UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

NETNUT LTD.,

Petitioner,

v.

BRIGHT DATA LTD. (f/k/a Luminati Networks Ltd.),

Patent Owner.

_____

Cases IPR2021-00465

Patent No. 9,742,866

_____

PETITIONER'S OPPOSITION TO PATENT OWNER'S NON-CONTINGENT MOTION TO AMEND

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes **Page(s)**

Regulations **Page(s)**

Other **Page(s)**

EXHIBIT LIST

Ex. No.	Description
1001	U.S. Patent No. 9,742,866 to Shribman et al. ("'866 patent")
1002	Excerpts from Prosecution History of the '866 patent (s/n 14/930,894)
1003	Expert Declaration of Keith J. Teruya
1004	CV of Keith J. Teruya
1005	Appendix of Challenged Claims
1006	Postel, RFC 791, Internet Protocol, DARPA Internet Program Protocol Specification (Information Sciences Institute, University of Southern California, September 1981)
1007	Fielding, et al., RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, (Internet Engineering Task Force, Network Working Group, June 1999)
1008	Reserved
1009	Reserved
1010	Exhibits considered by Keith J. Teruya
1011	Excerpts from Webster's Third New International Dictionary, ISBN: 978-0-87779-789-0 (2017) (Cover, Copyright Page, Definitions of "include" and "website")
1012	Wessels, "Squid: The Definitive Guide," ISBN-10: 9780596001629, ISBN-13: 978-0596001629, O'Reilly Media; 1st Ed. (January 1, 2004)
1013	Reserved
1014	Luotonen, "Web Proxy Servers," ISBN-10: 0136806120, ISBN-13: 978-0136806127, Prentice Hall; 1st Ed. (December 30, 1997)
1015	Reserved
1016	Reserved
1017	U.S. Patent Publication No. 2011/0087733 to Shribman et al. ("Shribman") (Published April 14, 2011)
1018	European Patent Publication EP 2 597 869 A1 by Sharp KK, Published May 29, 2013
1019	Reserved
1020	Cooper et al., RFC 3040, Internet Web Replication and Caching Taxonomy (January 2001)
1021	Reserved
1022	Reserved
1023	Claim construction order, *Luminati Networks Ltd. v. UAB Tesonet*, No. 2:18-CV-299 (E.D. Tex.), slip op. (D.I. 121, Aug. 20, 2019)
1024	Reserved

Ex. No.	Description
1025	Reserved
1026	Reserved
1027	ISO/IEC 23009-1:2012(E), MPEG-DASH standard, Jan. 5, 2012
1028	Reserved
1029	Microsoft Computer Dictionary (5th Ed. 2002), definitions of Web site and Web page
1030	Reserved
1031	Reserved
1032	Reserved
1033	Claim construction order, *Luminati Networks Ltd. v. BIScience Inc.*, No. 2:18-CV-483 (E.D. Tex.), slip op. (D.I. 130, Dec. 6, 2019)
1101	Expert Declaration of Keith J. Teruya in Support of Petitioner's Opposition to Patent Owner's Non-Contingent Motion to Amend
1102	CV of Keith J. Teruya
1103	Exhibits considered by Keith J. Teruya
1104	U.S. Patent No. 8,560,604 to Shribman *et al*.
1105	U.S. Patent No. 6,266,704 to Reed *et al.*
1106	Reserved
1107	Reserved
1108	Reserved
1109	Reserved
1110	Reserved
1111	Reserved
1112	RFC 3986 (IETF, Jan. 2005)
1113	RFC 2817 (IETF, May 2000)
1114	U.S. Patent Publication No. 2013/0080575 to Prince et al. ("Prince"), Published March 28, 2013
1115	Printout of VIP72 Youtube web page at https://www.youtube.com/watch?v=L0Hct2kSnn4, retrieved Nov. 21, 2019
1116	VIP72 Scene Images extracted from VIP72.com/nvpnnet, MPEG-4 video recording of "nVPN.net | Double your Safety and use Socks5 +nVpn", accessed from https://www.youtube.com/watch?v=L0Hct2kSnn4, published September 11, 2011
1117	Declaration of Ronald Abramson authenticating Ex. 1116 Scene Images

Ex. No.	Description
1118	Certification dated Nov. 8, 2019 of Anjali Shresta of Google, Proof of Date for VIP72 Youtube web page and video
2020	Appendix A-1: Written Description Support
2021	Appendix A-2: Proposed, Substitute Claims
2023	Provisional Application No. 61/870,815 – drawings
2024	Nonprovisional Application No. 14/468,836 – abstract
2025	Nonprovisional Application No. 14/468,836 – specification
2026	Nonprovisional Application No. 14/468,836 – drawings
2027	Nonprovisional Application No. 14/468,836 – claims

Note: Exhibits with numbers beginning with "10" and "20" were previously filed.

I. INTRODUCTION

Petitioner opposes Patent Owner's non-contingent motion to amend and requests that the Board find substitute claims 29–38 unpatentable.

PO seeks to introduce by amendment limitations similar to what it previously sought by claim construction. The amendments seek to distinguish the claims by adding "tunneling" through "consumer electronic devices." PO claims (MTA at 10) that "none of the prior art references teach or suggest the use of a tunnel device as claimed." However, this assertion is incorrect, as a second embodiment (which PO completely overlooks) in Ex. 1017 (the Shribman '733 publication ("S733")), discloses consumer devices acting as intermediate content retrieval devices and accessed via tunneling. Other references, including Prince and VIP72.com (asserted by Petitioner in the IPR of related U.S. Patent No. 9,241,044 (the "'044 patent")), also disclose tunneling.

Moreover, partitioning content into chunks (which is at the core of the '866 claims), and keeping track of which devices have which chunks, is inconsistent with the claimed anonymity. The MTA should be denied.

II. PATENT OWNER FAILED TO MAKE REQUIRED THRESHOLD SHOWINGS

PO bears the burden of showing, *inter alia*, that the proposed amendments, in addition to being narrowing, "are supported in the original disclosure (and any earlier filed disclosure for which the benefit of filing date is sought)." *Unified Patents,*

LLC v. IdeaHub Inc., IPR2020-00702, Paper 52 at 33–34 (PTAB Sept. 15, 2021) (citing 35 U.S.C. § 316(d); 37 C.F.R. § 42.121); *see also Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 15 at 7 (PTAB Feb. 25, 2019) (precedential). Petitioner may also raise unpatentability under 35 U.S.C. § 112 as to the proposed substitute claims. PTAB Consolidated Trial Practice Guide (Nov. 2019), 72–73, available at https://www.uspto.gov/TrialPracticeGuideConsolidated (last visited Jan. 31, 2022); 35 U.S.C. § 316(d); 37 C.F.R. § 41.121.

A. The Substitute Claims Lack Adequate Written Description

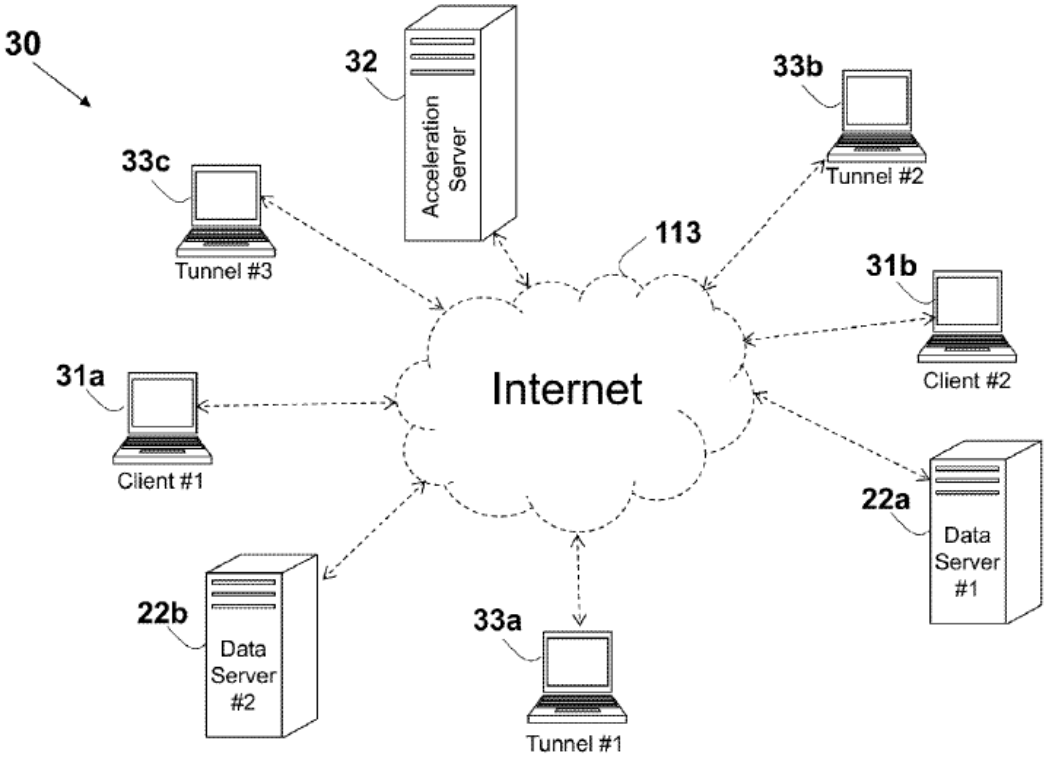


FIG. 5

Fig. 5 of the '866 patent is representative of the subject matter. The terms of the proposed amendment may be mapped onto Fig. 5 as follows:[1]

first device and its identifier, ***first identifier***	Client 31a and its IP address, respectively. *See, e.g.*, Ex. 2025 at 112–14.
first server and its identifier, ***second identifier***	Data Server #1 22a, *e.g.*, *id.* at 114. Identifiers may be "IP addresses or URLs." *Id.* at 139.
first tunnel device and its identifier, the ***group device identifier***	Tunnel #1 33a and its IP address. *E.g.*, *id.* at 112.
first request	Client 31a's request to the tunnel device for specified content. *Id.* at 114, 117–18, 145.

1. PO improperly relies on a provisional application

In the first column of Ex. 2020 (App'x A-1), PO asserts as written description support material found only in its provisional application. At time of the nonprovisional filing in this case, 37 C.F.R. § 1.57(d) (37 C.F.R. § 1.57(c) when the provisional was filed), provided in pertinent part that "'[e]ssential material' may be incorporated by reference, but only by way of an incorporation by reference to a U.S. patent or U.S. patent application publication" and that "[e]ssential material" is

[1] The '866 patent claims do not recite an analog to "acceleration server" 32, starting instead from simply reciting that there is a "group" of intermediate retrieval devices from which to choose. Hence, with one fewer "server" recited in the claims, what were the "second server," "third identifier," and "second request" in the '044 claims become the "first server," "second identifier," and "first request."

material "necessary to: (1) [p]rovide a written description of the claimed invention." However, a provisional patent application is not a "U.S. patent or U.S. patent application publication" under this regulation and cannot not be used for written description support. *ZTE (USA), Inc. v. CyWee Grp. Ltd.*, IPR2019-00143, Paper 87 at 116 (PTAB Feb. 17, 2021); *see also Nichia Corp. v. Emcore Corp.*, IPR2012-00005, Paper 27 at 3–4 (PTAB June 3, 2013) (rejecting provisional as written description support). *Cf. Droplets, Inc. v. E*TRADE Bank*, 887 F.3d 1309, 1318 (Fed. Cir. 2018); *Nomadix, Inc. v. Second Rule LLC*, No. CV 07-01946, 2009 WL 10668158, at *26 (C.D. Cal. Jan. 16, 2009) (pre-rule case, but commenting that "[i]f § 1.57 applied to the [challenged] patent, there would be no question that the … provisional application was improperly incorporated"). Accordingly, the entire first column of Ex. 2020 (specifically citing Prov. App. No. 61/870,815) should be disregarded for the purposes of establishing written description support (although the citations from the provisional would fall short in any case).

2. "Complete URL" in the first request lacks adequate written description support

A "wherein" clause specifies that the *second identifier* is a "complete URL." The MTA points to https://www.youtube.com/watch?v=9mSb3P7cZIE?ST=1:48 as a "complete URL." *See, e.g.*, Ex. 2020 at 18–19. This expression actually identifies *content* on a server. A field *within* this expression, "www.youtube.com", *does* identify an origin server (Ex. 1101 ¶ 40), and may be what PO intends as an example of

a "complete URL," but this is not clear from the MTA, let alone from the subject patent specification.

Though the written description shows an expression, as above, being used, for example, in a *database* maintained on the tunnel device (*e.g.*, Ex. 2026, Fig. 15a), it does not disclose the format of the claimed first request itself, *i.e.*, the content request from the client device to the tunnel device. *See, e.g.*, Ex. 2026 at Fig. 5b (element 56g), as well as Ex. 2025 at 114) (describing this as a "Content Request" without disclosing the format of the request).

PO points to no written-description support for anything that may reasonably be considered a "complete URL" within a request from a first client device to a tunnel device, as an identifier of the origin server from which specified content is being sought. [2]

[2] The cited provisional support is no better. For example, Fig. 130, block 13008 addresses a "back-end" process on the tunnel device, not the format of a request *to* the tunnel device. *See* Ex. 2020 at 18. Pages 18–19 of the provisional refer to "Back End" criteria, including "Wikipedia.org/contact.html" but do not disclose the form in which the tunnel device received the request. Ex. 2022 at 18–19. RFC 2616 makes clear that a recipient may learn the content origin by way of a Host header rather than the request URL. Ex. 1007 § 5.1.2 at 37.

The written description does mention the sending a "URL," but without any mention of whether it is relative, "complete," or absolute. Ex. 2020 at 18 ("The client device sends a 'Request List' message 226 e to the acceleration server 202, corresponding to a 'Request Agents List' step 231 c in the flowchart 230. This request includes the URL or any other identifier of the requested content."). This does not disclose or enable "complete URL" in the first request. As in *Nichia v. Emcore*, *supra*, PO here, seeking to amend, likewise failed to explain "why a person of ordinary skill in the art would have recognized that the inventor possessed the claimed subject matter." IPR2012-00005, Paper 27 at 4.

3. The written description does not support the full scope of the claimed anonymity features

The proposed amendment recites anonymity as between the first device (requesting client) and each of (i) the first server (*e.g.*, origin web server, with which the client's contact is only indirect), as well (ii) the first tunnel device.

PO cites support for the first aspect, anonymity of the first device vis-à-vis the first server. But there is no support for the second aspect (anonymity of the first device with respect to the first tunnel device). When PO addresses anonymity in the MTA, it only mentions it with respect to the data server rather than the tunnel device:

> Patent Owner respectfully submits no prior art references teach or suggest the claimed methods, including the anonymity limitation to prevent blocking or spoofing ***from the web server***.

MTA at 12. PO argues: "in every embodiment of [the reference], the client 4 directly

contacts the server 2 … and therefore, for example, there is no anonymity of client 4 with respect to server 2." *Id.* But the proposed claim is no different, likewise reciting the first device "(b) sending over the Internet a first request from the first device to the selected tunnel device" and "(c) … receiving over the Internet the content slice from the first server via the selected tunnel device," which on its face reflects a *lack* of anonymity between the first device and the first tunnel device. Moreover, the '866 written description itself describes "anonymous web browsing" as "browsing the World Wide Web while hiding the user's IP address and any other personally identifiable information *from the websites* that one is visiting." *See* Ex. 2020 at 19; Ex. 1001, 43:9–12 (emphasis added); *see also* Ex. 1001, 88:7–9, 96:18–20.

In Ex. 2020 (App'x A-1), at page 20, PO, without argument, seeks support for anonymity from the second server in "Fig. 13 and associated description." But this support does not stand up. Fig. 13 shows an additional proxy server 131 between the first device 132 and the remainder of the network elements:

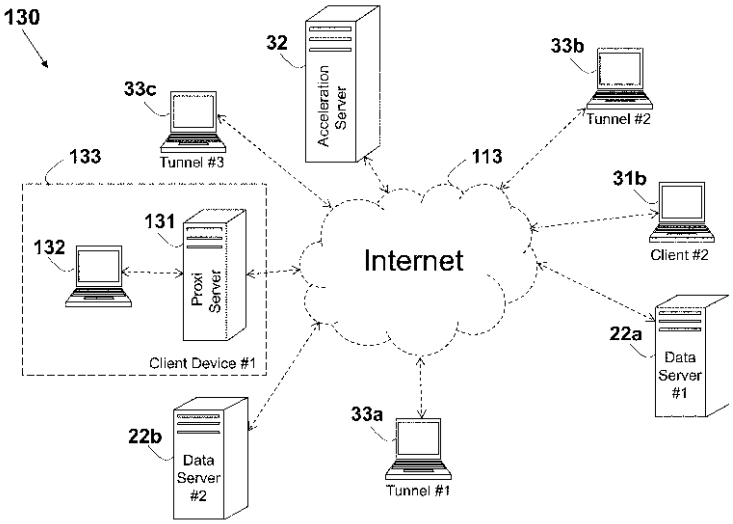


FIG. 13

However, this additional "Prox[y]" is shown in the figure itself *as being part of* "Client Device #1" – hardly conferring "anonymity" to that device, and failing to point to any disclosure even purporting to assert that it does. As the Board already noted with regard to Fig. 13 in its decision to institute *inter partes* review of the '044 patent, "the functionality of any device described in the patent may be implemented using multiple physical devices." IPR2021-00458, Paper 11 ("'044 Inst. Dec.") at 5 (and a "server" can also be a software process in the client device); Ex. 1101 ¶ 49. Fig. 13 does not at all reflect anonymity established as between the client (first device) and the tunnel with which it communicates. PO has again failed to explain its possession of this aspect of the claimed invention. Ex. 1101 ¶ 50. (As separately addressed in the following point, there is also a fundamental lack of enablement for anonymity of the first device from the tunnel device.)

B. There Is No Enablement of Anonymity from the Tunnel Device

The core of the '866 claims concerns "partitioning" "fresh content into a plurality of content slices" and serving the content slices responsive to requests therefor. This functionality, supporting piece-wise retrieval of content, requires keeping track of which devices in the system have cached which content. This mechanism is disclosed at Ex. 1001, 93:63–95:16. The written description is phrased in terms of functions that "may" be supported, but the subject matter as claimed here would not be operable without knowing where cached content slices can be found. Ex. 1101 ¶ 51. Thus, the devices in the '866 patent not only know who is making what requests, but what content they received responsive thereto. This is inconsistent with, and thus fails to enable, the claimed anonymity as to the tunnel device. Ex. 1101 ¶ 52.

C. "Complete URL" Is Indefinite

Returning to "complete URL," the term is also indefinite. PO's submission (Ex. 2020) gives as examples formats such as https://www.youtube.com (Ex. 2025 at 169). But URLs (a subset of URIs primarily for HTTP) are technically specified in RFC 3986 (Ex. 1112), and it is clear therefrom that URLs can have many other formats and be perfectly valid, including without limitation by IP address or registered name. *Id.* § 3.2.2 at 18. The term "complete URL" does not specify whether a name or an IP address (IPv4 or IPv6) is mandatory, whether the format must also contain the "scheme" (*e.g.*, http://, https://, ftp://, etc.). For these reasons, it is not

reasonably certain to a POSITA, based on the intrinsic and extrinsic evidence, what a "complete URL" is supposed to mean. Ex. 1101 ¶¶ 53–56.

PO may argue that "complete URL" means an "absolute URI" as defined in RFC 2616 § 5.1.2 and exemplified by the "https://www.youtube.com/watch?v=9mSb3P7cZIE?ST=1:48" video identifier. But that format is for a content identifier, not a device identifier. Ex. 1101 ¶ 57.

D. Mere Recitation of Results Should Be Given No Patentable Weight

The amendment seeks to claim the *result* of performing the method (achieving anonymity), but without reciting any manipulative difference in the amended claim (as compared to the original claim) that would achieve anonymity as between the first device and the first tunnel device. The mere stipulation of the *result* of anonymity should be accorded no patentable weight beyond what otherwise flows from the recited procedural limitations. *See In re Copaxone Consol. Cases*, 906 F.3d 1013, 1022–23 (Fed. Cir. 2018) (claim terms that are "superfluous, do[] not change the claimed method or require any additional structure or condition for the claims…[are] therefore non-limiting"). Or alternately, since the specification would appear to negate the anonymity of one of the variations ostensibly covered by the claim (*i.e.*, anonymity from the tunnel device), the limitation is indefinite. *See In re Mayhew*, 527 F.2d 1229, 1237–38 (C.C.P.A. 1976) (claims broader than what the specification indicates is practicable).

III. UNPATENTABILITY UNDER 35 U.S.C. § 103

A. GROUND 6: Obviousness of Substitute Claims over S733 Itself or in view of Sharp KK, Prince, Reed, and VIP72.com

1. Overview

S733, like the '866 patent (which incorporates U.S. Patent No. 8,560,604, which issued on S733), discloses partitioning fresh content into slices (called "chunks" or "portions of data" in S733 (Ex. 1017 ¶¶ 0016, 0055 (defining "chunks")), and distributing the chunks to other devices in response to content requests. *Id.* ¶ 0069. As further addressed below, S733 includes an embodiment that also discloses tunneling. *Id.* ¶ 0103 *ff.* Much like the scheme in the '866 patent (*see* "pre-connect" and "content fetch" phases, *e.g.*, Ex. 1001, 52:62–53:7, 83:49–51), the tunneling embodiment in S733 also works in two phases, the first a "connect phase" involving chained TCP connections through a designated agent (Ex. 1017 ¶¶ 0107–08), and the second a messaging phase over the chained TCP connections, *i.e.*, tunnels (*id.* ¶¶ 0109–14). The thrust of these amendments—to add tunneling to the claims—does nothing to save them under § 103.

To begin with, per the Board's interpretation of "tunnel" in its institution decision on the '044 patent ('044 Inst. Dec. at 19–20), the "second device" in the original claims would already have been regarded as a "tunnel." Ex. 1101 ¶ 59.

The provisional of the '866 patent, representing the tunnels as laptops (Ex. 2023 at Fig. 50), said the system also "works as described in Hola patent [serial no.

of S733].” Ex. 2022 at 1. The MTA points to nothing about tunneling or the use of consumer electronic devices that changes the architecture or procedural steps being claimed. These are all differences with no operational significance (Ex. 1101 ¶ 60), and should carry no patentable weight. *See, e.g., Ex Parte Dammers*, 155 U.S.P.Q. 284, at *2 (B.P.A.I. Nov. 29, 1961) (patentability of a method claim cannot be predicated solely on the structure of a mechanism used in practicing the method).

2. Substitute Claim 29

A method for fetching a [fresh] content over the Internet[, requested by a first device, identified in the Internet by a first identifier,] from a first server identified in the Internet by a second identifier via a group of multiple [tunnel] devices, each identified in the Internet by an associated group device identifier,

S733 describes the retrieval by a client (first device) of a **“fresh” content** or non-cached content from a data server (first server) where the requested content is not already cached by an agent (tunnel device). *See, e.g.*, Ex. 1017 ¶ 0089. Furthermore, as addressed in connection with step (b) below, S733 itself, as well as numerous other analogous references, also disclose tunnel devices and the use of tunneling protocols. Disclosure of the other aspects of the preamble will be clear from the discussion below of the claim steps.

the method comprising the step of partitioning the [fresh] content into a plurality of content slices, each content slice containing at least part of the [fresh] content, and identified using a content slice identifier, and for each of the content slices, comprising the steps of:

Ex. 1017 ¶ 0089 (“The selected agent … stores the information it receives

from the server (both the headers of the request, as well as chunks of the response itself) in its database, for this particular response to the client, as well as for future use to other clients that may request this data….”). S733 further discloses piece-wise retrieval of the slices, as addressed with respect to the steps below. Likewise, as addressed in the Petition, Sharp KK also discloses partitioning content into identified slices, and their retrieval through an intermediate device. The Petition also addressed the rationale for combining Sharp KK and S733. Pet. at 48.

(a) selecting a [tunnel] device from the group;

Ex. 1017 ¶ 0084 (“[T]he client … decides which of the agents in the list to use as its agent for this particular information request.”). (*See* below, where the further “wherein” limitations on what is a “tunnel device,” and how this is met by S733, are specifically addressed.)

(b) sending over the Internet a first request [from the first device] to the selected [tunnel] device using [a tunneling protocol and]the group device identifier of the selected [tunnel] device, the first request including the content slice identifier and the second identifier[, the first request identifies the source of the fresh content as the first server];

Block 360 in Fig. 9 of S733, and correspondingly in ¶ 0081, disclose that client sends the “original request” to all agents in the list received from acceleration server to determine which agent in the list is best suited to assist with the request. Ex. 1017 ¶ 0081 & Fig. 9; ¶ 0106 (2nd emb.). The “all agents” includes the agent regarded as the “selected tunnel device” in proposed substitute claim 29 (Ex. 1003

¶ 0086). An example given for the "original request" is GET http://www.aol.com/index.html HTTP/1.1. Ex. 1017 ¶ 0081. This "original request" corresponds to the "first request" of substitute claim 29. Ex. 1003 ¶ 87.

This request includes both the first content slice identifier, as it identifies the web page content to be fetched (/index.html), which is subsumed by the second identifier, the "complete URL." The "complete URL" further specifies the domain and subdomain (www.aol.com) of the first server "aol.com"—*i.e.*, the server that is the source of the first fresh content, and thus also the second identifier. Ex. 1003 ¶ 88; *see also* Ex. 1017 ¶ 0110 (2nd emb.). This identifier for the index.html web page constitutes a "slice" identifier, insofar as, per the '866 patent, "the content may be a website content comprising multiple webpages, and *the partitioning may be based webpages level*." Ex. 1001, 57:60–67, 104:22–24 (emphasis added).

Moreover, Sharp KK discloses piecewise retrieval at a more fragmentary level where the fragments are requested and identified by content slice identifier as well as the second identifier, as recited in this step. *See* Pet. at 40–41.

Tunneling – This limitation of course also recites communicating with "tunnels" using a "tunneling protocol."

This again raises the question of what exactly *is* tunneling, particularly since this would now be an explicit claim term. The MTA does not address the scope of the terms "tunnel" or "tunneling protocol." At best, it offers a circular definition of

"tunnel device." MTA at 10 ("[A] tunnel device is a very specific type of client device that is … configured to be a tunnel device…."). The claim language does not address what a tunnel device is, functionally, other than to limit its usage thereof to a consumer device running a consumer operating system. The MTA also does not purport to take a position on the meaning of "tunneling protocol."

However, RFC 2616 (Ex. 1007 § 1.3 at 10) defines "tunnel" as "[a]n intermediary program which is acting as a blind relay between two connections."[3] The proposed claim reinforces the intended "blind relay" nature of a tunnel by changing the word "from" (in step c below), to "via," implying a mere pass-through. As for "tunneling protocol," the '866 patent describes this as "where one network protocol (the delivery protocol) encapsulates a different payload protocol." Ex. 1001, 29:34–36. "Tunneling enables the encapsulation of a packet from one type of protocol within the datagram of a different protocol." *Id.*, 29:36–38. Further, according to the '866 patent, "[t]ypically, the delivery protocol operates at an equal or higher OSI [layered network model] layer than does the pay load protocol." *Id.*, 29:45–47; *see* Ex. 1101

[3] Petitioner previously asserted in the IPR regarding the related '044 patent that "tunnel" is not a term of art (IPR2021-00458, Paper 1 at 13 n.3), but on further review this proves to be incorrect. Ex. 1101 ¶ 70 n.1. In any case, Petitioner does not see any material issue with the Board's construction. '044 Inst. Dec. at 20.

¶ 70 (confirming this summary).

S733 discloses tunneling in accordance with these definitions. This is well-reflected in the second embodiment in the S733 reference (beginning at Ex. 1017 ¶ 0103), where pass-through TCP "pre-connections" are established (*id.* ¶ 0107–08), and protocol messages are passed back and forth over those connections (*id.* ¶ 0109–14), including lower or equal layer protocols. Examples given in S733 of "other protocols" carried (*see id.* ¶ 0103), include "Ethernet" (Layer 2 (lower)) over TCP (Layer 4 (higher)), and "UDP" (Layer 4) over TCP (same Layer level) – both "tunneling" according to the explanation in the '866 patent, as well as POSITA understanding. Ex. 1101 ¶ 71. Without question, running Ethernet or UDP over TCP as disclosed in the second embodiment of S733 *is* tunneling. *Id.* ¶ 72.

Moreover, as addressed below, apart from the disclosure of a tunnel arrangement within the second embodiment of S733 itself, using a tunneling protocol would have been an obvious variation on the first embodiment of S733, based on other well-known examples, including examples of tunneling that were pervasive by 2013.

As for the combination of the two embodiments disclosed in S733, its disclosure not only suggests but teaches such combination. The disclosure of the second (tunneling) embodiment expressly refers to the principal figure of the first embodiment (Fig. 3), stating "[f]or purposes of illustration of TCP/IP communication [the extension to tunneling], reference may be made to FIG. 3, wherein the Web server

is a TCP/IP server." Ex. 1017 ¶ 0103. S733's description of its second embodiment makes repeated references to corresponding steps in the first embodiment, *e.g.*, in referring to the selection of an agent, it states: "This step is performed in a similar manner to that described with regard to the main HTTP embodiment of the invention." *Id.* ¶ 0106. It refers to two other steps as well, performed "in the same manner as in the main embodiment." *Id.* ¶ 0111. Likewise, the description of the first embodiment similarly discloses that its server 152 "is not limited to being an HTTP server" and that "the present invention may relate to any other communication protocol." *Id.* ¶ 0037; *see also* ¶¶ 0056, 0098. A POSITA would understand from these parallels throughout the disclosure and the use of Fig. 3 in S733 to explain the second embodiment, that the "messaging" phase of the second embodiment, though designed for many protocols, would also equally include where the carried protocol was HTTP (as used in the first embodiment). Ex. 1101 ¶ 75.

Beyond these disclosures within the four corners of S733 itself, it is also the case that merely using a tunneling protocol in conjunction with even the first embodiment of S733 (even if S733 had stopped there) would have been obvious.

As of the 2013 date of the claimed invention, it was routine and ordinary to use tunneling protocols through proxies for fetching content. This is evident in S733 itself as well as several of the other references already cited in the Petition.

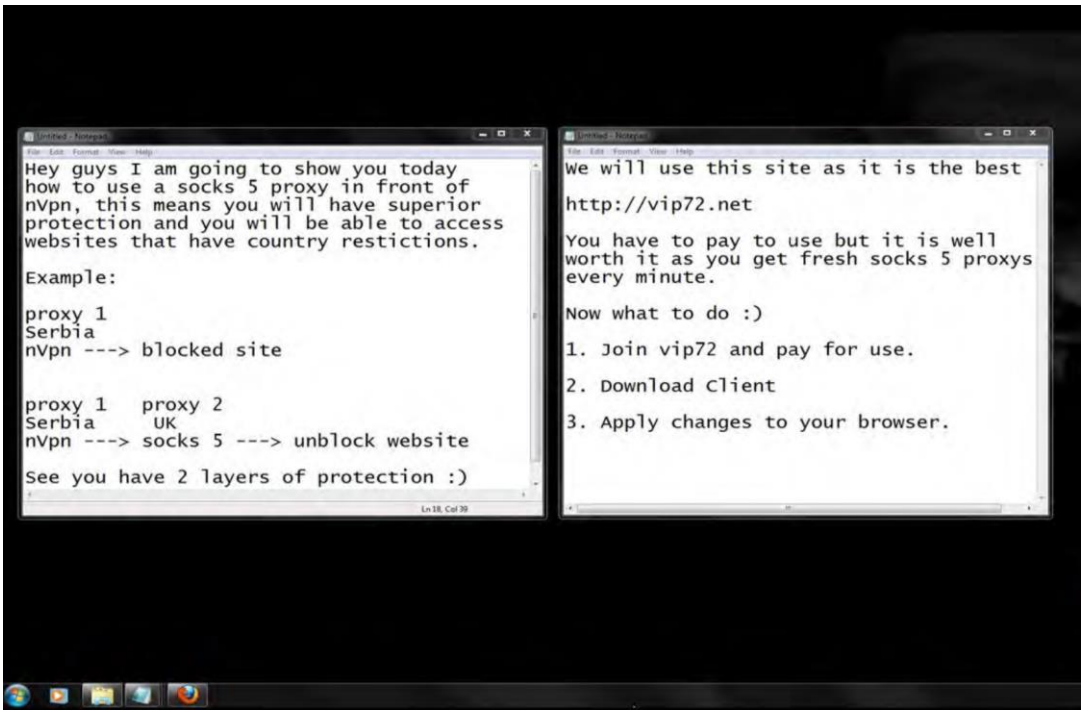
For example, Prince, cited as Ex. 1021 in the Petition of the '044 patent, and

cited as Ex. 1114 here, discloses a proxy, likewise "brokered" from a plurality of available intermediate devices as in substitute claim 29, which is used to tunnel incompatible versions of the IP protocol: IPv6 over IPv4 (an example of tunneling communications which are at the *same* network layer): "In another embodiment, the transition module 225 *encapsulates the packet carrying the incoming request into a packet of a different protocol type* when transitioning to a different IP version type for an outgoing request." Ex. 1114 ¶ 0072 (emphasis added), ¶ 0071 (IPv6/IPv4), ¶ 0073 (HTTP/HTTPS).

Also disclosed in Prince (Ex. 1114 ¶ 0073) is "HTTPS" (secure HTTP, which uses encryption to protect against eavesdroppers on a browsing session) is an extremely common use case (and was in 2013). Ex. 1101 ¶ 79. Like HTTP, HTTPS must often be accessed through proxies, for example because of institutional firewalls requiring proxies for Internet access. *Id.* ¶ 80. Requests and responses via https that go through a proxy must be tunneled, because https involves an *encrypted* stream that the proxy cannot read. The proxy in such a case cannot read, rewrite, and relay such content requests, and can only pass them through in encrypted form and unmodified. This issue is so prevalent that a special HTTP command, called "CONNECT" (which differs from the lower-layer TCP CONNECT) had to be created to allow for persistent HTTP connections (over TCP) so that communications such as https could be tunneled over HTTP proxies. *See* Ex. 1007 § 9.9, p. 57 (1999) ("This

specification reserves the method name CONNECT for use with a proxy that can dynamically switch to being a tunnel (e.g. SSL tunneling [44].”); *see also* Ex. 1113 § 5.2 (documenting the method); Ex. 1101 ¶ 81. It would have been more than obvious – indeed a commercial *necessity* by 2013 – to include HTTPS capability in any commercially-offered system along the lines of S733, because otherwise users would be unable to use the system, as they were by that date accustomed to doing, to securely access web content. *Id.* The method already in S733 would have been sufficient to carry HTTPS. *Id.*

To the same effect is VIP72.com, likewise cited in the Petition against the ’044 patent (Ex. 1116 at 8 (Ex. 1028 in IPR2021-00458)).



Though the Board expressed concern as to *documentary* disclosure of some

claim limitations by VIP72.com as a primary reference, it remains a strong secondary reference in combination with S733, at least for the limited point of using a tunneling protocol over a proxy, reflected in the above text. VIP72.com was seeking to address the same need as in S733 and the '866 patent for proxies available on demand, and on its face it discloses, in written form, using a tunneling protocol (socks 5, all the way to the data server, as well as VPN, just between the first device and the tunnel device) as well as anonymity ("protection") from the origin server. *See also* Ex. 1009 (RFC 1928), documenting the SOCKS protocol, version 5 (*i.e.*, socks 5) as of March 1996, as a protocol to "transparently and securely traverse a firewall" (*id.* at 1), with requests and responses that may be "encapsulated" (*i.e.*, tunneled) within a TCP communication (*id.* at 4, 6). Ex. 1116 reflects a printed publication (on YouTube) which, as addressed in the Petition was publicly available as pictured above in 2011 (the text was part of the published video), and was readily understandable to a POSITA as teaching the use of a tunneling protocol (socks 5) for anonymity purposes, through brokered proxies. Ex. 1101 ¶ 83.

Reed (Ex. 1105), discussed at length in the '866 patent (Ex. 1001, 28:3–29:33), is not limited to particular hardware and is based on retrieval through a network set up by "longstanding socket connections" (Ex. 1105, 4:35–39) among intermediary devices ("onion routers") by encrypted communications tunneled through the onion routers over the established connections (*e.g.*, Abstract). A POSITA

understands this as tunneling, because every communication is blindly relayed through the intermediary. Moreover, every message transported is the same or lower layer than the layer of the tunnel (*id.*, 1:67–2:5), further fitting the definition of "tunneling protocol" in the '866 patent itself. Ex. 1001, 29:34–47. Ex. 1101 ¶ 84.

(c) in response to receiving the sent first request by the selected [tunnel] device, receiving over the Internet the content slice [from the first server via] ~~from~~ the selected [tunnel] device; and

All requested content from the first server must at least the first occasion come from the first server. Ex. 1101 ¶ 85. When it is so obtained, it is distributed among peers in S733 per ¶ 0089 therein and thereby becomes cached. If so cached, the slices are sent to requesting clients as requested (Ex. 1017 ¶¶ 0091–92). If not so cached, the requesting agent (tunnel) gets the requested content from the first server and lists itself as the only peer for the slices involved (*id.* ¶ 0094), and the requesting client gets the requested content slice via the same tunnel – satisfying the limitation. Ex. 1101 ¶ 85. The disclosure of the second embodiment in S733 makes clear that it has the same capability, but through its pre-established TCP connections (*i.e.*, tunnel). Ex. 1017 ¶¶ 106–10.

[(d) in response to receiving the content slice, sending the content slice to the first device using the first identifier and;]

The agent (tunnel device) in S733 sends the content slice to the first device using its Internet identifier (IP address), and does so in response to itself receiving the content slice. *See* Ex. 1017 ¶ 0089 ("The selected agent … provides itself as the

only peer for [the received] chunks … [and] [t]his list is then sent back to the client [necessarily using its IP address]), ¶ 0090 ("the client sends a request to each of the peers listed for the chunk [only the selected agent in this case, listed as the only peer] to download the chunk"). Similarly as to Sharp KK. Ex. 1018 ¶ 281; Ex. 1101 ¶ 86; *see also* Ex. 1003 ¶ 74.

wherein the method further ~~comprising~~[comprises] the step of constructing the [fresh] content from the received plurality of content slices, and

See Ex. 1017 ¶ 0095 ("The client … checks whether all of the chunks for this request were received," also disclosing that "the client … passes the data on to the Web browser or other application of the client that made the original request, for it to use as it had originally intended."). A POSITA understands the "use as intended," *e.g.*, by a web browser, to mean constructing the received fresh content for presentation to a user, and in any case this is obvious. Ex. 1101 ¶ 87. Similarly, *see* Pet. at 41 as to Sharp KK.

wherein each of the [tunnel] devices in the group is a client device [comprising a consumer electronic device with a client operating system and

S733 discloses consumer devices as peers. A stated object of S733 is "making the Internet faster *for the consumer.*" Ex. 1017 ¶ 0008. The consumer is thus using the "client communication device[s]" disclosed in S733 to realize the claimed benefits. Ex. 1101 ¶ 88. S733 discloses a plurality of distributed peer devices having switchable functionality: "communication device 200 of FIG. 4 may serve as a

client, agent, or peer." Ex. 1017 ¶ 0041; *see also* Ex. 1017 ¶¶ 0035, 0059 (same). The specification imposes no special requirements on the components of this device. *See id.* ¶ 0041. Its memory (210) "may contain an operating system (O/S) 230" (¶ 0045) and also an "Internet browser" or an 'email program" (Figs. 4 and 5, ¶¶ 0045–46), shown as browsing sites such as aol.com (¶ 0078) – typical consumer applications and uses. Ex. 1101 ¶ 89. This functionality is provided by a software application implementing client-agent-peer functionalities in parallel (Ex. 1017 ¶ 0059), which the device obtains by download (*id.* ¶¶ 0073, 0102). Thus, agent 122 (first tunnel device) of S733, which is simply one of the plurality of peers participating in the specified consumer Internet acceleration scheme, satisfies this limitation. Ex. 1101 ¶ 89.

wherein the second identifier is a complete URL and

As explained above, for the purposes of § 103 analysis, we assume a "complete URL" is of the form "https://www.youtube.com/watch?v=9mSb3P7cZIE?ST=1:48," or at least http://www.youtube.com (or contains the latter), as identified by PO. As described above, S733 discloses the use of a second identifier of this form, *i.e.*, http://www.aol.com/index.html (*e.g.*, Ex. 1017 ¶ 0081), which, to the extent "complete URL" may be understood, either is or contains a "complete URL." So does Sharp KK, in a request to a proxy. *See, e.g.*, Ex. 1018, Fig. 8 & ¶¶ 107–10.

wherein the first device remains anonymous as to the first tunnel device and the first server].

To the same extent supported in the '866 specification, this limitation is disclosed in S733, in which client 102 can remain anonymous from web server 152. That is because clients retrieve requested content from peer caches whenever possible and when fresh content is needed it is only the selected agent that makes the corresponding request to the data server, revealing the agent's IP address, but not the requesting client's. Ex. 1017 ¶ 0089 ("the selected agent then sends the request directly to the server"). This is exactly the same basis on which the '866 patent states (Ex. 1001, 88:1–9) that it provides anonymity. Ex. 1101 ¶ 91. The written description only supports anonymity as between the first device and the data server, because as addressed above the specification and claims recite direct communications between the first device and tunnel device (*e.g.*, Ex. 1001, 88:24–26 ("Content Request" message "is … sent from the first client device … to the selected tunnel device"), as well as claim step b) and fail to support (and in the case of the '866 patent with its portioning and caching of content, even enable) anonymity of the first device from the tunnel device. Ex. 1101 ¶ 92.

3. Substitute Claims 30–38

Substitute claims 30–38 contain no substantive amendments, other than as derived from base claim 29. *See* Ex. 2021 at 1–2. The obviousness of the separate limitations of the dependent claims are fully addressed in the Petition, and nothing in

the amendments to the base claim changes the grounds previously stated as to the dependent claims. *See* Pet. at 43–50, 54–55, 57.

IV. CONCLUSION

For at least the foregoing reasons, the substitute claims are unpatentable and the motion to amend should be denied.

Respectfully submitted,

/Ronald Abramson/
Ronald Abramson, Reg. No. 34,762
Ari J. Jaffess, Reg. No. 74,558
M. Michael Lewis, Reg. No. 50,478

Dated: January 31, 2022

LISTON ABRAMSON LLP
The Chrysler Building
405 Lexington Avenue, 46 FL
New York, NY 10174
Telephone: (212) 822-0163

CERTIFICATION OF PAGE COUNT

The undersigned hereby certifies that the portions of the above-captioned Petitioner's Opposition to Patent Owner's Non-Contingent Motion to Amend specified in 37 C.F.R. § 42.24(a)(1) include 25 pages, in compliance with the 25-page limit set forth in 37 C.F.R. § 42.24(b)(3). This page count was prepared using Microsoft Word/Office 365.

Dated: January 31, 2022

/Ronald Abramson/
Ronald Abramson

CERTIFICATE OF SERVICE

The undersigned certifies that on January 31, 2022, a complete and entire copy of this Petitioner's Opposition to Patent Owner's Non-Contingent Motion to Amend was provided to the Patent Owner by filing through the PTAB E2E System and via email to Thomas M. Dunham <tomd@ruyakcherian.com> and Elizabeth A. O'Brien <elizabetho@ruyakcherian.com> as authorized in Patent Owner's mandatory notices.

Dated: January 31, 2022

/Ronald Abramson/
Ronald Abramson