve it or to use it to render the webpage.

II. Comparison of Infringement Allegations in Proposed Amended Counterclaims against Amazon and Proposed Amended Complaints

Proposed Amended Counterclaims Against Amazon[9]	Proposed Second Amended Complaint[10]
Alleged "INFRINGEMENT OF U.S. PATENT NO. 6,928,442"	
Amazon has infringed at least claims 10 and 11 of the '442 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Amazon's infringement is literal and/or under the doctrine of equivalents and Amazon is liable for its infringement of the '442 patent pursuant to 35 U.S.C. § 271.	Defendant has infringed at least claims 10 and 11 of the '442 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Defendant's infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '442 patent pursuant to 35 U.S.C. § 271.
For example, claim 10 covers "a method, in a system in which a plurality of files are distributed across a plurality of computers." On information and belief, Amazon has used a system of notifications and authorizations to distribute a plurality of files, *e.g.*, the web server customers' asset files containing content necessary to render the web server customers' webpages, across a plurality of computers such as S3 web host servers, intermediate cache servers and endpoint caches used by browsers rendering the web server customers' webpages.	For example, claim 10 covers "a method, in a system in which a plurality of files are distributed across a plurality of computers." On information and belief, Defendant has used a system of notifications and authorizations to distribute a plurality of files, *e.g.*, Defendant's files containing content necessary to render its webpages, across a plurality of computers such as production servers, origin servers, intermediate cache servers and endpoint caches used by browsers rendering Defendant's webpages.
Claim 10 then recites the act of "obtaining a name for a data file, the name being based at least in part on a given function of the data, wherein the data used by the function comprises the contents of the particular file." As set forth above, on information and belief, Amazon generated ETags for the asset files used to render web server customers' webpages using a hash function,	Claim 10 then recites the act of "obtaining a name for a data file, the name being based at least in part on a given function of the data, wherein the data used by the function comprises the contents of the particular file." As set forth above, on information and belief, Defendant generated or otherwise obtained ETags for its webpage and asset files used to render its webpages using a

[9] Proposed Amended Counterclaims, *Amazon.com Inc. v. PersonalWeb Techs., LLC*, No. 5:18-cv-00767-BLF, ¶¶ 46-50.
[10] Proposed Second Amended Complaint, *PersonalWeb Techs., LLC v. Airbnb, Inc.*, No. 5:18-cv-00149-BLF, ¶¶ 52-56.

wherein the ETags were based on the contents of the particular files. Moreover, Amazon caused the intermediate caches [*sic*] servers and endpoint caches to obtain these ETags in HTTP 200 responses sent from the S3 web host servers. On information and belief, Amazon caused intermediate cache servers to obtain ETags in conditional GET messages from endpoint and intermediate caches, as described *supra*.	hash function, wherein the ETags were based on the contents of the particular files. Moreover, Defendant caused the intermediate caches [*sic*] servers and endpoint caches to obtain the ETags in HTTP 200 responses sent from Defendant's origin servers. On information and belief, Defendant caused intermediate cache servers and its origin servers to obtain ETags in conditional GET messages from endpoint and intermediate caches, as described *supra*.
Claim 10 then recites the act of "determining, using at least the name, whether a copy of the data file is present on at least one of said computers." On information and belief, as set forth above, S3 web host servers have, and Amazon has caused the intermediate cache servers between an endpoint cache and one of the S3 web host servers to, in response to receiving a conditional GET request with an If-None-Match header, determine whether it has a file present that matches the URI in the conditional GET and to compare the ETag in the conditional GET to the Etag for that URI and determine whether a copy of the content having that ETag is present.	Claim 10 then recites the act of "determining, using at least the name, whether a copy of the data file is present on at least one of said computers." On information and belief, as set forth above, Defendant has caused its origin servers and the intermediate cache servers between an endpoint cache and one of its origin servers to, in response to receiving a conditional GET request with an If-None-Match header, determine whether it has a file present that matches the URI in the conditional GET and to compare the ETag in the conditional GET to the ETag for that URI and determine whether a copy of the content having that ETag is present.
Claim 10 then recites the act of "determining whether a copy of the data file that is present on a at least one of said computers is an unauthorized copy or an unlicensed copy of the data file." On information and belief, as set forth above, if there was a match, the origin or intermediate cache server determined that the copy of the asset file present at the downstream intermediate cache server and/or the endpoint cache was an authorized or licensed copy of the data file. Conversely, if there was no match, it determined that the copy of the asset file present at the downstream intermediate cache server and/or the endpoint cache was an unauthorized copy of the asset file. Likewise, if the browser determined that it had a file with a matching URL, the browser determined that it was still authorized to use that asset file.	Claim 10 then recites the act of "determining whether a copy of the data file that is present on a at least one of said computers is an unauthorized copy or an unlicensed copy of the data file." On information and belief, as set forth above, if there was a match, the origination or intermediate cache server determined that the copy of the file present at the downstream intermediate cache server and/or the endpoint cache was an authorized or licensed copy of the data file. Conversely, if there was no match, it determined that the copy of the file present at the downstream intermediate cache server and/or the endpoint cache was an unauthorized copy of the data file. Likewise, if the browser determined that it had a file with a matching URI, the browser determined that it was still authorized to use that file.

Proposed Amended Counterclaims Against Amazon[11]	Proposed Second Amended Complaint[12]
Alleged "INFRINGEMENT OF U.S. PATENT NO. 8,099,420"	
Amazon has infringed claims 25, 26, 27, 29, 30, 32, 34–36, and 166 of the '420 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner recited herein. Amazon's infringement is literal and/or under the doctrine of equivalents and Amazon is liable for its infringement of the '420 patent pursuant to 35 U.S.C. § 271.	Defendant has infringed claims 25, 26, 27, 29, 30, 32, 34–36, and 166 of the '420 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner recited herein. Defendant's infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '420 patent pursuant to 35 U.S.C. § 271.
For example, claim 166 covers a "system comprising hardware, including at least a processor, and software, in combination with said hardware." On information and belief, Amazon's system has comprised hardware including a processor, such as its S3 web host servers, and the associated Amazon S3 software system which has been used in combination with its hardware.	For example, claim 166 covers a "system comprising hardware, including at least a processor, and software, in combination with said hardware." On information and belief, Defendant has controlled the distribution of its website content across a system that included hardware including a processor, such as its production servers as well as origin servers, intermediate cache servers, and endpoint caches; and software, in combination with such hardware, such as a web development framework, software utilized in implementing the HTTP web protocol, and the software used on host servers that Defendant used to serve its webpages.
Claim 166 then recites "(A) for a particular data item in a set of data items, said particular data item comprising a corresponding particular sequence of bits." On information and belief, Amazon's system has controlled the distribution of asset files necessary to render the web host customers' webpages which represent particular data items, and each of these files comprise a corresponding sequence of bits.	Claim 166 then recites "(A) for a particular data item in a set of data items, said particular data item comprising a corresponding particular sequence of bits." On information and belief, Defendant's system has controlled the distribution of asset files and webpage base files necessary to render its webpages which represent particular data items, and each of these files comprise a corresponding sequence of bits.

[11] Proposed Amended Counterclaims, *Amazon.com Inc. v. PersonalWeb Techs., LLC*, No. 5:18-cv-00767-BLF, ¶¶ 61–66.
[12] Proposed Second Amended Complaint, *PersonalWeb Techs., LLC v. Airbnb, Inc.*, No. 5:18-cv-00149-BLF, ¶¶ 81–86.

Claim 166 then recites that for the particular data item to "(a1) determine one or more content-dependent digital identifiers for said particular data item, each said content-dependent digital identifier being based at least in part on a given function of at least some of the bits in the particular sequence of bits of the particular data item, wherein two identical data items will have the same digital identifiers as determined using said given function." On information and belief, Amazon's system has applied hash functions to various web server customers' webpage asset files to all of the bits of the asset file's content to determine an ETag for the file's content; whereby two asset files having the same content had the same ETag values. On information and belief, Amazon associated the ETag values were with corresponding files' URIs.	Claim 166 then recites that for the particular data item to "(a1) determine one or more content-dependent digital identifiers for said particular data item, each said content-dependent digital identifier being based at least in part on a given function of at least some of the bits in the particular sequence of bits of the particular data item, wherein two identical data items will have the same digital identifiers as determined using said given function." On information and belief, Defendant's system has applied hash functions to each of various Defendant's webpage base files to all of the bits of the file's content to determine a fingerprint, an ETag, or both for the file's content; whereby two identical data items have the same ETag values and the same fingerprint values. On information and belief, fingerprints were included in files' URI and ETag values were associated with files' URIs.
Claim 166 then recites that for the particular data item "(a2) selectively permits the particular data item to be made available for access and to be provided to or accessed by or from at least some of the computers in a network of computers, wherein the data item is not to be made available for access or provided without authorization, as resolved based, at least in part, on whether or not at least one of said one or more content-dependent digital identifiers for said particular data item corresponds to an entry in one or more databases, each of said one or more databases comprising a plurality of identifiers, each of said identifiers in each said database corresponding to at least one data item of a plurality of data items, and each of said identifiers in each said database being based, at least in part, on at least some of the data in a corresponding data item." On information and belief, Amazon's S3 web host servers included databases containing ETag values associated with the various URIs for asset files necessary to render the web server	Claim 166 then recites that for the particular data item "(a2) selectively permits the particular data item to be made available for access and to be provided to or accessed by or from at least some of the computers in a network of computers, wherein the data item is not to be made available for access or provided without authorization, as resolved based, at least in part, on whether or not at least one of said one or more content-dependent digital identifiers for said particular data item corresponds to an entry in one or more databases, each of said one or more databases comprising a plurality of identifiers, each of said identifiers in each said database corresponding to at least one data item of a plurality of data items, and each of said identifiers in each said database being based, at least in part, on at least some of the data in a corresponding data item." On information and belief, Defendant's system has included one or more web servers with databases containing ETag values associated with the URIs for various of the asset and webpage base

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

Proposed Amended Counterclaims Against Amazon[13]	**Proposed Second Amended Complaint[14]**
Alleged "INFRINGEMENT OF U.S. PATENT NO. 7,802,310"	
Amazon has infringed at least claim 20 of the '310 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Amazon's infringement is literal and/or under the doctrine of equivalents and Amazon is liable for its infringement of the '310 patent pursuant to 35 U.S.C. § 271.	Defendant has infringed at least claims 20 and 69 of the '310 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Defendant's infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '310 patent pursuant to 35 U.S.C. § 271.
For example, claim 20 covers a "computer-implemented method operable in a system which includes a plurality of computers." On information and belief, Amazon used the claimed computer	For example, claim 20 covers a "computer-implemented method operable in a system which includes a plurality of computers." On information and belief, Defendant used the claimed computer

[13] Proposed Amended Counterclaims, *Amazon.com Inc. v. PersonalWeb Techs., LLC*, No. 5:18-cv-00767-BLF, ¶¶ 54-57
[14] Proposed Second Amended Complaint, *PersonalWeb Techs., LLC v. Airbnb, Inc.*, No. 5:18-cv-00149-BLF, ¶¶ 60–63.

implemented method by using a system of notifications and authorizations to control the distribution of data items, such as asset files, necessary to render its web host customers' webpages, across a plurality of computers such as S3 web host servers, intermediate cache servers, and endpoint caches.	implemented method by using a system of notifications and authorizations to control the distribution of data items, such as various webpage and asset files, necessary to render its webpages, across a plurality of computers such as production servers, origin servers, intermediate cache servers, and endpoint caches.
Claim 20 then recites "controlling distribution of content from a first computer to at least one other computer, in response to a request obtained by a first device in the system from a second device in the system, the first device comprising hardware including at least one processor, the request including at least a content-dependent name of a particular data item, the content-dependent name being based at least in part on a function of at least some of the data comprising the particular data item, wherein the function comprises a message digest function or a hash function, and wherein two identical data items will have the same content-dependent name." On information and belief, as set forth above, Amazon has caused downstream intermediate cache servers and endpoint caches to send conditional GET requests with If-None-Match headers containing ETags that are fielded by upstream cache or S3 web host servers. On information and belief, the ETags were content-dependent names for asset files based on hashing the asset file's contents; and when the asset file's content changed a new content-dependent name was determined. On information and belief, in Amazon's method, a first computer, such as the intermediate cache server or S3 web host server, received such conditional GET requests from a second computer, such as a user browser or other intermediate cache server, regarding webpage asset files, the requests including ETags associated with the respective file.	Claim 20 then recites "controlling distribution of content from a first computer to at least one other computer, in response to a request obtained by a first device in the system from a second device in the system, the first device comprising hardware including at least one processor, the request including at least a content-dependent name of a particular data item, the content-dependent name being based at least in part on a function of at least some of the data comprising the particular data item, wherein the function comprises a message digest function or a hash function, and wherein two identical data items will have the same content-dependent name." On information and belief, as set forth above, Defendant has caused downstream intermediate cache servers and endpoint caches to send conditional GET requests with If-None-Match headers containing ETags that are fielded by upstream cache or origin servers. On information and belief, the ETags were content-dependent names for a data item based on hashing the data item's contents; and when the file's content changed a new content-dependent name was determined. On information and belief, in Defendant's method, a first computer, such as the intermediate cache server or origin server, received such conditional GET requests from a second computer, such as a user browser or other intermediate cache server, regarding data items, such as webpage or asset files, the requests including ETags associated with the respective data items.
Claim 20 then recites "based at least in part on said content-dependent name of said particular data item, the first device (A) permitting the content to be provided to or accessed by the at	Claim 20 then recites "based at least in part on said content-dependent name of said particular data item, the first device (A) permitting the content to be provided to or accessed by the at

least one other computer if it is not determined that the content is unauthorized or unlicensed, otherwise, (B) if it is determined that the content is unauthorized or unlicensed, not permitting the content to be provided to or accessed by the at least one other computer." On information and belief, the first computer, such as an upstream intermediate cache server or S3 web host server, maintained a plurality of ETags associated with a web server customer's asset files On information and belief, the ETag in a request and the ETag maintained by the first computer for the particular data item sought by the request were compared to determine whether the associated content present at the downstream computer was still authorized to be used/served or whether new authorized content must be provided thereto. If it was determined that the data item corresponding to the received ETag was still authorized to be used, the first computer sent back an HTTP 304 response authorizing the downstream cache server or end-user cache to access the asset file content already present in order to serve it or to use it to render the webpage. On information and belief, if it had been determined that the data item corresponding to received E-tag was no longer authorized, the first computer sent back an HTTP 200 response which indicated to the downstream cache server or end-user cache that it was not authorized to access the old asset file content and must access the new authorized asset file content contained in the HTTP 200 response to serve it or to use it to render the webpage.	least one other computer if it is not determined that the content is unauthorized or unlicensed, otherwise, (B) if it is determined that the content is unauthorized or unlicensed, not permitting the content to be provided to or accessed by the at least one other computer." On information and belief, the first computer, such as an upstream intermediate cache server or origin server, maintained a plurality of ETags associated with Defendant's asset and webpage base files On information and belief, the ETag in a request and the ETag maintained by the first computer for the particular data item sought by the request were compared to determine whether the associated content present at the downstream computer was still authorized to be used/served or whether new authorized content must be provided thereto. If it was determined that the data item corresponding to the received ETag was still authorized to be used, the first computer sent back an HTTP 304 response authorizing the downstream cache server or end-user cache to access the file content already present in order to serve it or to use it to render the webpage. On information and belief, if it had been determined that the data item corresponding to received E-tag was no longer authorized, the first computer sent back an HTTP 200 response which indicated to the downstream cache server or end-user cache that was not authorized to access the old content and must access the new authorized file content contained in the HTTP 200 response to serve it or to use it to render the webpage.