

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

U.S. Patent No. 9,742,866

EXHIBIT 1101

**DECLARATION OF KEITH J. TERUYA
IN SUPPORT OF PETITIONER'S OPPOSITION TO
PATENT OWNER'S NON-CONTINGENT MOTION TO AMEND**

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

I, KEITH J. TERUYA, declare the following:

1. I have been retained by counsel for NetNut Ltd. to provide my opinions on certain issues in connection with substitute claims 29–38 of U.S. Patent No. 9,742,866 (the '866 patent), as shown in Ex. 2021 (Appendix A-2).

2. I am being compensated at a normal hourly rate for my time in preparing this declaration, with reimbursement for actual expenses. My compensation is not tied to the outcome of this matter, and not based on the substance of the opinions rendered here.

3. In preparing my opinions expressed herein, I have reviewed the '866 patent and its prosecution history and all of the patents and printed publications listed in Exhibit 1103. I may rely upon these materials, my knowledge and experience, and/or additional materials to rebut arguments raised by the patent owner. Further, I may also consider additional documents and information in forming any necessary opinions, including documents that may not yet have been provided to me.

4. I am familiar with the technology described in the '866 patent as of its earliest claimed priority date of August 28, 2013. I have been asked to provide my technical review, analysis, insights, and opinions regarding the '866 patent, including patentability issues regarding substitute claims 29–38. I have used my experience and insight along with the above-noted references as the basis for my

opinions, which support the grounds of unpatentability set forth in Petitioner's Opposition to Patent Owner's Non-Contingent Motion to Amend.

I. QUALIFICATIONS

5. I have a long professional background in information technology and network engineering, and for the past 20 years I have been the chief executive officer of a specialized Internet hosting company that I founded, which among other things provides Tier I Network Operations Center capabilities for corporations, local municipalities, Federal Government programs, and regulatory agencies in and around southern California.

6. My day-to-day work in my present capacity involves direct hands-on as well as strategic involvement in the issues of networked data distribution and access addressed by the '866 patent, including without limitation architecting and configuring high-capacity content servers, proxy servers, content distribution networks (CDNs), edge and origin servers, peer-to-peer communications, as well as the lower-level routing and switching infrastructure and communications protocols and standards underlying such systems.

7. In prior positions, I was the Chief Technology Architect (in addition to being the CEO) for 15 years for a company I founded that was the original communications technology "skunk-works" for Novell Inc. In this capacity, I designed basic and advanced telecommunications and network interfaces for Novell and

other companies and developed a mastery of the standards and protocols underlying the Internet. I authored the Network Communications Services Interface (“NCSI”) that became a de-facto communications software LAN/WAN standard, with more than 3 million deployments of software. I also developed protocol adjustments in Novell IPX Protocol for adaptive packet buffering required by LAN/WAN communication (Asynchronous and LAPB X.25) gateways, receiving Industry Product of the Year awards for successive years (1988, 1990, 1991 and 1996).

8. I previously served for 10 years architecting network information processing technologies for Goldman Sachs as a senior consultant. In this capacity, I was the architect, designer, development manager, and developer in Goldman’s Network Workstation Technologies Department. I was also the architect of Goldman’s product strategy and deployment of online delivery of consolidated live market data information into local and wide area network-based workstations for mission critical securities trading operations in the worldwide trading rooms of the firm. In particular, I developed proprietary adaptive buffering protocols to mitigate stream delays when terrestrial transatlantic data links were routed through backup satellite connections affecting the flow of streaming market data feeds used for program trading operations.

9. As Chief Technology Officer of ShowBizData Inc. between 2000 and 2002 as an “early adopter” pioneered the online Internet streaming of various lived events of the Cannes Film Festival, BFTA Awards and the Sundance Film Festival using both commercial and proprietary systems we architected and developed.

10. I am also a Network Computing Paradigm Award recipient.

11. A copy of my curriculum vitae is attached as Exhibit 1102.

12. I believe that I am qualified to provide reliable opinions in the field of the '866 Patent, including what a person of ordinary skill in the art (“POSITA”) would have understood from the prior art in this field at that time and his or her view of obviousness therein.

II. LEGAL STANDARDS I HAVE BEEN ASKED TO APPLY

My Understanding of Patent Owner’s Required Threshold Showing

13. I have been informed that a threshold showing from the Patent Owner is required before amended claims are considered by the Board. I further understand that this specifically requires Patent Owner to show that its substitute claims (i) respond to a ground of unpatentability; (ii) do not enlarge claim scope; and (iii) do not introduce new matter.

My Understanding of Indefiniteness, Enablement, and Written-Description Support

14. I understand that for claim language to be sufficiently definite for compliance with 35 U.S.C. § 112(b), the claim language must inform a POSITA with reasonable certainty of the claim scope.

15. I understand that to provide adequate enablement to comply with 35 U.S.C. § 112(a), a patent must provide sufficient detail so that a POSITA can make and use the claimed invention without having to resort to too much experimentation. While some experimentation can be okay, undue experimentation is not.

16. I understand that to provide adequate written-description support to comply with 35 U.S.C. § 112(a), a patent must describe the claimed invention in sufficient detail so that a POSITA can reasonably conclude that the inventor had possession of the claimed invention. I have also been informed that the Patent Owner is forbidden from relying on essential material present only in a provisional application that was incorporated by reference. It is my understanding that 37 C.F.R. § 1.57(d) explains that “‘Essential 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.” 37 C.F.R. § 1.57(d).

My Understanding of Obviousness

17. I understand a patent claim is invalid if the claimed invention would have been obvious to a POSITA at the time the invention was made. This means

that even if all of the requirements of the claim cannot be found in a single prior art reference that would anticipate the claim, the claim can still be invalid based on a combination of references that would have been obvious to a POSITA at the time of the invention.

18. I understand that an obviousness analysis requires an understanding of the scope and content of the prior art, any differences between the alleged invention and the prior art, and the level of ordinary skill in evaluating the pertinent art.

19. I further understand that to prove prior art or a combination of prior art renders a patent claim obvious, it is necessary to: (1) identify the particular references that, singly or in combination, make the patent claim obvious; (2) specifically identify which elements of the patent claim appear in each of the asserted references; and (3) explain how the prior art references could have been combined in order to create the inventions claimed in the challenged claim, and why it would have been obvious to a POSITA at the time of the alleged invention to have made that combination. I also understand that it is sufficient to establish invalidity if the combined limitations of any one embodiment within the scope of the claim may be found in or are obvious over the prior art.

20. I understand that exemplary rationales that may support a conclusion of obviousness include:

- Combining prior art elements according to known methods to yield predictable results;
- Simple substitution of one known element for another to obtain predictable results;
- Use of known technique to improve similar devices (methods, or products) in the same way;
- Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
- “Obvious to try” – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
- Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; and
- Some teaching, suggestion, or motivation in the prior art that would have led a POSITA to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

21. I further understand that the above list of rationales provided is not all-inclusive. Other rationales may also be sufficient, so long as there is a link

between the factual underpinnings relied on and an articulated rationale for why those factors render the invention obvious.

22. I understand certain objective indicia can also be important evidence regarding whether a patent is obvious or nonobvious. Such indicia include: (1) commercial success of products covered by the patent claims; (2) a long-felt need for the invention; (3) failed attempts by others to make the invention; (4) copying of the invention by others in the field; (5) unexpected results achieved by the invention as compared to the closest prior art; (6) praise of the invention by the infringer or others in the field; (7) the taking of licenses under the patent by others; (8) expressions of surprise by experts and those skilled in the art at the making of the invention; and (9) the patentee proceeded contrary to the accepted wisdom of the prior art. I understand that to have legal weight, there must be a nexus—a connection—between any such secondary considerations and the alleged invention.

23. I also understand that “obviousness” is a legal conclusion based on the underlying factual issues of the scope and content of the prior art, the differences between the claimed invention and the prior art, the level of ordinary skill in the field of the prior art, and any objective indicia of non-obviousness. For that reason, I am not rendering a legal opinion on the ultimate legal question of obviousness.

24. Rather, my testimony addresses the underlying facts and provides factual analysis that would support a legal conclusion of obviousness or

nonobviousness. When I use the term obvious, it is with reference to the perspective of one of ordinary skill at the time of claimed invention.

III. CLAIM CONSTRUCTION

25. I understand the Board construed certain claim terms in the Institution Decision, prior to Patent Owner’s amendments. Those constructions are summarized below:

Claim Terms	Board’s Construction
“client device”	“a device that is operating in the role of a client by requesting services, functionalities, or resources from other devices”

Paper 11 at 14–15.

26. To the extent these constructions are applicable to substitute claims 29–38, I apply them herein.

IV. LEVEL OF ORDINARY SKILL IN THE ART

27. I understand the Board adopted the definition of a person of ordinary skill in the art I articulated in my prior declaration, dated January 24, 2021. Paper 11 at 11–13. I apply this definition herein.

V. OVERVIEW OF THE ’866 PATENT

28. I discussed the ’866 patent and background in my previous declaration. Ex. 1003 ¶¶ 28–34. I incorporate that that discussion herein.

VI. OVERVIEW OF THE SUBSTITUTE CLAIMS

29. The original claims were addressed at length in my prior declaration. The original claims of the '866 patent differ from the claims of the companion '044 patent primarily with regard to the further claimed aspect of piece-wise retrieval of the requested content (in content “slices”). The changes in the proposed substitute claims, however, do not directly address the content slice aspect, focusing instead on making corresponding amendments to the features that are *in common* between the '044 and '866 claims. As Patent Owner has done with respect to the '044 patent, the thrust of the proposed amendments for the '866 patent is likewise to seek to add limitations that specify “tunneling”—reciting that the intermediate devices used for content retrieval (sliced or not) will be “tunnel devices” (further specified to be “consumer electronic devices” with “client operating systems”) and that the request from the first device to the first tunnel device in particular uses a “tunneling protocol.” The amendments also specify the use of a “complete URL” in identifying the origin content server (second server), and the claimed results of anonymity with respect to the tunnel device as well as the second server, as well as specifying various clarifications, such as that the method steps are performed by the first device; that the content retrieved is “fresh” content; that the first device receives the second identifier from the first server “in response to the first request”; and that

it receives the requested content from the tunnel device “in response to the second request.”

VII. SCOPE AND CONTENT OF THE PRIOR ART

30. I discussed the scope and content of prior art to the '866 patent, including European Pat. Publication No. EP 2 597 869 A1 by Sharp KK (“Sharp KK”) (Ex. 1018); U.S. Patent Publication No. 2011/0087733 to Shribman *et al.* (“S733”) (Ex. 1017); and Internet RFCs and Standards in my previous declaration in this proceeding. Ex. 1003 ¶¶ 49–63. I incorporate that discussion herein.

31. In my declaration regarding related U.S. Patent No. 9,241,044 (the “’044 patent”), I discussed the scope and content of certain other prior art, including VIP-72.com (Ex. 1115–18) and U.S. Patent Publication No. 2013/0080575 to Prince *et al.* (“Prince”) (Ex. 1114). IPR2021-00458, Ex. 1003 ¶¶ 36–63. I incorporate that discussion herein.

32. As will be addressed, a number of the references originally cited herein teach “tunneling” communications through intermediary devices. Further responsive in this regard is Reed, *et al.*, U.S. Patent No. 6,266,704 (“Reed”) (July 24, 2001), cited herein as Ex. 1105. Reed and technically related publications by the same group at the U.S. Naval Laboratory, concerning “onion routing” and the TOR anonymity network, are cited and discussed at length in the '866 Patent (Ex. 1001, 28:3–29:33). These references are addressed in the '866 patent as “Background”

but become particularly relevant as Patent Owner now seeks to make a patentable distinction out of “tunneling.”

33. Reed teaches the use of a tunneling protocol through a chain of intermediary devices, with a layer of encryption for each intermediary node in the path to a responding device. Ex. 1105, Abstract, Fig. 2, 3:21–41. The chain of intermediaries is established by “longstanding socket connections” (4:35–39), established at the application (highest) network layer (1:67–2:5). None of the intermediate nodes know both the identity of the requester and the content of its requests or responses, and the responding device (*e.g.*, web server) cannot determine the identity of the requesting device, thereby providing strong anonymity (Abstract).

VIII. LACK OF ADEQUATE WRITTEN DESCRIPTION

34. Fig. 5 of the ’866 patent is representative of the subject matter.

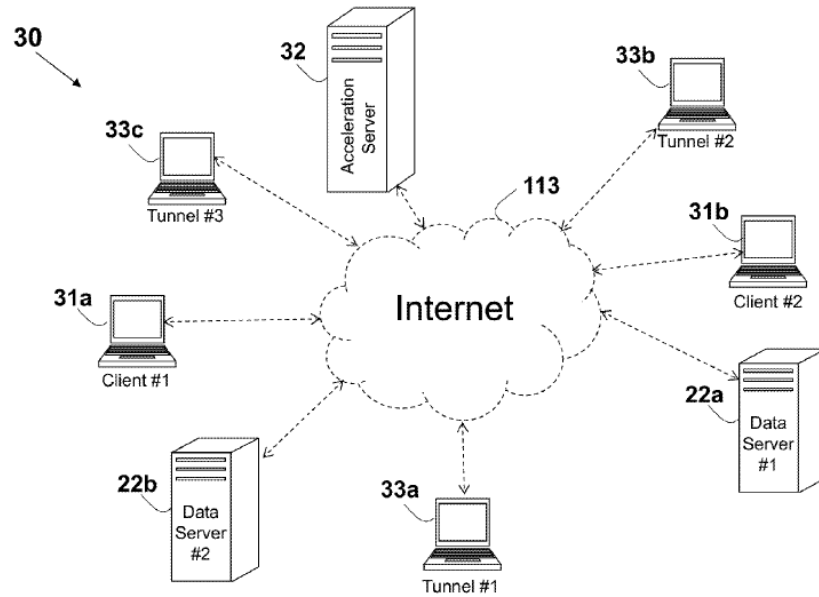


FIG. 5

35. The terms of Patent Owner’s proposed amendments in the substitute claims may be mapped onto Fig. 5 as follows:

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

36. As stated above, I understand that Patent Owner may not rely upon Prov. App. No. 61/870,815 to satisfy the written-description support requirement of 35 U.S.C. § 112(b).

“Complete URL”

37. A “wherein” clause in the proposed amendment specifies that the *second identifier* is a “complete URL.”

38. A POSITA would understand that, in sending an Internet content request through an intermediary, there is nothing special (or unusual) about using a “long” format for the request, that is, a format that specifies the full network path to the responding device, and/or the full path on the device itself to the requested content (exactly what such an identifier might be is addressed below, with regard to indefiniteness). The applicable standards, including RFCs 3986 and 2616 (*e.g.*, Ex. 1017 § 5.1.2) document numerous permissible forms of requests that meet such requirements.

39. 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. However, this is not a URL for the data server (it is a URL for *content* on the data server).

40. A field *within* this expression, “www.youtube.com”, *does* identify an origin server. However, I do not see that the MTA even addresses or intends this, and in any case the issue of what a particular *database* may contain fails to address whether the “*first request* includ[es] ... the second identifier” in the prescribed form of a “complete URL.”

41. I do not see in the subject patent specification any specified format or content for the “first request” that “includ[es] the second identifier” in the form of a “complete URL.” Ex. 2020 cites nothing any more pertinent than the above-mentioned database (*e.g.*, Ex. 2026, Fig. 15a). The other references are generalities, such as the word URL by itself (*e.g.*, *id.* at 72–73, 145). The disclosure fails to reflect the format of the claimed first request itself, *i.e.*, the content request from the client device to the tunnel device.

42. This information is also missing from the drawings. *See, e.g.*, Ex. 2026 at Fig. 5b (element 56g), as well as Ex. 2025 at 114), which simply show a “Content Request” without disclosing the format of the request.

43. In sum, Patent Owner points to no written-description support for anything that may reasonably be considered a “complete URL” within a request from a first device to a tunnel device, as an identifier of the origin server from which specified content is being sought.

44. 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. A POSITA would understand that 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. There is thus no teaching here, express or implied, specifically as to the format of the request from the first device to the tunnel device.

45. The written description does mention the sending of 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. The Patent Owner here has failed to explain why a person of ordinary skill in the art would have recognized from the written description that the inventor possessed the claimed subject matter.

The Claimed Anonymity Features

46. 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.

47. Patent Owner argues that “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.” MTA at 12. 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.

48. In Ex. 2020 (App’x A-1), at page 20, Patent Owner, without argument, seeks support for anonymity, from the tunnel device, 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:

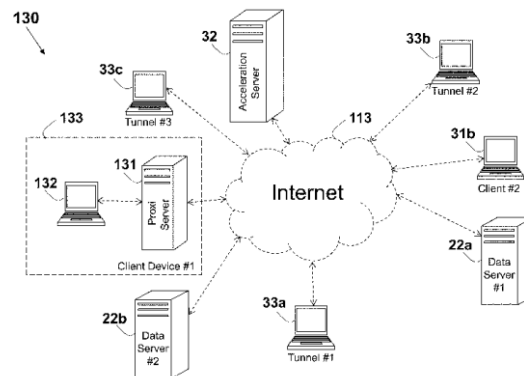


FIG. 13

49. 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 (it doesn't even imply that the proxy 131 has any different external address than the client itself). As the Board already noted with regard to Fig. 13, "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).

50. Fig. 13 does not at all reflect anonymity established as between the client (first device) and the tunnel with which it communicates. Patent Owner has again failed to explain its possession of this aspect of the claimed invention.

IX. LACK OF ENABLEMENT OF ANONYMITY FROM THE TUNNEL DEVICE

51. 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, in order to serve them.

52. 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 is a further reason why the written description fails to enable, the claimed anonymity as to the tunnel device.

X. “COMPLETE URL” IS INDEFINITE

53. I have been instructed that, under the applicable law, patent terms must be sufficiently clear to inform persons of skill in the art, with reasonable certainty, as to their scope. The scope and meaning of the term “complete URL” as used in the proposed amended claims falls short of this requirement, in my opinion.

54. The proposed amendments themselves provide no indication of what “complete URL” means. Patent Owner does not even purport to cite any support for the meaning of this term from its expert, Dr. Rhyne (who submitted nothing further in support of this motion). The term does not appear in the written description or original claims.

55. The term “complete URL” (referred to above as generally suggesting a “long”-form format) has been used informally to connote a combination based on the absolute and relative forms of a URL (*see* Microsoft, Absolute and Relative URLs, <https://docs.microsoft.com/en-us/sql/ado/guide/data/absolute-and-relative-urls?view=sql-server-ver15#:~:text=An%20absolute%20URL%20contains%20all,the%20absolute%20and%20relative%20URLs> (Aug. 27, 2020, retrieved January 30, 2022) (“*In effect*, the ‘complete URL’ of the target is specified by concatenating the absolute and relative URLs” (emphasis added)). However, as

is evident from the wording of this quote itself (*i.e.*, “in effect”), this is not in my view intended as a precise definition. Since the relative form of the URL contains the path to the resource, and the absolute form does as well, taken literally, a mere “concatenation” as suggested would be redundant and result in two path strings (resulting in an error). The most that can be said in my view is that a POSITA might regard a “complete URL” as a URL sufficient to positively specify both the location of the server from which a response is ought and what specific resource on that server is being sought. But this falls short of a precise definition of how to format such a URL. In addition, because it addresses the content as well as the origin of the content, it does not align with the claim language, which is directed to an identifier specifically for the recited first server – not the content on the server. Thus, such an understanding of “complete URL” as informally indicated in the Microsoft materials does not provide the degree of certainty for patent claim terms that I understand the law requires.

56. Patent Owner’s submission (Ex. 2020) gives as examples, in alleged support for this term, 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.

57. Patent Owner 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. I therefore see no clear direction in the claim wording itself, the disclosure, or the applicable standards, as to what the limits maybe on what constitutes a “complete URL.”

XI. OBVIOUSNESS OF SUBSTITUTE CLAIMS OVER S733 ITSELF OR IN VIEW OF SHARP KK, PRINCE, REED, AND VIP72.COM

58. As is manifestly clear from its own provisional application (Ex. 2022, 2023), the ’866 patent sought to build directly on the precursor of the inventors’ own previously published S733 disclosure, which previously spelled out a scheme of proxied, chunk-wise retrieval of Internet content (including content not previously cached), through an array of consumer devices (schematically shown in the Ex. 2023 provisional drawings as *laptops* (see Fig. 50 on the first page of the exhibit) with corresponding text that stated: “works as described in Hola patent [serial number of S733]”) (Ex. 2022 at 1). 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, a distinct embodiment in S733 also discloses tunneling. Ex. 1017 ¶ 103 *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 second 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). This second embodiment is in fact “tunneling.” The thrust of these amendments is to add tunneling to the claims, which does nothing to save them under § 103.

59. To begin with, in its institution decision on the ’044 patent, the Board already treated the second device as being a “tunnel,” as it construed this term. ’044 Inst. Dec. at 19–20. This aspect of the amendment merely clarifies how a POSITA would have viewed the original claims, *i.e.*, as reciting “a device operating to receive requests from client devices for content from a data server, that fetches the requested content from the data server, and that sends the retrieved content to the client device,” per the Board’s existing construction (*id.* at 20). Expressly specifying that the “second device” is a “tunnel device” only reflects a characteristic that was already present.

60. Furthermore, the MTA points to nothing about a tunneling device, tunneling protocols, the use of consumer electronic devices, or “complete URLs” that change steps of performing the claimed method. The architecture remains the same and the information exchanged through that architecture remains the same. In addition, the claimed anonymity aspects concern a mere result, which the disclosure does not support in any case to the full extent claimed. These are all differences with no operational significance, nothing that changes the technical substance of the actual *method steps* now being claimed from what they originally were.

61. Moreover, as I will next address, the claimed distinguishing features are in any case readily found in pertinent prior art.

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,

62. 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:

63. As to the “partitioning,” *see* 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. My prior declaration also addressed the combination of Sharp KK and S733. Ex. 1003 ¶ 95.

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

64. *See* 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 also* 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];

65. 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.

66. 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, which, based on its examples in Ex. 2020, is what Patent Owner might regard as a “complete URL.” The “complete URL” (in S733) thus 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).

67. 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.

68. **Tunneling** – This limitation of course also recites communicating with “tunnels” using a “tunneling protocol.”

69. This raises the question of what exactly *is* tunneling? 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.”

70. 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,”¹

¹ I stated in my original declaration in the IPR regarding the related ’044 patent (IPR2021-00458, Ex. 1003 ¶ 29) that the terminology “tunnel device” “is not

and the Board also defined this term in its decision to institute *inter partes* review of the related '044 patent as “a device operating to receive requests from client devices for content from a data server, that fetches the requested content from the data server, and that sends the retrieved content to the client device.” '044 Inst. Dec. at 19–20. 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.

standard.” This particular wording was inartful, in that my declaration did address “tunneling proxies” at length, and such usage, again as reflected in my prior declaration, is well understood. Furthermore RFC 2616 defines “tunnel” as stated in the text above – which definition reflects the concept I was referring to in discussing tunneling proxies in my opening declaration, though I did not have it in mind at the time that there also happened to be a specific definition of this term in, *e.g.*, RFC 2616, which definition is of course generally accepted. In any case, I do not see any material issue with the Board’s construction of this term in the -00458 IPR. '044 Inst. Dec. at 20.

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.

71. S733 discloses tunneling in accordance with these definitions. This is well-reflected in the second embodiment in the S733 reference (beginning at Ex. 1017 ¶ 103), 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). These are both “tunneling” according to the explanation in the '866 Patent, as well as the noted definitions and a POSITA’s understanding.

72. Without question, running Ethernet or UDP over TCP as disclosed in the second embodiment of S733 is an instance of using a tunneling protocol to send communications through a tunnel device.

73. 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 (again as separately described below) of tunneling that were pervasive by 2013.

74. As for the combination of the two embodiments disclosed in S733, its disclosure not only suggests but teaches to combine the features of the first embodiment in order to better understand the operation of the second. 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.” 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).

75. The sum of these disclosures would be understood by a POSITA to explain how retrieval of web content may be accelerated by employing a network of consumer devices as intermediary retrieval agents, and further to teach embodiments in which such a network may be operated, for a wide variety of communications purposes and protocols, including but not limited to HTTP, over tunneled connections.

76. 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.

77. 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.

78. For example, Prince 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).

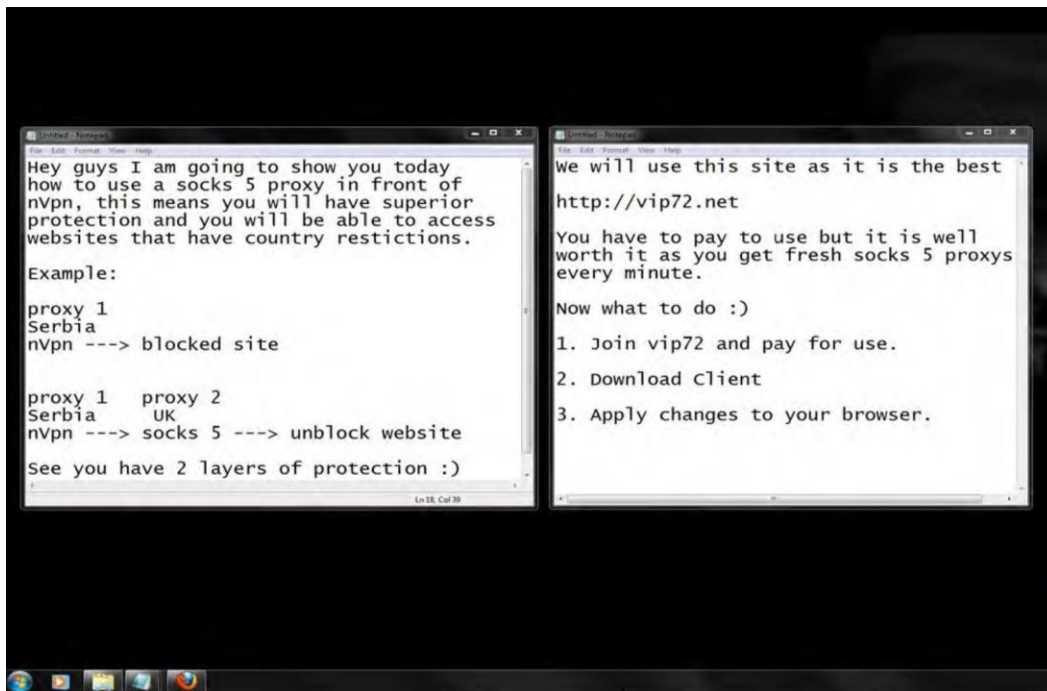
79. Also disclosed in Prince (Ex. 1114 ¶ 0073) is “HTTPS” (secure HTTP, which uses encryption to protect against eavesdroppers on a browsing session) is an extremely common use case (and was in 2013).

80. Like HTTP, https must often be accessed through proxies, for example because of institutional firewalls requiring proxies for Internet access.

81. 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); 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. The method already in S733 would have been sufficient to carry HTTPS as a messaging protocol.

82. 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)).



83. VIP72.com was seeking to address the same need as in S733 and the '044 patent for proxies available on demand. On its face, VIP72.com 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.

84. Reed (Ex. 1105), discussed at length in the ’866 Patent (Ex. 1001, 28:3–29:33), is specifically an anonymity solution that routes communications in multiply-encrypted form over chains of intermediaries (*see* Ex. 1105, 7:44–55). To do so, the communications are routed through the intermediaries over “longstanding socket connections” (4:35–39), established at the application (highest) network layer (1:67–2:5). A POSITA understands this as tunneling because every communication is blindly relayed through the intermediary. Moreover, every message transported is by definition at the same or lower layer than the layer of the tunnel (1:67–2:5), further fitting the definition of “tunneling protocol” in the ’866 patent itself. Ex. 1001, 29:34–47.

(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

85. At such time before any content from a given content server (first server) will have been cached, it all must be obtained (on at least the first occasion)

from the first server, since the claim also says the first server is the source of the fresh content. At such time that it is so obtained, the content 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. The disclosure of the second embodiment 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;

86. While the wording here raises a question as to who might perform this step, it is nevertheless the case that S733 discloses it as drafted. 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]) and ¶ 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. *See* my prior declaration, Ex. 1003 ¶ 74.

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

87. *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.

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

88. S733 discloses consumer devices as peers. S733 discloses a methodology aimed at “making the Internet faster *for the consumer*” (Ex. 1017 ¶ 0008). The stated object was “accelerating data communications ... for at least one client communication device ... originating a data request for obtaining the data from a data server.” *Id.* ¶ 0016. To be sure, the communication device 200 disclosed could be anything containing the “general components of a computer.” *Id.* ¶ 0041. However, it is obvious and there is no question from the disclosure that the “client communication device[s]” disclosed in S733 include consumer devices, because as consumers are the intended beneficiaries of the disclosed technology, and thus the intended

users of the disclosed communication device[s] 200, seeking that benefit. In short, the scheme disclosed is gather a plurality of consumer devices as users, and at the same time make their devices available on a peer-to-peer basis to intermediate cached content retrieval from origin content servers on the Internet.

89. The '866 patent itself draws an equivalence between its devices and those of S733 (as its issued counterpart, U.S. Pat. No. 8,560,604) (Ex. 1001, 83:13–24), and it utilizes 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). As noted, 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. This functionality is provided by a software application implementing client-agent-peer functionalities in parallel (¶ 0059), which the device obtains by download (¶¶ 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, is also a client, and may thus be the device of a consumer, *i.e.*, a consumer electronic device with a client operating system.

wherein the second identifier is a complete URL and

90. As explained above, for the purposes of § 103 analysis, I will 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 Patent Owner. 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:

```
( c ) Session 120 "Client 4a To Proxy 3a" Content Request(1 2 1)
GET http://example.com/content1 HTTP/1.1
Accept: video/mp4
Host: example.com
```

See, e.g., Ex. 1018, Fig. 8 & ¶¶ 107–10. Sharp KK is just an example of the form in which such a content request may be made. The illustrated format, in “absoluteURI” form, is no different than that expected under RFC 2616, as addressed above.

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

91. 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.

92. 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.

Substitute Claims 30–38

93. 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 I addressed in my prior declaration as to the dependent claims. Ex. 1003 ¶¶ 79–99, 108–09, 114–15.

* * * * *

94. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark and that I may accordingly be subject to cross-examination. If such cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

95. This declaration represents only those opinions I have formed to date. I reserve the right to revise, supplement, and/or amend my opinions stated herein based on new information and on my continuing analysis of the materials produced in this proceeding.

I declare under penalty of perjury that the foregoing is true and correct.

Executed at McMinnville, Oregon on January 31, 2022.


KEITH J. TERUYA