IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Larson *et al.*
U.S. Patent No.: 7,921,211 Attorney Docket No.: 38868-0007IP3
Issue Date: April 5, 2011
Appl. Serial No.: 11/840,560
Filing Date: August 17, 2007
Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

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

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 7,921,211 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

I. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1) 1
A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1) 1
B. Related Matters Under 37 C.F.R. § 42.8(b)(2) 1
C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3) 2
D. Service Information 3

II. PAYMENT OF FEES – 37 C.F.R. § 42.103 3

III. REQUIREMENTS FOR IPR UNDER 37 C.F.R. § 42.104 3
A. Grounds for Standing Under 37 C.F.R. § 42.104(a) 3
B. Challenge Under 37 C.F.R. § 42.104(b) and Relief Requested 3
C. Claim Construction under 37 C.F.R. §§ 42.104(b)(3) 5
1. Domain Name (Claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60) ... 6
2. Domain Name Service System (Claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60) 6
3. Indicate/Indicating (Claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60) 7
4. Secure Communication Link (Claims 1, 16-17, 20-23, 26-27, 31-32, 35-36, 47, 51, and 60) 8
5. Transparently (Claims 27 and 51) 9
6. Between [A] and [B] (Claims 16, 27, 33, 40, 51, and 57) 9

IV. SUMMARY OF THE ‘211 PATENT 10
A. Brief Description 10
B. Summary of the Prosecution History of the ’211 Patent 10
C. The Effective Priority Date of the Claims of the ‘211 Patent 12

V. MANNER OF APPLYING CITED PRIOR ART TO EVERY CLAIM FOR WHICH AN IPR IS REQUESTED, THUS ESTABLISHING A REASONABLE LIKELIHOOD THAT AT LEAST ONE CLAIM OF THE ‘211 PATENT IS UNPATENTABLE 13
A. [GROUND 1] – Provino Anticipates Claims 1, 2, 6, 14-17, 19-23, 26-28, 33-41, 43-47, 50-52, and 57-60 13
1. Provino Anticipates Claims 1 25
2. Provino Anticipates Claims 36 29
3. Provino Anticipates Claims 60 31
4. Provino Anticipates Claims 2 and 37 33
5. Provino Anticipates Claim 6 34
6. Provino Anticipates Claims 14 and 38 34
7. Provino Anticipates Claims 15 and 39 35
8. Provino Anticipates Claims 16 and 40 35

9. Provino Anticipates Claims 17 and 41 38
10. Provino Anticipates Claims 19 and 43 41
11. Provino Anticipates Claims 20 and 44 41
12. Provino Anticipates Claims 21 and 45 42
13. Provino Anticipates Claims 22 and 46 42
14. Provino Anticipates Claims 23 and 47 43
15. Provino Anticipates Claims 26 and 50 44
16. Provino Anticipates Claims 27, 33, 51, and 57 45
17. Provino Anticipates Claims 28 and 52 46
18. Provino Anticipates Claims 29 and 53 46
19. Provino Anticipates Claims 30 and 54 47
20. Provino Anticipates Claims 31 and 55 48
21. Provino Anticipates Claims 32 and 56 48
22. Provino Anticipates Claims 34 and 58 49
23. Provino Anticipates Claims 35 and 59 49

B. [GROUND 2] – Provino In View of RFC 1034 Renders Obvious Claims 20, 21, 35, 44, 45, and 59 50

C. [GROUND 3] – Provino In View of Kosiur Renders Obvious Claims 29-32 and 53-56 52

D. [GROUND 4] – Provino In View of RFC 2660 Renders Obvious Claims 16, 27, 33, 40, 51, and 57 55

VI. REDUNDACY 57

VII. CONCLUSION 58

EXHIBITS

MSFT-1001	U.S. Patent No. 7,921,211 to Larson et al. ("the '211 patent")
MSFT-1002	Excerpts from the Prosecution History of the '211 Patent ("the Prosecution History")
MSFT-1003	(Reserved)
MSFT-1004	Curriculum Vitae of Roch Guerin
MSFT-1005	(Reserved)
MSFT-1006	(Reserved)
MSFT-1007	(Reserved)
MSFT-1008	U.S. Patent No. 6,557,037 to Provino ("Provino")
MSFT-1009	(Reserved)
MSFT-1010	Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987
MSFT-1011	Postel, J., et al., RFC 1591, "Domain Name System Structure and Delegation," March 1994
MSFT-1012	Rescorla, E., *et al.*, RFC 2660, draft 01, "The Secure HyperText Transfer Protocol," February 1996
MSFT-1013	VirnetX's Opening Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc., et al.*, 6:10-CV-417 (11/4/11) (EDTX)
MSFT-1014	VirnetX's Reply Claim Construction Brief in *VirnetX Inc. v. Cisco Systems, Inc., et al.*, 6:10-CV-417 (12/19/11) (EDTX)
MSFT-1015	Memorandum Opinion and Order in *VirnetX Inc. v. Cisco Systems, Inc., et al.*, 6:10-CV-417 (4/25/12) (EDTX)

MSFT-1016	Action Closing Prosecution (nonfinal) in Inter Partes Reexamination, Control No. 95/001,789, September 26, 2012 (USPTO)
MSFT-1017	Final Office Action in Inter Partes Reexamination – Right of Appeal Notice, Control No. 95/001,856, June 25, 2013 (USPTO)
MSFT-1018	(Reserved)
MSFT-1019	IPR2013-00397, Patent Owner's Preliminary Response
MSFT-1020	IPR2013-00398, Patent Owner's Preliminary Response
MSFT-1021	(Reserved)
MSFT-1022	(Reserved)
MSFT-1023	Declaration of Dr. Roch Guerin re the '211 Patent and Provino
MSFT-1024	Dave Kosiur, Building and Managing Virtual Private Networks (1998) ("Kosiur")

Microsoft Corporation ("Petitioner" or "Microsoft") petitions for *Inter Partes* Review ("IPR") under 35 U.S.C. §§ 311–319 and 37 C.F.R. § 42 of claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60 ("the Challenged Claims") of U.S. Patent No. 7,921,211 ("the '211 patent"). As explained in this petition, there exists a reasonable likelihood that Microsoft will prevail with respect to at least one of the Challenged Claims.

The Challenged Claims are unpatentable based on teachings set forth in at least the references presented in this petition. Microsoft respectfully submits that an IPR should be instituted, and that the Challenged Claims should be canceled as unpatentable.

I. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Petitioner, Microsoft Corporation, is the real party-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '211 patent is the subject of a number of civil actions including: (i) Civ. Act. No. 6:13-cv-00211-LED (E.D. Tex.), filed February 26, 2013; (ii) Civ. Act. No. 6:12-cv-00855-LED (E.D. Tex.), filed November 6, 2012; (iii) Civ. Act. No. 6:10-cv-00417-LED (E.D. Tex.), filed August 11, 2010; (iv) Civ. Act. No. 6:11-cv-00018-LED (E.D. Tex), (iv) Civ. Act. No. 6:13-cv-00351-LED (E.D. Tex), filed April 22, 2013 ("the 2013 VirnetX litigation"); (v) Civ. Act. No. 6:13-mc-00037 (E.D. Tex); and (vi) Civ. Act. No. 9:13-mc-80769 (E.D. Fld).

The ''211 patent is also the subject of two *inter partes* reexamination nos. 95/001,789 and 95/001,856. On September 26, 2012, the Office issued an Action Closing

Prosecution in the '789 proceeding, maintaining rejections of all 60 claims in the '211 patent, including rejections based on a prior art reference relied upon in this Petition. Ex. 1016 at 3, 10. In particular, the Office has rejected each of claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60 as being anticipated by Ex. 1008 (Provino). *Id*. Similarly, on June 25, 2013, the Office issued a Right of Appeal Notice in the '856 proceeding maintaining rejections of all 60 claims (with the exception of claim 11) in the '211 patent. Ex. 1017 at 3.

The '211 patent is the subject of two petitions for *inter partes* review filed by RPX Corporation, which have been designated as IPR2014-00174 and IPR2014-00175. The '211 patent was also the subject of petitions for *inter partes* review filed by New Bay Capital, LLC, which was designated as IPR2013-00378 and subsequently dismissed, and by Apple, Inc., which were designated as IPR2013-00397 and IPR2013-00398 and not instituted.

Concurrently with this petition, the Petitioner is filing two other petitions for *inter partes* review of the '211 patent, identified as attorney docket numbers 38868-0007IP1 and 38868-007IP2.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Microsoft provides the following designation of counsel.

LEAD COUNSEL	BACKUP COUNSEL
W. Karl Renner, Reg. No. 41,265 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 T: 202-783-5070 F: 202-783-2331	Kevin E. Greene, Reg. No. 46,031 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 T: 202-626-6376 F: 202-783-2331

D. Service Information

Please address all correspondence and service to counsel at the address provided in Section I(C). Microsoft also consents to electronic service by email at IPR38868-0007IP3@fr.com.

II. PAYMENT OF FEES – 37 C.F.R. § 42.103

Microsoft authorizes the Patent and Trademark Office to charge Deposit Account No. 06-1050 for the fee set in 37 C.F.R. § 42.15(a) for this Petition and further authorizes payment for any additional fees to be charged to this Deposit Account.

III. REQUIREMENTS FOR IPR UNDER 37 C.F.R. § 42.104

A. Grounds for Standing Under 37 C.F.R. § 42.104(a)

Microsoft certifies that the '211 Patent is eligible for IPR. The present petition is being filed within one year of service of a complaint against Microsoft in the 2013 VirnetX litigation.[1] Microsoft is not barred or estopped from requesting this review challenging the Challenged Claims on the below-identified grounds.

B. Challenge Under 37 C.F.R. § 42.104(b) and Relief Requested

Microsoft requests an IPR of the Challenged Claims on the grounds set forth in the table shown below, and requests that each of the Challenged Claims be found unpatentable. An explanation of how these claims are unpatentable under the statutory grounds iden-

[1]The complaint in the 2013 VirnetX litigation was served on April 23, 2013.

tified below is provided in the form of a detailed description that indicates where each element can be found in the cited prior art, and the relevance of that prior art. Additional explanation and support for each ground of rejection is set forth in Exhibit MSFT-1023, the Declaration of Dr. Roch Guerin ("Guerin Declaration"), referenced throughout this Petition.

Ground	'211 Patent Claims	Basis for Rejection
Ground 1	**1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60**	Anticipated under § 102 by Provino
Ground 2	**20, 21, 35, 44, 45, 59**	Obvious under § 103 based on Provino in view of RFC 1034
Ground 3	**29-32, 53-56**	Obvious under § 103 based on Provino in view of Kosiur
Ground 4	**16, 27, 33, 40, 51 and 57**	Obvious under § 103 based on Provino in view of RFC 2660 draft 01

The '211 patent issued from a string of applications allegedly dating back to an original application filed on October 30, 1998. However, as outlined in section IV.C, the effective filing date for the embodiments recited by claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60 of the '211 patent is no earlier than February 15, 2000.

Provino qualifies as prior art under 35 U.S.C § 102(e). Specifically, Provino (Ex. 1008) is a patent that was filed on May 29, 1998 and issued April 29, 2003. Ex. 1008. Therefore, Provino is a patent that issued on an application that was filed before the '211 Patent's earliest effective date of February 15, 2000.

RFC 1034 qualifies as prior art under 35 U.S.C. § 102(b). Specifically, RFC 1034 (Ex. 1010) was published in November 1987 by the Internet Engineering Task Force (IETF). Ex. 1010.

Kosiur qualifies as prior art under 35 U.S.C § 102(b). Specifically, Kosiur (Ex. 1024) was published at the latest on September 1, 1998, and therefore qualifies as prior art under 35 U.S.C § 102(b). Ex. 1024.

RFC 2660 qualifies as prior art under 35 U.S.C § 102(b). Specifically, draft 01 of RFC 2660 (Ex. 1012) was published in August 1999 by the Internet Engineering Task Force (IETF). RFC 2660 was publically distributed no later than August 1999. Ex. 1012.

C. Claim Construction under 37 C.F.R. §§ 42.104(b)(3)

A claim subject to IPR is given its "broadest reasonable construction in light of the specification of the patent in which it appears."[2] 37 C.F.R. § 42.100(b). For purposes of this proceeding only, Microsoft submits constructions for the following terms. All remaining

[2] Because the standards of claim interpretation applied in litigation differ from PTO proceedings, any interpretation of claim terms in this IPR is not binding upon Microsoft in any litigation related to the subject patent. *See In re Zletz*, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989). Additionally, Microsoft does not acquiesce to Patent Owner's or the district court's (or anyone else's) constructions, and otherwise reserves all of its rights to argue, contest, and/or appeal the constructions.

terms should be given their plain meaning.

1. Domain Name (Claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60)

The Patent Owner has asserted to the PTAB that that a "domain name" means "a name corresponding to a network address." *See* Ex. 1019 at 31-32; Ex. 1020 at 28-29. In view of the Patent Owner's assertion, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider the term "domain name" as encompassing "a name corresponding to a network address."

2. Domain Name Service System (Claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60)

The Patent Owner has asserted to the PTAB and in litigation that no construction of "domain name service system" was necessary." Ex. 1013 at 24-25; Ex. 1019 at 37-39; Ex. 1020 at 34-36. According to the Patent Owner, the claims themselves define the characteristics of the domain name service system. *Id*. In view of the Patent Owner's assertions, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider the term "domain name service system" as encompassing any system with the characteristics described by the claims.

In general, under a broadest reasonable construction standard, a "system" can include one or more discrete computers or devices. Ex. 1023 at 15. This is consistent with the '211 patent's specification at col. 40, lines 35-48. This section describes a domain name service system that includes a modified DNS server 2602 and a gatekeeper server

2603, which is shown as being separate from the modified DNS server. Ex. 1001 at col. 40, lines 35-48 and fig. 26. Moreover, this sections states that "although element 2602 [(the modified DNS server)] is shown as combining the functions of two servers [(the DNS proxy 2610 and DNS server 2609)], the two servers can be made to operate independently." Ex. 1001 at col. 40, lines 46-48.

Also, the Examiner in the '789 and '856 reexamination proceedings concluded that the broadest reasonable construction of a system encompasses a single or multiple devices. Ex. 1016 at 17; Ex. 1017 at 23 (a "DNS **system** is reasonably interpreted as comprising a single device or multiple devices.").

Accordingly, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider the term "domain name service system" as encompassing any system with the characteristics specified by the claims, where the system may include one or more devices or computers.

3. Indicate/Indicating (Claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60)

The Patent Owner has asserted to the PTAB that no construction of "indicate" or "indicating" is necessary. Ex. 1019 at 44-46; Ex. 1020 at 41-43. Similarly, in litigation for the '211 patent, the Patent Owner asserted no construction of "indicate" or "indicating" was necessary, and the Court also declined to construe the term. Ex. 1013 at 31; Ex. 1015 at 28. In light of this, we consider the previous reexamination proceedings. In the '789 and '856 reexamination proceedings, the Examiner found that, under the broadest reasonable con-

struction, the term encompassed:

> ... the ability of the user to communicate using a secure link after boot-up." If the user attempts to establish a secure communication link using a DNS system after booting and is able to do so, then the user has been provided a broadly recited and **discernible** "indication" that the DNS in some manner supports establishing a communication link.

Ex. 1017 at 24 (emphasis original).

The Examiner also found that, under the broadest reasonable construction, the term encompassed:

> "a visible message or signal to a user that the DNS system supports establishing a secure communication link

Ex. 1016 at 20; Ex. 1017 at 25 (emphasis original).

The Examiner further concluded that, under the broadest reasonable construction, "[n]either the specification nor the claim language provides a basis for limiting 'indicating' to a visual indicator." Ex. 1017 at 26.

The broadest reasonable construction of "indicate" or "indicating" should thus encompass a visible or non-visible message or signal that the DNS system supports establishing a secure communication link, including the establishment of the secure communication link itself.

4. Secure Communication Link (Claims 1, 16-17, 20-23, 26-27, 31-32, 35-36, 47, 51, and 60)

The Patent Owner has asserted to the PTAB that "secure communication link" should mean a "direct communication link that provides data security through encryption." Ex. 1019 at 40-43; Ex. 1020 at 37-40. In view of the Patent Owner's assertions, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider the term "secure communication link" as encompassing a "direct communication link that provides data security through encryption."

5. Transparently (Claims 27 and 51)

The Patent Owner has asserted to the PTAB that "transparently" means that "the user need not be involved in creating the [secure communication link]/[secure link]." Ex. 1019 at 46-47; Ex. 1020 at 43-44. In view of the Patent Owner's assertions, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider the term "transparently" as encompassing "the user need not be involved in creating the [secure communication link]/[secure link]."

6. Between [A] and [B] (Claims 16, 27, 33, 40, 51, and 57)

In prior litigation on the '211 patent, the Patent Owner argued against the Defendant's construction that "between" should mean "extend from one endpoint to the other," and instead stated that "between" should only apply to the "public communication paths." Ex. 1014 at 11. Under the Patent Owner's contentions, a secure communication link is "between" two endpoints where encryption is used on the public communication paths between the two endpoints, regardless of whether the encryption extends completely from the first

endpoint to the second endpoint. *Id.* In view of the Patent Owner's assertions, it is reasonable, for purposes of this proceeding in which the broadest reasonable construction standard applies, to consider a secure communication link "between [A] and [B]" to encompass a secure communication link on the public communication paths between the two endpoints, regardless of whether that secure communication link fully extends from the first endpoint to the second endpoint.

IV. SUMMARY OF THE '211 PATENT

A. Brief Description

Generally, the '211 patent purportedly provides a domain name service for establishing a secure communication link. Ex. 1001 at Abstract, Col. 3, line 10. In particular, the '211 patent generally describes a domain name service system configured: (1) to be connected to a communication network, (2) to store a plurality of domain names and corresponding network addresses, (3) to receive a query for a network address, and (4) indicate in response to the query whether the domain name service system supports establishing a secure communication link. Ex. 1001 at Col. 55, lines 38-46.

The '211 patent includes 60 claims, of which claims 1, 36, and 60 are independent.

B. Summary of the Prosecution History of the '211 Patent

U.S. 7,921,211 issued on April 5, 2011 from U.S. Patent Application No. 11/840,560 ("the '560 application"), which was filed on August 17, 2007 with 3 claims as a continuation of U.S. Patent Application No. 10/714,849 ("the '849 application"), now U.S. Patent No.

7,418,504. *See* Ex. 1002 at 1005-1017, 1098.

In a first Office action dated March 19, 2010, the Examiner rejected claims 1-3 under 35 U.S.C. 112, second paragraph, as well as on the ground of non-statutory obviousness-type double patenting over the '504 patent, and also under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,864,666 (Shrader). *See* Ex. 1002 at 522-528. In response, the Applicants cancelled claim 1-3 and added new claims 4-63, stating that "[p]ending claims 4-63 are similar to claims 1-59 of the '504 Patent, except that they have been modified to add the limitation in independent claim 4 (and similar limitations to claims 39 and 63) that there is an indication in response to a query whether the domain name service system supports establishing a secure communication link." *See* Ex. 1002 at 192-205. Further, in response to the Examiner's rejection of claim 1 under 35 U.S.C. 112, second paragraph, the Applicants stated that "[t]he source of the query message can be from any source in communication with the system for providing a domain name service." Ex. 1002 at 202. In a second (Final) Office action dated October 21, 2010, the Examiner maintained the non-statutory obviousness-type double-patenting rejection of claims 4-63 over the '504 patent. *See* Ex. 1002 at 64-70.

In response, the Applicants filed a Terminal Disclaimer with respect to the '504 patent on December 22, 2010. *See* Ex. 1002 at 44-61.

The Examiner then issued a Notice of Allowance with the following statement of reasons for allowance:

> The prior arts of record do not teach or a domain name service system configured and arranged to be connected to a communication network, to store a plurality of domain names and corresponding network addresses, to receive a query for a network address, and to indicate in response to the query whether the domain name service system supports establishing a secure communication link.

Ex. 1002 at 23-27.

The Applicants paid the issue fee, and the '211 patent issued on April 5, 2011. Ex. 1002 at 15, 18.

C. The Effective Priority Date of the Claims of the '211 Patent

The '211 patent issued from U.S. Application No. 11/840,560, filed August 17, 2007. The '560 application is a continuation of application 10/714,849, filed November 18, 2003, which is a continuation of application 09/558,210, filed on April 26, 2000, which is a continuation-in-part of application 09/504,783, filed on February 15, 2000, which is a continuation-in-part of U.S. Application No. 09/429,643, filed on October 29, 1999. The '849, '210, '783 and '643 applications each attempt to claim priority to Provisional Application Nos. 60/137,704, filed June 7, 1999 and 60/106,261, filed October 30, 1998 .

Claims 1, 36 and 60 of the '211 patent are independent claims. Claims 2-35 depend directly or indirectly from claim 1, and claims 37-59 depend directly or indirectly from claim 36. Accordingly, claims 2-35 and 37-59 cannot enjoy an effective filing date earlier than that

of claims 1 and 36, respectively, from which they depend (*i.e.*, no earlier than February 15, 2000).

Claims 1, 36 and 60 of the ’211 patent rely on information not found in the disclosure of any application filed prior to the ’783 application on February 15, 2000. For example, claims 1 and 60 of the ’211 patent require “a **domain name service** for establishing a secure communication link.” Claims 1, 36, and 60 likewise recite “a **domain name service system**.” No application filed prior to the ’783 application mentions the phrase “domain name service,” much less provides a written description of systems or processes corresponding to the ’211 patent claims. The effective filing date of claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60 of the ’211 patent thus is not earlier than **February 15, 2000.**

V. MANNER OF APPLYING CITED PRIOR ART TO EVERY CLAIM FOR WHICH AN IPR IS REQUESTED, THUS ESTABLISHING A REASONABLE LIKELIHOOD THAT AT LEAST ONE CLAIM OF THE ‘211 PATENT IS UNPATENTABLE

This request shows how the primary references above, alone or in combination with other references, disclose the limitations of the Challenged Claims, thereby invalidating claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60 of the '211 patent. As detailed below, this request shows a reasonable likelihood that the Requester will prevail with respect to claims 1, 2, 6, 14-17, 19-23, 26-41, 43-47, and 50-60 of the ‘211 patent.

A. [GROUND 1] – Provino Anticipates Claims 1, 2, 6, 14-17, 19-23, 26-28, 33-41, 43-47, 50-52, and 57-60

Provino has an effective filing date of May 29, 1998, and is prior art under at least

§102(e).

During the '789 reexamination proceedings, the Examiner concluded that the '211 claims do not include any features that patentably distinguish the '211 patent claims from Provino. Ex. 1016 at 27. The Examiner noted that "[t]he biggest structural difference between the [the '211 patent] and Provino teachings discussed above is that, in [the '211 patent], the DNS proxy (server) 2610 forwards the message to gatekeeper 2603 while, in Provino, the DNS server 17 provides a network address that the initiator uses to contact firewall 30. However, whether the DNS request is forwarded or redirected is an unclaimed feature not necessary for an understanding of the claims." *Id*. This continues to be the case and, as described below, Provino anticipates claims 1, 2, 6, 14-17, 19-23, 26-28, 33-41, 43-47, 50-52, and 57-60 of the '211 patent.

Overview of Provino

Provino describes "systems and methods for easing communications between devices connected to public networks such as the Internet and devices connected to private networks." Ex. 1008 at 1:14-16; *see* Ex. 1023 at ¶ 16. In particular, Provino describes a system that facilitates communications between a client device 12(m) connected to ISP 11 and a server 31(s) located within virtual private network (VPN) 15. *See* Ex. 1008 at 9:32 to 10:33; Ex. 1023 at ¶ 16. An example of the architecture of Provino's system is illustrated in Figure 1 of Provino.

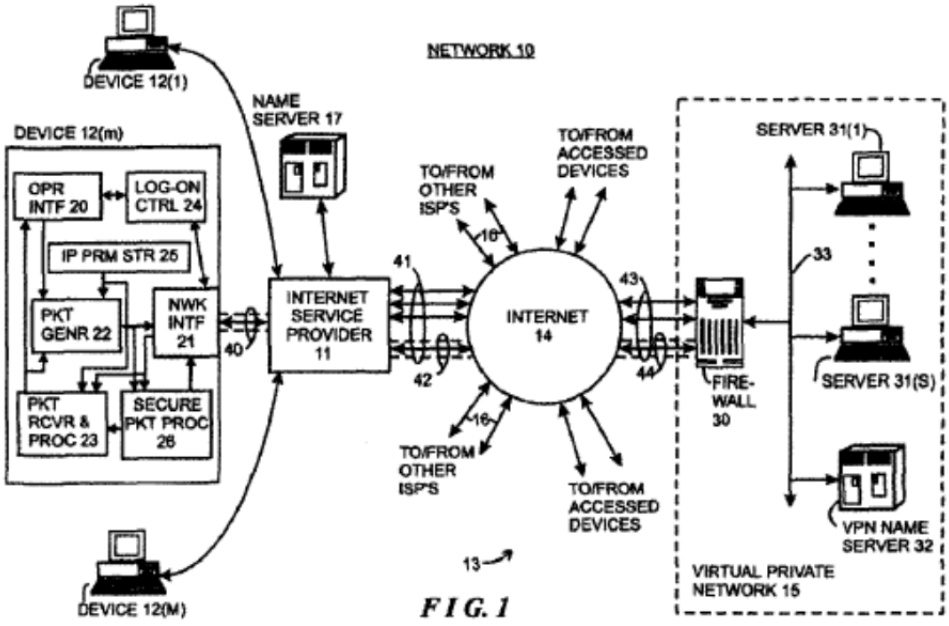

FIG. 1

For a device 12(m) external to VPN 15 to communicate with a server 31(s) within VPN 15, Provino describes a two phase process for establishing communications. *See* Ex. 1008 at 12:1-2; Ex. 1023 at ¶ 17. During the first phase described by Provino, the device 12(m) establishes a secure tunnel with VPN 15, via firewall 30, and identifies a VPN name server 32 inside VPN 15. Ex. 1008 at 9:61-65, 10:58-64; Ex. 1023 at ¶ 17. In particular, during the first phase, the client device 12(m) obtains an address for the firewall 30 from standard ISP name server 17 by initiating a request for the address and establishes a secure tunnel with firewall 30 by exchanging encryption/decryption information. Ex. 1008 at 12:20-24; Ex. 1023 at ¶ 17. During the second phase, the client device 12(m) uses the secure tunnel to send encrypted message packets to VPN 15, via firewall 30. Ex. 1008 at 12:8-16; Ex. 1023 at ¶ 17. In particular, during the second phase, the client device 12(m) communicates with VPN name server 32 to obtain addresses for servers (e.g., server 31(s))

inside the VPN 15, and then uses those addresses to send encrypted messages to those servers, via firewall 30. Ex. 1008 at 12:8-16; Ex. 1023 at ¶ 17.

Further details of the first phase are provided next. The client device 12(m) first locates the firewall 30 by obtaining "an integer Internet address for the firewall" which, in some cases, is "provided by a the [sic] nameserver 17 after a human-readable Internet address was provided by the operator or a program." Ex. 1008 at 12:20-24; Ex. 1023 at ¶ 19. After the client device 12(m) obtains the address of firewall 30 from nameserver 17, the device 12(m) sends a message packet to the firewall 30, requesting establishment of a secure tunnel. Ex. 1008 at 9:47-52; Ex. 1023 at ¶ 19. If the firewall 30 determines that the client device 12(m) is authorized to access the VPN 15, then the firewall 30 provides the device 12(m) with encryption and decryption information, such as identification of an encryption/decryption algorithm and associated encryption and decryption keys. Ex. 1008 at 9:61-65; Ex. 1023 at ¶ 19. The device 12(m) subsequently uses the encryption and decryption information to securely communicate with the VPN 15, thus establishing a secure tunnel through the Internet 14 to the VPN 15. *See* Ex. 1008 at 12:2-4; Ex. 1023 at ¶ 19. As shown in Annotation 1 below, the creation of the secure tunnel between device 12(m) and VPN 15 effectively extends the VPN to include the device 12(m) via Internet 14. Ex. 1008 at 6:10-15; Ex. 1023 at ¶ 19.

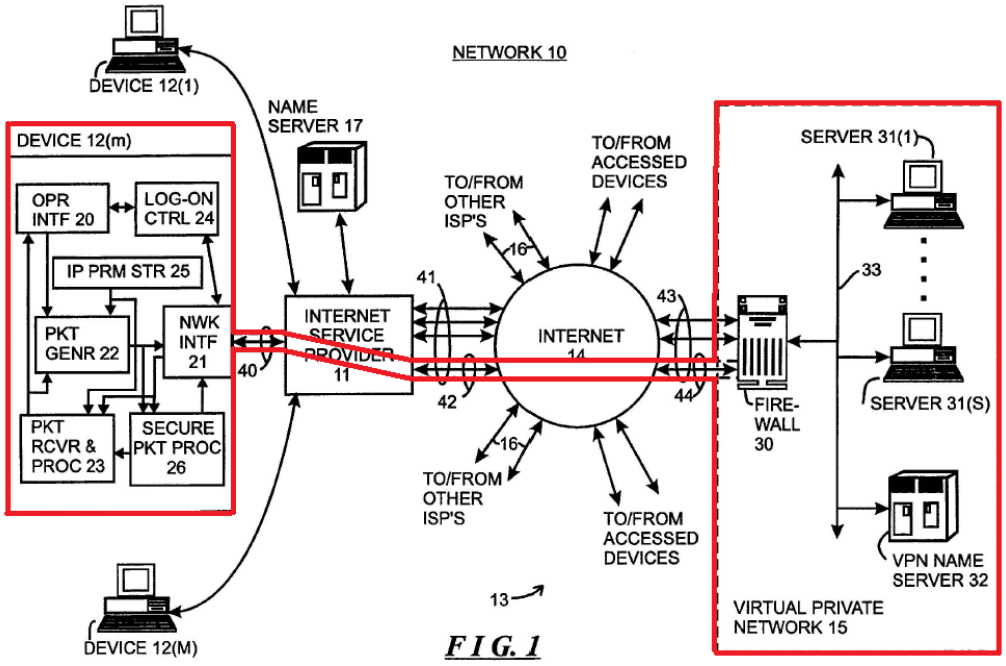

FIG. 1

(Annotation 1)

Provino further discloses that, during this first phase, in addition to encryption and decryption information, the firewall 30 may also provide the device 12(m) with an identification of a VPN nameserver 32 in the VPN 15. Ex. 1008 at 10:58-64; Ex. 1023 at ¶ 20. Functionally, the VPN nameserver 32 "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses." Ex. 1008 at 9:2-5; Ex. 1023 at ¶ 20. In particular, the client device 12(m) utilizes the VPN nameserver 32 (in the subsequent second phase) to locate servers inside the VPN by obtaining "the appropriate integer Internet addresses for the human-readable Internet addresses which may be provided by the operator of device 12(m)." Ex. 1008 at 10:64-67; Ex. 1023 at ¶ 20. Provino describes that message packets transferred over the Internet "conform to that defined by the so-called Internet protocol 'IP'" and that, in particular, the in-

teger Internet address of a message packet is an "IP parameter." Ex. 1008 at 3:62-65, 7:51-53; Ex. 1023 at ¶ 20. Provino also describes that the integer Internet address of the server 31(s) is "in the form of an 'n'-bit integer (where 'n' may be thirty two or 128)." Ex. 1008, 1:45-47; Ex. 1023 at ¶ 20.

Further details of the second phase are provided next. After creating a secure tunnel to VPN 15 and identifying VPN name server 32, "the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more servers 31(s) in the virtual private network 15, in the process obtaining resolution [of] human-readable Internet addresses to integer Internet addresses as necessary from the nameserver 32 that was identified by the firewall 30 during the first phase." Ex. 1008 at 12:8-16; *see* Ex. 1023 at ¶ 21.

In particular, in the second phase of Provino, a user of client device 12(m) may instigate communications with secure servers within VPN 15 (e.g., a server 31(s)) by using a human-readable Internet address that is associated with server 31(s). *See* Ex. 1008 at 13:31-40; Ex. 1023 at ¶ 22. Provino describes that, in general, the client device 12(m) will "initially access the nameserver 17… to attempt to obtain the integer Internet address associated with the human-readable Internet address." Ex. 1008 at 11:6-10; Ex. 1023 at ¶ 22. If the standard ISP nameserver 17 cannot resolve the hostname (e.g., because the requested server 31(s) is within a VPN), then the standard ISP nameserver 17 returns a message indicating that it does not have the integer address for the requested human-readable address

of server 31(s). Ex. 1008 at 11:10-15; Ex. 1023 at ¶ 22. In this case, the client device 12(m) sends a request message packet to the VPN nameserver 32, through the firewall 30, in attempting to identify the integer address of the server 31(s). Ex. 1008 at 11:10-15; Ex. 1023 at ¶ 22.

Below, in Annotations 2 and 3 of FIG. 1, the client's exchange with VPN nameserver 32 is highlighted. *See* Ex .1023 at ¶ 23. In particular, to resolve the human-readable Internet address using VPN nameserver 32, the device 12(m) initiates "a request message packet for transmission to the nameserver 32 through the firewall 30 and over the secure tunnel." Ex. 1008 at 11:13-16; Ex. 1023 at ¶ 23. This request process is illustrated in Annotation 2 of FIG. 1, which shows the device 12(m) sending a request message packet to the nameserver 32 (via firewall 30) to request the integer Internet address corresponding to the human-readable Internet addresses of a server 31(s). *See* Ex. 1023 at ¶ 23.

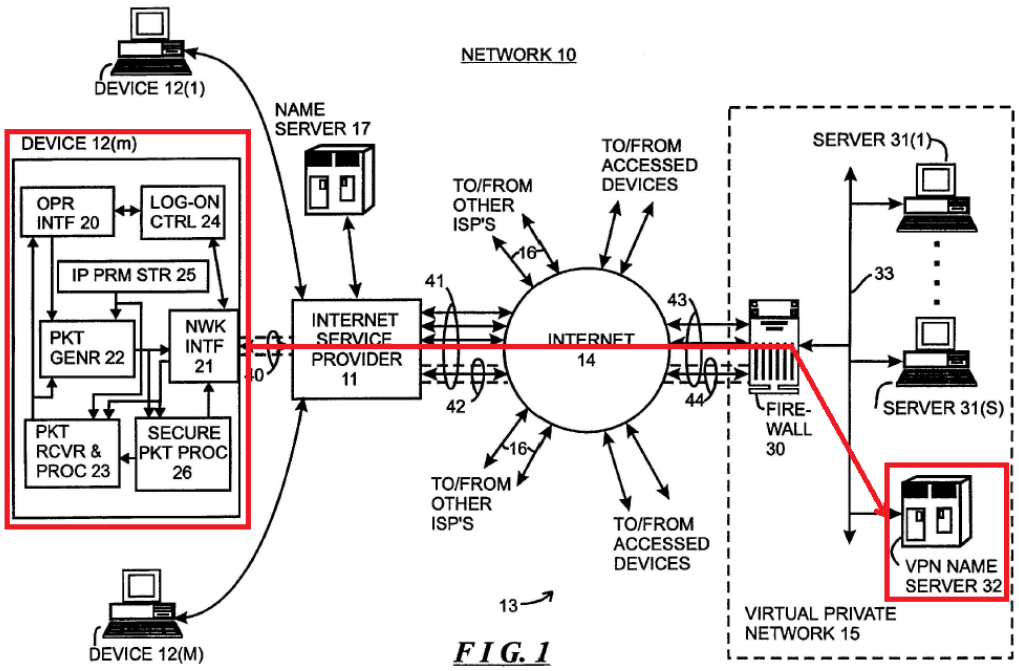

FIG. 1

(Annotation 2)

The VPN nameserver 32 receives the message request packet from the client device 12(m), via firewall 30, and attempts to resolve the human-readable Internet address of server 31(s) into an integer Internet address. Ex. 1008 at 11:19-21; Ex. 1023 at ¶ 24. If a corresponding integer address is found, then the VPN name server 32 returns the integer address back to the client device 12(m), via the firewall 30. Ex. 1008 at 11:21-25; Ex. 1023 at ¶ 24. Therefore, as a result of the client device 12(m) sending a request message packet to the VPN name server 32, Provino describes that the device 12(m) receives the integer Internet address for server 31(s) in a message packet transmitted from nameserver 32 via firewall 30, as illustrated in Annotation 3 of FIG. 1. *See* Ex. 1008 at 11:16-25; Ex. 1023 at ¶ 24.

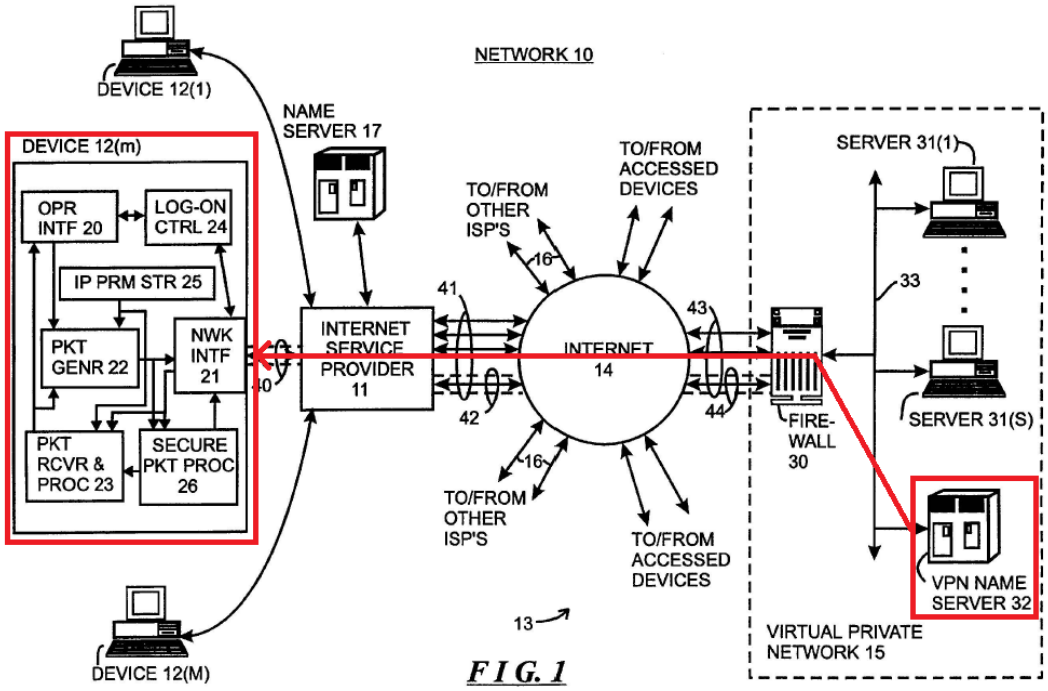

FIG. 1

(Annotation 3)

Otherwise, if the nameserver 32 does not have an association between the requested human-readable Internet address for server 31(s) and an integer Internet address, "the nameserver 32 can provide a response message packet so indicating." Ex. 1008 at 11:50-54; Ex. 1023 at ¶ 25. If the client device 12(m) is unable to obtain an integer Internet address associated with the human-readable Internet address from any of the nameservers to which it has access, then the client device 12(m) "may so notify its operator or program which requested the access." Ex. 1008 at 11:64-65; Ex. 1023 at ¶ 25.

Once the client device 12(m) receives the integer Internet address for server 31(s) from VPN name server 32, the client device 12(m) stores the address in a local cache, "along with the association of the human readable address thereto," in IP parameter store 25. Ex. 1008 at 11:35-39; Ex. 1023 at ¶ 28. The client device 12(m) subsequently uses the stored integer Internet address and associated human readable address to communicate with server 31(s) by sending messages via the encrypted tunnel to firewall 30, which forwards the messages to server 31(s). Ex. 1008 at 10:28-32, 11:40-45; Ex. 1023 at ¶ 28. In particular, Provino describes that "the device [12(m)] can use that integer Internet address in generating message packets for transmission to the server 31(s) which is associated with the human-readable Internet address." Ex. 1008 at 15:27-30; Ex. 1023 at ¶ 28. This transmission to the server 31(s) is illustrated in Annotation 4 of FIG. 1, below. Ex. 1023 at ¶ 28

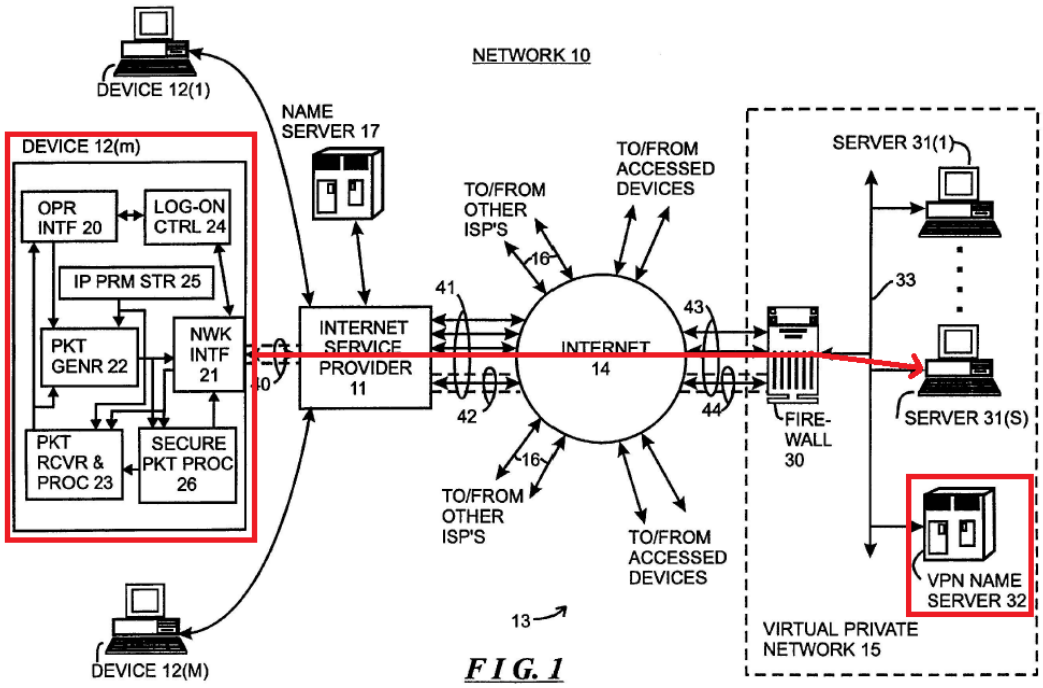

FIG. 1

(Annotation 4)

Provino additionally describes the transfer of information stored on server 31(s) to device 12(m). Ex. 1008 at 9:6-13; Ex. 1023 at ¶ 29. By describing that device 12(m) generates a message packet for transmission to server 31(s) and receives information transferred from server 31(s), Provino describes that device 12(m) leverages the resolved secure computer network address (i.e., integer Internet address) to send access request messages to server 31(s) that contains a request for information stored on server 31(s). *See* Ex. 1023 at ¶ 29. Thus, once the device 12(m) obtains the integer Internet address of server 31(s) from nameserver 32 during the second phase of establishing communications with server 31(s), the device 12(m) may send access requests to server 31(s) using the secure tunnel established with the firewall 30 in the first phase of the communication process. Ex. 1008 at 15:21-30; Ex. 1023 at ¶ 29.

In Annotation 5 of FIG. 1, which follows, firewall 30 is shown as limiting access to server 31(s) by computers outside of the VPN 15. *See* Ex. 1008 at 9:6-27; Ex. 1023 at ¶ 30. Provino describes that, both before and after creation of the secure tunnel, the firewall 30 authenticates message requests from client device 12(m) by determining whether the device 12(m) is authorized to access server 31(s) within the VPN 15. *See* Ex. 1008 at 9:56-60, 12:26-32; Ex. 1023 at ¶ 30.

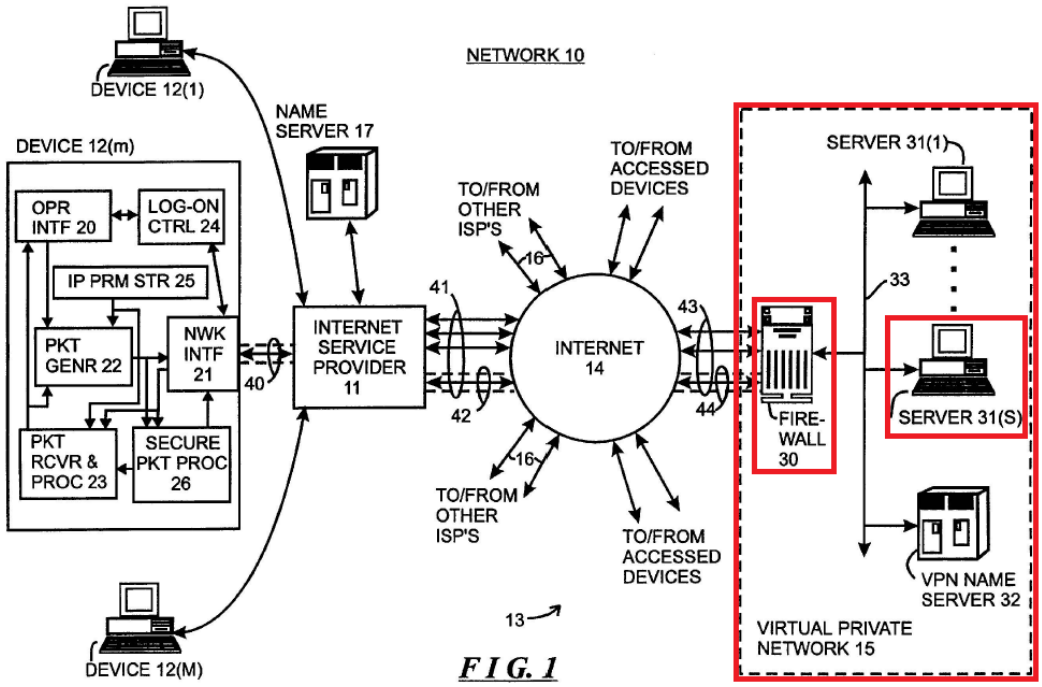

FIG. 1

(Annotation 5)

For example, in the first phase, if the firewall 30 accepts the secure tunnel establishment request from client device 12(m), then the firewall 30 "will generate a response message packet for transmission to the device 12(m) that identifies the encryption and decryption algorithms and keys" to be used in establishing the secure tunnel. Ex. 1008 at 12:26-32; Ex. 1023 at ¶ 31.

In addition, in the second phase, in order for the device 12(m) to access the server 31(s), the device 12(m) must be authorized to do so. Ex. 1008 at 9:20-27; Ex. 1023 at ¶ 32. In particular, if the requesting message indicates a device 12(m) that is authorized to access the server 31(s), then "firewall 30 will forward the message packet to the server 31(s)." Ex. 1008 at 9:20-23; Ex. 1023 at ¶ 32. Otherwise, if the client device 12(m) is not authorized to access server 31(s), then "the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response message packet to the source device indicating that the source was not authorized to access the server 31(s)." Ex. 1008 at 9:21-27; Ex. 1023 at ¶ 32.

Provino also describes that its system utilizes various services that use protocols and application programs. Ex. 1023 at ¶ 33. For example, "[e]ach device 12(m) communicates with the ISP 11 to transfer message packets thereto for transfer over the Internet 14, or to receive message packets therefrom received by the ISP 11 over the Internet 14, using any convenient protocol such as the well-known point-to-point protocol ("PPP") if the device 12(m) is connected to the ISP 11 using a point-to-point link, any conventional multi-drop network protocol if the device 12(m) is connected to the ISP 11 over a multi-drop network such as the Ethernet." Ex. 1008 at 4:23-35; Ex. 1023 at ¶ 33. Provino also describes that its system includes "network and/or telephony interface devices for interfacing the respective device to the ISP 11." Ex. 1008 at 4:43-45; Ex. 1023 at ¶ 33. Provino further discloses a system that is configured to process "programs, including application programs, under con-

trol of an operating system, to generate processed data" and that a "video display unit permits the device to display processed data and processing status to the user." Ex. 1008 at 4:44-49; Ex. 1023 at ¶ 33.

Provino explains that its system uses computing devices (*i.e.*, computers, servers, firewalls, etc.) that have software running on them, which necessarily include a machine-readable medium comprising instructions executable in a domain name service system. *See* Ex. 1008 at 4:35-49. For example, Provino's client device 12(m) includes processing, memory, and mass storage devices and includes programs under control of an operating system to generate processed data. *Id*. Also, Provino describes that its firewall 30 and servers 31(*s*) also include, for example, personal computers, computer workstations, and the like, and also include mini-and mainframe computers, mass storage systems, computer servers. *See* Ex. 1008 at 6:19-25.

1. Provino Anticipates Claims 1

Provino discloses a "*system for providing a domain name service for establishing a secure communication link,*" as recited in the preamble to claim 1. Ex. 1023 at ¶¶ 17, 18. For example, Provino's standard nameserver 17 and the VPN nameserver 32 (with the assistance of firewall 30 as appropriate) resolve human-readable Internet addresses for servers into respective integer Internet addresses. Ex. 1008 at 1:56-60, 7:37-43, 12:56-59; Ex. 1023 at ¶¶ 18, 20, 22-24, 26. Further, as described above, Provino discloses that the firewall 30 and nameservers 17 and 32 establish a secure communication link between the cli-

ent device 12(m) and the VPN 15/server 31(s) that provides data security through encryption. *See* Ex. 1008 at 12:1-25; *see also* Ex. 1023 at ¶¶ 17-19.

Provino's system includes a "*domain name service system configured and arranged to be connected to a communication network"* and *"store a plurality of domain names and corresponding network addresses,*" as recited in claim 1. Ex. 1023 at ¶¶ 16-19, 22. For example, Provino's firewall 30, standard nameserver 17, and VPN nameserver 32 operate as a "domain name service system," under the broadest reasonable interpretation of that term. Provino's firewall 30 and nameservers 17 and 32 are connected to a public network, such as the Internet. Ex. 1008 at 4:23-26, 8:58-65; Ex. 1023 at ¶¶ 16-19, 22. Accordingly, Provino's firewall 30, standard nameserver 17, and VPN nameserver 32 are configured and arranged to be (and are) connected to a communication network. *Id*.

Provino also explains that its nameservers 17 and 32 operate as DNS servers and resolve human-readable Internet addresses into corresponding integer Internet address. Ex. 1008 at 1:56-60, 7:37-43, 12:56-59; Ex. 1023 at ¶¶ 18, 20, 22-24, 26. To provide such name resolution functionality, the DNS servers would need to be configured to store the human-readable Internet addresses and corresponding integer Internet address. Ex. 1023 at ¶¶ 18, 20, 22-24, 26.

Provino's integer Internet address is an IP address and, hence, a network address. Ex. 1008 at 3:62-65, 7:51-53; Ex. 1023 at ¶ 18, 20-22. Provino describes that message packets transferred over the Internet "conform to that defined by the so-called Internet pro-

tocol 'IP'" and that the integer Internet address of a message packet is an "IP parameter." Ex. 1008 at 3:62-65, 7:51-53; Ex. 1023 at ¶ 18, 20-22. Provino also describes that the integer Internet address of the server 31(s) is "in the form of an 'n'-bit integer (where 'n' may be thirty two or 128)." Ex. 1008, 1:45-47; Ex. 1023 at ¶ 20. Thirty-two and 128 are the number of bits in Internet Protocol Version 4 and 6 IP addresses, respectively. Ex. 1023 at ¶ 20. Based on these disclosures, one of ordinary skill in the art would understand that the integer Internet address of the server 31(s) is an IP address (and hence a network address). *See* Ex. 1023 at ¶ 20.

Furthermore, the human-readable Internet address of server 31(s) is a "domain name," under that terms broadest reasonable interpretation, because the human-readable Internet address is a name corresponding to a network address. Ex. 1008 at 1:45-47, 3:62-65, 7:51-53, 10:58-67.

As a result, Provino's DNS servers 17 and 32 store a plurality of domain names and corresponding network addresses.

Provino's domain name service system is configured and arranged to "*receive a query for a network address*" as recited in claim 1. For example, as described above, Provino shows that each of the standard nameserver 17, the firewall 30, and the VPN name server 32 receives a request message packet from device 12(m) requesting the integer Internet address for server 31(s) within the VPN 15. *See* Ex. 1008 at 9:56-60, 11:13-25; Ex. 1023 at ¶ 17-18, 22-24, 28. Similarly, as described above, the standard name server 17 receives a

request for the address for the firewall 30. Ex. 1008 at 12:20-24; Ex. 1023 at ¶ 17, 18.

Provino's domain name service system is configured and arranged to "*indicate in response to the query whether the domain name service system supports establishing a secure communication link*" as required by claim 1. As described above, Provino includes various disclosures of indicating, according to the term's broadest reasonable construction, in response to queries whether its system supports establishing a secure tunnel. Ex. 1008 at 9:61-65, 10:58-64; Ex 1023 at 17, 18, 20-24. For example, during phase one, the standard name server 17, in response to a request from the client 12(m) for the address of a firewall, returns the address of the firewall 30 to the client 12(m). Ex. 1008 at 12:20-24; Ex. 1023 at 17, 18. Since the firewall 30 supports the secure tunnel, the firewall's address is a visible or non-visible message or signal that Provino's DNS system supports establishing a secure communication link. Ex. 1023 at ¶ 17, 18, 20-24. In addition, subsequently in phase two, after having received a request message packet from the client device 12(m) for the integer Internet address of the secure server 31(s), the firewall 30 either responds to the client device 12(m) with the requested address (obtained from the VPN nameserver 32) to allow the device 12(m) to securely communicate with the secure server 31(s), or else the firewall 30 responds to the device 12(m) with a response message packet that the system is unable to find an integer Internet address. 1008 at 14:57-64; Ex. 1023 at ¶ 20-24, 28. Therefore, the firewall 30, in response to the request message packet from the device 12(m), provides a visible or non-visible message or signal whether Provino's DNS system supports establish-

ing a secure communication link, under the terms broadest reasonable interpretation, between the device 12(m) and a secure server 31(s). *See* Ex. 1023 at ¶ 20-24. In addition, the VPN nameserver 32 also provides, in response to a request message packet received from the firewall 30 (forwarded on behalf of the client 12(m)), either the integer Internet address of a secure server 31(s) to allow the client device 12(m) to connect with the secure server 31(s) in the VPN 15 or else a response message packet that no such address was found. *See* Ex. 1008 at 11:50-55; Ex. 1023 at ¶ 22-24, 28. Therefore, the VPN nameserver 32, in response to a query for a network address from the firewall 30, also provides a visible or non-visible message or signal whether Provino's DNS system supports establishing a secure communication link, under the term's broadest reasonable interpretation, between the client device 12(m) and the VPN server 31(s) in the VPN 15. *See, e.g.*, Ex. 1008 at 12:8-16; *see also* Ex. 1023 at ¶ 20-24, 28.

Moreover, as described above, messages sent via the secure tunnel from client device 12(m) to VPN 15 are encrypted. Ex. 1008 at 9:65 to 10:4, 10:14-27; *See* Ex. 1023 at ¶ 17, 28. Accordingly, the connection between the client device 12(m) and the VPN 15/server 31(s) via the secure tunnel is a secure communication link, under that term's broadest reasonable interpretation, because the secure tunnel is a direct communication link between the client device 12(m) and the VPN 15/server 31(s).

2. Provino Anticipates Claims 36

Provino describes "*[a] machine-readable medium comprising instructions executable*

in a domain name service system, the instructions comprising code for" performing actions that are specified by those instructions. Provino explains that its system uses computing devices (*i.e.*, computers, servers, firewalls, etc.) that have software running on them, which necessarily include a machine-readable medium comprising executable instructions.

Provino's machine-readable medium comprises instructions comprising code for "connecting the domain name service system to a communication network." Ex. 1023 at ¶¶ 16-19, 22, 35. As described in § 1 above, Provino's firewall 30, standard nameserver 17, and VPN nameserver 32 are each connected to a communication network, such as the Internet. Ex. 1008 at 4:23-26, 8:58-65; Ex. 1023 at ¶¶ 16-19, 22.

In addition, Provino's machine-readable medium comprises instructions comprising code for "storing a plurality of domain names and corresponding network addresses." As described in § 1, Provino explains that its nameservers 17 and 32 operate as DNS servers and include software programs configured to perform operations of resolving human-readable Internet addresses (domain names, as described above) into corresponding integer Internet address (network addresses, as described above). Ex. 1008 at 1:56-60, 7:37-43, 12:56-59; Ex. 1023 at ¶¶ 20-24, 26. To provide such name resolution functionality, the DNS servers would need to store the human-readable Internet addresses and corresponding integer Internet address. Ex. 1023 at ¶ 26.

In addition, Provino's machine-readable medium comprises instructions comprising code for "receiving a query for a network address." Ex. 1023 at ¶ 35. As described in § 1

above, Provino shows that each of the standard nameserver 17, the firewall 30, and the VPN name server 32 receives a request message packet from device 12(m) requesting the integer Internet address for server 31(s) within the VPN 15. *See* Ex. 1008 at 9:56-60; Ex. 1023 at ¶¶ 17-18, 22-24, 28. Similarly, as described in § 1 above, the standard name server 17 receives a request for the address for the firewall 30. Ex. 1008 at 12:20-24; Ex. 1023 at ¶¶ 17, 18.

Provino's machine-readable medium comprises instructions comprising code for "indicating in response to the query whether the domain name service system supports establishing a secure communication link." Ex. 1023 at ¶¶ 17-20, 22-24, 28. As explained in § 1, above, Provino's system, upon receiving a query for a network address, provides various visible or non-visible messages or signals of whether it supports establishing a secure communication link (e.g., the standard nameserver 17 providing the integer Internet address of the firewall 30 in response to a request from the client device 12(m), as well as the firewall 30 either returning the integer Internet address of the VPN server 31(s) or else returning a response message packet indicating that the address was not found in response to a request from the client device 12(m), as well as the VPN nameserver 32 returning the same to the firewall 30 in response to a request from the firewall 30). *See, e.g.*, 1008 at 12:8-16; *see also* Ex 1023 at ¶ 17-20, 22-24, 28.

3. Provino Anticipates Claims 60

Provino discloses "*a method of providing a domain name service for establishing a*

secure communication link, the method comprising" the steps recited in claim 60. As explained in § 1, above, Provino describes various actions involved in providing a domain name service.

Provino describes "connecting a domain name service system to a communication network" as well as "storing a plurality of domain names and corresponding network addresses; and receiving a query for a network address for communication." Ex. 1023 at ¶¶ 16-19, 20, 26. As described in § 1above, Provino's firewall 30, standard nameserver 17, and VPN nameserver 32 are connected to a communication network, such as the Internet. Ex. 1008 at 4:23-26, 8:58-65; Ex. 1023 at ¶¶ 16-19, 22. Provino also explains that its nameservers 17 and 32 operate as DNS servers and resolve human-readable Internet addresses (domain names, as described above) into corresponding integer Internet address (network addresses, as described above). Ex. 1008 at 1:56-60, 7:37-43, 12:56-59; Ex. 1023 at ¶ 26. To provide such name resolution functionality, the DNS servers would need to store the human-readable Internet addresses and corresponding integer Internet address. Ex. 1023 at ¶ 26.

Furthermore, as described above, Provino shows that each of the standard nameserver 17, the firewall 30, and the VPN name server 32 receives a request message packet from device 12(m) requesting the integer Internet address for server 31(S) within the VPN 15. *See* Ex. 1008 at 9:56-60; Ex. 1023 at ¶¶ 17-18, 22-24, 28. Similarly, as described in § 1 above, the standard name server 17 receives a request for the address for the firewall 30.

Ex. 1008 at 12:20-24; Ex. 1023 at ¶¶ 17-18.

Provino discloses "upon receiving a query for a network address for communication, indicating whether the domain name service system supports establishing a secure communication link." Ex. 1023 at ¶¶ 17-18, 22-24, 28. As explained in § 1, above, Provino's system, upon receiving a query from either the device 12(m) or the firewall 30, provides various visible or non-visible messages or signals whether it supports establishing a secure communication link (e.g., the standard nameserver 17 returning the address of the firewall 30, as well as the firewall 30 and VPN nameserver 32 either returning the integer Internet address of the VPN server 31(s) to the device 12(m) or the firewall 30, respectively, or else returning a response message packet indicating that the address was not found). *See, e.g.*, Ex. 1008 at 12:8-16; *see also* Ex 1023 at ¶ 17, 18, 20-24, 28.

4. Provino Anticipates Claims 2 and 37

Provino discloses a system and a medium comprising instructions that anticipate claims 2 and 37. Ex. Claim 2 depends from claim 1 and specifies that "*at least one of the plurality of domain names comprises a top-level domain name*." Claim 37 depends from claim 36 and specifies that "*the instructions comprise code for storing the plurality of domain names and corresponding network addresses including at least one top-level domain name.*" Provino shows that its system contains nameservers (operating as DNS servers) and those nameservers can store multiple domain names. *See* Ex. 1008 at 1:56-60, 7:37-43, 12:56-59; *see also* Ex. 1023 at ¶¶ 24-26. Provino shows that some of the nameservers

are standard nameservers (e.g., nameserver 17). *See* Ex. 1008 at 7:34-46; Ex. 1023 at ¶¶ 17, 18. Prior to February of 2000, one of ordinary skill in the art would understand that domain names handled by standard domain name servers would contain a top-level domain. Ex. 1023 at ¶ 27. By showing a standard nameserver connected to the Internet, Provino discloses that the domain names include "a top-level domain name." Ex. 1023 at ¶¶ 17, 18, 27.

5. Provino Anticipates Claim 6

Provino discloses "*The system of claim 1, wherein the communication network includes the Internet*" as recited by claim 6. As described in § 1 above, Provino shows that each of the standard nameserver 17, the firewall 30, and the VPN name server 32 are connected to the Internet. *See, e.g.*, Ex. 1008 at 12:8-16; Ex. 1023 at ¶¶ 16-19, 22.

6. Provino Anticipates Claims 14 and 38

Provino discloses a system and a medium comprising instructions that anticipate claims 14 and 38. Claims 14 and 38 depend from claims 1 and 36, respectively, and specify "*responding to the query for the network address.*" Provino describes a system that is configured to respond to requests for network addresses. As described above, Provino shows that the standard nameserver 17 (which responds to the client device 12(m) with the address of the firewall 30), and the VPN nameserver 32 (which responds to the firewall 30 with the address of the VPN server 31(s)), and the firewall 30 (which responds to the client device 12(m) by relaying the address of the VPN server 31(s) received from the VPN name-

server 32), each responds to requests for integer Internet addresses. Ex. 1008 at 1:56-60, 7:37-43, 12:56-59; Ex. 1023 at ¶¶ 17-18, 22-24, 28.

7. Provino Anticipates Claims 15 and 39

Provino discloses a system and a medium comprising instructions that anticipate claims 15 and 39. Claims 15 and 39 depend from claims 1 and 36, respectively, and specify "*providing in response to the query, the network address corresponding to a domain name from the plurality of domain names and the corresponding network addresses.*" As described above, Provino describes that prior to phase one, the standard nameserver 17 provides, in response to a request message packet from device 12(m), the integer Internet address of the firewall 30 so that the device 12(m) can establish a secure tunnel with the firewall 30. Ex. 1008 at 12:17-26; Ex 1023 at ¶¶ 17, 18. In addition, in phase two, client device 12(m) receives, in response to its request message packet, an integer Internet address for server 31(s) in a message packet provided from nameserver 32 via firewall 30. *See* Ex. 1008 at 11:16-25; Ex. 1023 at ¶¶ 22-24, 28. Provino also describes standard nameserver 17 providing an integer Internet address of a non-VPN server, in response to a request message packet from device 12(m). Ex. 1008 at 7:37-46; Ex 1023 at ¶¶ 17, 18.

8. Provino Anticipates Claims 16 and 40

Provino discloses a system and a medium comprising instructions that anticipate claims 16 and 40. Claim 16 depends from claim 1 and specifies the system is configured to "*receive the query initiated from a first location, the query requesting the network address*

associated with a domain name, wherein the domain name service system is configured to provide the network address associated with a second location, and wherein the domain name service system is configured to support establishing a secure communication link between the first location and the second location." Claim 40 depends from claim 36 and specifies the machine readable medium comprising instructions for "*receiving the query for a network address associated with a domain name and initiated from a first location, and providing a network address associated with a second location, and establishing a secure communication link between the first location and the second location.*"

Provino discloses "*receiv[ing] the query initiated from a first location, the query requesting the network address associated with a domain name*" (claim 16) and "*receiving the query for a network address associated with a domain name and initiated from a first location*" (claim 40). For example, as described above, Provino includes various disclosures of a query requesting/for a network address, such as request message packets received by standard name server 17 from device 12(m) for the integer address of the firewall 30 (prior to phase one) and for the integer address of servers (in phase two), as well as request message packets received by the firewall 30 and VPN name server 32 from client device 12(m) for the integer Internet address of server 31(s). *See* Ex. 1008 at 12:1-26; *see also* Ex. 1023 at ¶¶ 17-18, 22-24, 28. Each of those request message packets is a query for a network address **initiated** by the client device 12(m) (a first location). Ex. 1023 at ¶¶ 17-18, 22-24, 28.

Provino also discloses that "*the domain name service system is configured to provide the network address associated with a second location*" (claim 16) and "*providing a network address associated with a second location*" (claim 40). Provino includes various disclosures of this feature. For example, Provino discloses that, prior to establishing a secure tunnel, the standard nameserver 17 provides the integer Internet address of firewall 30 to device 12(m) so that device 12(m) can contact firewall 30 to establish a secure tunnel with VPN 15/firewall 30. *See* Ex. 1008 at 12:17-26; *see also* Ex. 1023 at ¶¶ 17, 18.

In addition, Provino discloses that the VPN nameserver 32 "serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses." Ex. 1008 at 9:2-5; Ex. 1023 at ¶¶ 22-24, 28. After resolving the human-readable Internet address, the VPN nameserver 32 provides the integer Internet address to the firewall 30, which provides the address to the client 12(m). *See* Ex. 1008 at 11:16-25; Ex. 1023 at ¶¶ 22-24, 28.

The server 31(s), firewall 30, or the VPN 15 are each a second location that is associated with the provided network addresses (network address of firewall 30 and network address of server 31(s)). Ex. 1023 at ¶¶ 20-24.

Provino also discloses *wherein the domain name service system is configured to support establishing a secure communication link between the first location and the second location*" (claim 16) and "*establishing a secure communication link between the first location and the second location*" (claim 40). For example, when device 12(m) receives the integer

Internet address of firewall 30 from the nameserver 17, the firewall 30 supports establishing (and does establish) a secure tunnel between the client device 12(m) and the firewall 30/ VPN 15. *See* Ex. 1008 at 12:17-26; *see also* Ex. 1023 at ¶¶ 17-20. The nameserver 17 supports this establishment by providing the address of the firewall 30 to the client 12(m). *See* Ex. 1008 at 12:17-26; *see also* Ex. 1023 at ¶¶ 17, 18. As described above, the secure tunnel is a "secure communication link" under that term's broadest reasonable interpretation.

In addition, when the device 12(m) obtains the integer Internet address of server 31(s) from nameserver 32 during the second phase of establishing communications with server 31(s), the device 12(m) may send access requests to server 31(s) using the secure tunnel established with the firewall 30 in the first phase of the communication process. Ex. 1008 at 15:21-30; Ex. 1023 at ¶¶ 22-24, 28. The communication between the device 12(m) and server 31(s) involves the device 12(m) sending messages over the secure tunnel to firewall 30, which forwards the messages to server 31(s). Ex. 1008 at 10:28-32, 11:40-45; Ex. 1023 at ¶¶ 21-22. Therefore, in this case, Provino discloses that the firewall 30 is configured to support establishing (and does establish) a secure communication link between a first location (the client device 12(m)) and a second location (either the server 31(s) or the VPN 15). Ex. 1023 The nameserver 32 supports this establishment by providing the address of the server 32 to the client 12(m). Ex. 1008 at 15:21-30; Ex. 1023 at ¶¶ 22-24, 28.

9. Provino Anticipates Claims 17 and 41

Provino discloses a system and a medium comprising instructions that anticipate claims 17 and 41. Claim 17 depends from claim 1 and specifies the system performs the actions it was configured to perform in claim 1, with the exception that instead of requiring the domain name service system to "indicate in response to the query whether the domain name service system supports establishing a secure communication link" as recited in claim 1, claim 17 only requires that the domain name service system "comprises an indication that the domain name service system supports establishing a secure communication link." Ex. 1001 at col. 55. As explained in § 1, above, Provino describes systems that perform those actions, because Provino's firewall 30 and VPN nameserver 32 both provide, in response to queries from the client device 12(m) and firewall 30, respectively, visible or non-visible messages or signals whether it supports establishing a secure communication link. Ex. 1023 at ¶¶ 17, 18, 20-24.

In addition, Provino includes various disclosures of indications, according to the term's broadest reasonable construction, that its DNS system supports establishing the secure communication link. For example, during phase one, the standard name server 17, in response to a request for the address of the firewall, returns the firewall's address. Ex. 1008 at 12:20-24; Ex. 1023 at ¶ 17, 18. Since the firewall supports the secure tunnel, the firewall's address is a visible or non-visible message or signal that Provino's DNS system supports establishing a secure communication link. Also during phase one, the firewall 30 provides the client device 12(m) with encryption and decryption information that is used for

the secure tunnel. Ex. 1008 at 9:60-65, 10:56-67; Ex. 1023 at ¶ 20-24. Since the encryption and decryption information is used for the secure tunnel, this information is a visible or non-visible message or signal that Provino's DNS system supports establishing a secure communication link. In addition, subsequently in phase two, the VPN nameserver 32 provides the integer Internet address of a secure server 31(s) to allow the client device 12(m) to connect, over the secure tunnel, with the secure server 31(s) in the VPN 15. *See, e.g.*, Ex. 1008 at 12:8-16; *see also* Ex. 1023 at ¶ 22-24, 28. Since the address of the secure server is used to communicate over the secure tunnel, the address is a visible or non-visible message or signal that the DNS system supports establishing a secure communication link. Lastly, in phase one and two, a secure communication link is established between the client 12(m) and VPN 15 and server 31(s), respectively. Ex. 1023 at ¶ 17, 18, 22-24, 28.

Claim 41 depends from claim 36 and specifies that the instructions include code for "*indicating that the domain name service system supports the establishment of a secure communication link*," while claim 36 recites "*indicating in response to the query whether the domain name service system supports establishing a secure communication link*." As explained in § 2, above, Provino describes indicating that its domain name service system supports the establishment of a secure communication link. Ex. 1008 at 9:60-65, 10:56-67. For example, the nameserver 17 providing the client with address of the firewall 30, the firewall 30 providing the client 12(m) with the encryption/decryption information returned by the firewall 30, the nameserver 32 providing the client 12(m) with the address of the server

31(s), and establishing the connection between the client 12(m) and the VPN 15/server 31(s) are all indicating, according to the term's broadest reasonable construction, that Provino's DNS system supports the establishment of a secure communication link.

10. Provino Anticipates Claims 19 and 43

Provino discloses a system and a medium comprising instructions that anticipate claims 19 and 43. Claims 19 and 43 depend from claims 1 and 36, respectively, and specify the system of claim 1 wherein "*the domain name service system comprises a server*" or the machine readable medium of claim 36 wherein "*the code resides on a server*." Provino shows nameservers 17 and 32 and firewall 30, each of which comprise a server. *See, e.g.*, Ex. 1008 at 1:56-60, 6:19-25; *see also* Ex. 1023 at ¶¶ 17-18, 22-24, 26.

11. Provino Anticipates Claims 20 and 44

Provino discloses a system and a medium comprising instructions that anticipate claims 20 and 44. Claims 20 depends from claim 19 and specifies "wherein the domain name service system further comprises a domain name database, and wherein the domain name database stores the plurality of domain names and the corresponding network addresses." Claim 44 depends from claim 43 and specifies "wherein the instructions comprise code for storing a plurality of domain names and corresponding network addresses so as to define a domain name database." Provino describes a system that includes nameservers 17 and 32 (operating as DNS servers). *See* Ex. 1008 at 1:56-60, 7:37-43, 12:56-59; *see also* Ex. 1023 at ¶¶ 17-18, 22-24, 26. Prior to February of 2000, one of ordinary skill in the

art would understand that, by their nature, these name servers would contain a database to store a plurality of domain names and associated network addresses, in order to perform the function of domain name resolution. Ex. 1023 at ¶ 26. Provino accordingly discloses a domain name database that stores domain names and corresponding network addresses. Ex. 1023 at ¶¶ 17-18, 22-24, 26.

12. Provino Anticipates Claims 21 and 45

Provino discloses a system and a medium comprising instructions that anticipate claims 21 and 45. Claim 21 depends from claim 1 and specifies "wherein the domain name service system comprises a server, wherein the server comprises a domain name database, and wherein the domain name database stores the plurality of domain names and the corresponding network addresses." Claim 45 depends from claim 36 and specifies "wherein the code resides on a server, and the instructions comprise code for creating a domain name database configured to store the plurality of domain names and the corresponding network addresses." As described above in §§ 10 and 11, Provino discloses nameservers 17 and 32 that include a server, which one of skill in the art would understand as including a database to store a plurality of domain names and associated network addresses. Ex. 1023 at ¶¶ 17-18, 22-24, 26. Provino therefore anticipates claims 21 and 45.

13. Provino Anticipates Claims 22 and 46

Provino discloses a system and a medium comprising instructions that anticipate claims 22 and 46. Claims 22 and 46 depend from claims 1 and 36, respectively, and speci-

fy "*stor[ing] the corresponding network addresses for use in establishing secure communication links.*" Provino describes a system that includes nameservers (operating as DNS servers) that resolve domain names into IP addresses for use in establishing secure communication links. *See* Ex. 1008 at 1:56-60, 7:37-43, 12:56-59; *see also* Ex. 1023 at ¶¶ 17-18, 22-24, 26. For example, Provino shows that "the nameserver 32 serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses" and, as discussed above, the integer Internet addresses are used to establish a secure communication link between the client 12(m) and the server 31(s). Ex. 1008 at 9:2-5; Ex. 1023 at ¶¶ 22-24, 28. In addition, Provino discloses that standard nameserver 17 provides the integer Internet address of firewall 30 to client device 12(m), and the client device 12(m) uses that address to establish a secure tunnel (i.e., a secure communication link) with the firewall 30. *See* Ex. 1008 at 12:17-26; *see also* Ex. 1023 at ¶¶ 17, 18. In order to resolve human-readable Internet addresses for firewall 30 and servers (e.g., server 31(s)) to respective integer Internet addresses, the VPN nameserver 32 and pubic name server 17 would need to store domain names and corresponding network addresses. *See* Ex. 1023 at ¶¶ 17-18, 22-24, 26.

14. Provino Anticipates Claims 23 and 47

Provino discloses a system and a medium comprising instructions that anticipate claims 23 and 47. Claims 23 and 47 depend from claims 1 and 36, respectively, and specify "*authenticat[ing] the query for the network address.*" As described above, Provino de-

scribes that both before and after creation of a secure tunnel, the firewall 30 authenticates request message packets from device 12(m) by determining whether the device 12(m) is authorized to access a server 31(s) within the VPN 15. *See* Ex. 1008 at 9:56-60, 12:26-32; Ex. 1023 at ¶¶ 30-32. Thus, in order for the device 12(m) to access the server 31(s), the request message packet sent by device 12(m) must be authenticated by firewall 30. *See* Ex. 1023 at ¶¶ 30-32.

15. Provino Anticipates Claims 26 and 50

Provino discloses a system and a medium comprising instructions that anticipate claims 26 and 50. Claims 26 and 50 depend from claims 1 and 36, respectively, and specify "*wherein at least one of the plurality of domain names [is configured so as to enable/enables] establishment of a secure communication link.*" As described above, Provino describes that the device 12(m) may receive the integer Internet address of firewall 30 from standard nameserver 17, which enables the device 12(m) to establish a secure tunnel with firewall 30. *See* Ex. 1008 at 12:17-26; *see also* Ex. 1023 at ¶¶ 17, 18. In addition, Provino describes VPN nameserver 32 that can resolve human-readable Internet addresses (i.e., domain names) associated with servers (e.g., server 31(s)) internal to the VPN 15. *See* Ex. 1008 at 12:8-16; *see also* Ex. 1023 at ¶¶ 22-24, 28. When a request message packet is sent by device 12(m) to resolve such a domain name, and if the firewall 30 authorizes the device 12(m), then a secure tunnel between the external device 12(m) and the internal server 31(s) is established. *See* Ex. 1008 at 12:1-16; *see also* Ex. 1023 at ¶¶ 30-32. Thus,

these domain names are configure to enable (and enable) establishment of a secure communication link.

16. Provino Anticipates Claims 27, 33, 51, and 57

Provino discloses a system and a medium comprising instructions that anticipate claims 27, 33, 51, and 57. Dependent claims 33 (from claim 1) and 57 (from claim 36) each specify the domain name service system is configured to "*enable establishment of a secure communication link between a first location and a second location"* and claims 27 (from claim 1) and 51 (from claim 36) further specify this is done "*transparently to a user at the first location*."

To establish the secure tunnel between the client 12(m) (first location) and the firewall 30 (second location), the client device 12(m) first locates the firewall 30 by obtaining "an integer Internet address for the firewall" which, in some cases, is "provided by a the [sic] nameserver 17 after a human-readable Internet address was provided by the operator or a program." Ex. 1008 at 12:20-24; Ex. 1023 at ¶¶ 19, 34. After the client device 12(m) obtains the address of firewall 30 from nameserver 17, the device 12(m) sends a message packet to the firewall 30, requesting establishment of a secure tunnel, which is established if the client is authorized. Ex. 1008 at 12:2-4, 9:47-65; Ex. 1023 at ¶¶ 17-22. Provino does not describe the steps of contacting the firewall 30 and establishing a secure tunnel with the VPN 15 as requiring user involvement. *See* Ex. 1023 at ¶¶ 17-22, 34. In fact, Provino describes that no user involvement is needed as the integer Internet address of firewall 30

may have, in some cases, "been provided by a the nameserver 17 after a human-readable Internet address was provided by the operator ***or a program***." Ex. 1008 at 12:20-25; *see* Ex. 1023 at ¶¶ 19, 34.

Therefore, Provino describes a scenario in which a program, instead of a user, requests the address of the firewall 30, allowing the client device 12(m) (a first location) to establish a secure tunnel with the firewall 30 in the VPN 15 (either of which is a second location). *See* Ex. 1023 at ¶¶ 19, 34. As such, Provino discloses that a user is not required to be involved in establishing the secure tunnel. Ex 1023 at ¶¶ 19, 34. Therefore, the establishment of the secure communication link is transparent (under the broadest reasonable interpretation of that term) to a user at the client device 12(m).

17. Provino Anticipates Claims 28 and 52

Provino discloses a system and a medium comprising instructions that anticipate claims 28 and 52. Claims 28 and 52 depend from claims 1 and 36, respectively, and specify "*wherein the secure communication link uses encryption.*" The Provino system uses encryption for the secure tunnel. *See* Ex. 1008 at 9:65 to 10:33; *see also* Ex. 1023 at ¶¶ 17, 19, 20, 31, 34.

18. Provino Anticipates Claims 29 and 53

Provino discloses a system and a medium comprising instructions that anticipate claims 29 and 53. Claims 29 and 53 depend from claims 1 and 36, respectively, and specify that "*the secure communication link is capable of supporting a plurality of services.*" Ex.

As described above, Provino describes that its system utilizes various services, under the broadest reasonable interpretation of that term, that use protocols and application programs. Ex 1023 at ¶¶ 20, 33. For example, Provino discloses that "[e]ach device 12(m) communicates with the ISP 11 to transfer message packets thereto for transfer over the Internet 14, or to receive message packets therefrom received by the ISP 11 over the Internet 14, using any convenient **protocol** such as the well-known **point-to-point protocol** ("PPP") if the device 12(m) is connected to the ISP 11 using a point-to-point link, any conventional **multi-drop network protocol** if the device 12(m) is connected to the ISP 11 over a multi-drop network such as the Ethernet." Ex. 1008 at 4:23-35; Ex. 1023 at ¶ 33. Provino also describes that its system includes "network and/or telephony interface devices for interfacing the respective device to the ISP 11." Ex. 1008 at 4:43-45; Ex. 1023 at ¶ 33. Provino further discloses a system that is configured to process "**programs**, including **application programs**, under control of an operating system, to generate processed data" and that a "**video display unit** permits the device to display processed data and processing status to the user." Ex. 1008 at 4:44-49; Ex. 1023 at ¶ 33.

19. Provino Anticipates Claims 30 and 54

Provino discloses a system and a medium comprising instructions that anticipate claims 30 and 54. Claims 30 and 54 depend from claims 29 and 53, respectively, and specify that "*the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.*" Ex. 1001 at cols.

57, 58. As described above, Provino describes that its system utilizes various protocols and application programs. Ex 1023 at ¶¶ 20, 33. For example, Provino discloses **point-to-point protocol** ("PPP") and **multi-drop network protocol** that can be used by device 12(m). Ex. 1008 at 4:23-35; Ex. 1023 at ¶¶ 20, 33. Provino further discloses a system that is configured to process "**programs**, including **application programs**, under control of an operating system, to generate processed data." Ex. 1008 at 4:44-49; Ex. 1023 at ¶ 33.

20. Provino Anticipates Claims 31 and 55

Provino discloses a system and a medium comprising instructions that anticipate claims 31 and 55. Claims 31 and 55 limit claims 30 and 54, respectively, by specifying "*wherein the plurality of application programs comprises items selected from a group consisting of the following: video conferencing, e-mail, a word processing program, and telephony.*" Ex. 1001 at cols. 57, 58. As described above, Provino describes that its system includes "network and/or telephony interface devices for interfacing the respective device to the ISP 11." Ex. 1008 at 4:43-45; *see* Ex. 1023 at ¶ 33.

21. Provino Anticipates Claims 32 and 56

Provino discloses a system and a medium comprising instructions that anticipate claims 32 and 56. Claims 32 and 56 depend from claims 29 and 53, respectively, and specify "*wherein the plurality of services comprises audio, video, or a combination thereof.*" Ex. 1001 at cols. 57, 58. As described above, Provino further discloses a system that is configured to process "programs, including application programs, under control of an operating

system, to generate processed data" and that a "**video display unit** permits the device to display processed data and processing status to the user." Ex. 1008 at 4:44-49; *see* Ex. 1023 at ¶ 33.

22. Provino Anticipates Claims 34 and 58

Provino discloses a system and a medium comprising instructions that anticipate claims 34 and 58. Claims 34 and 58 depend from claims 33 and 57, respectively, and specify that the "*query [is] initiated from the first location, wherein the second location comprises a computer, and wherein the network address is an address associated with the computer.*" Ex. 1001 at cols. 57, 59. As discussed in §§ 1, 7, and 14, Provino includes various disclosures of these features. For example, Provino discloses that the client device 12(m) initiates a request message packet to the standard nameserver 17 to request the integer Internet address of the firewall 30 associated with VPN 15 before establishing a secure tunnel, or initiates a request message packet to firewall 30 to request the integer Internet address of server 31(s) in VPN 15. *See* Ex. 1008 at 12:1-26; *see also* Ex. 1023 at ¶¶ 17-18, 22-24, 28. The firewall 30, VPN 15, and server 31(s) are each a second location. Further, Provino discloses that the firewall 30, server 31(s), and VPN 15 each comprises a computer. *See* Ex. 1008 at 5:66 to 6:28; *see also* Ex. 1023 at ¶ 35.

23. Provino Anticipates Claims 35 and 59

Provino discloses a system and a medium comprising instructions that anticipate claims 35 and 59. Claims 35 and 59 depend from claims 1 and 36, respectively, and speci-

fy "*wherein the domain name service system comprises a domain name database connected to a communication network and storing a plurality of domain names and corresponding network addresses for communication, wherein the domain name database is configured so as to provide a network address corresponding to a domain name in response to a query in order to establish a secure communication link*." Ex. 1001 at cols. 57, 59. As explained in §§ 11 and 12, above, Provino's nameserver 17 includes a domain name database connected to a communication network and storing a plurality of domain names and corresponding network addresses for communication. *See* Ex. 1008 at 1:56-60, 7:37-43, 12:56-59; *see also* Ex. 1023 at ¶¶ 24-26. The nameserver 17 is configured to provide to the client 12(m) the address of the firewall 30 (which corresponds to a human-readable Internet address) in response to a query, which the client 12(m) uses to establish the secure tunnel with the firewall 30. *See* Ex. 1008 at 1:56-60, 7:37-43, 12:16-26; Ex. 1023 at ¶¶ 17, 18.

B. [GROUND 2] – Provino In View of RFC 1034 Renders Obvious Claims 20, 21, 35, 44, 45, and 59

As explained above, Provino discloses all of the limitations of claims 20, 21, 35, 44, 45, and 59. *See* §§ 11, 12, and 24, *above*. To the extent the Patent Owner contends Provino does not show a "domain name database," this distinction does not render claims 20, 21, 35, 44, 45, and 59 patentable.

RFC 1034 discloses that each name server in the Domain Name System includes a domain name database for the zones managed by the name server: "Name servers are the repositories of information that make up the domain database" and the domain

name database "is divided up into sections called zones, which are distributed among the name servers." Ex. 1010 at § 4.1; Ex. 1023 at ¶ 37. As a particular example, RFC 1034 describes a domain name database being shared by a name server and a resolver: "a resolver on the same machine as a name server might share a database consisting of the the [sic] zones managed by the nameserver and the cache managed by the resolver. Ex. 1010 at § 3.1; Ex. 1023 at ¶¶ 26, 38.

Provino discloses name servers (e.g., nameservers 17 and 32) which return a corresponding IP address in response to a query for a domain name. *See* Ex. 1008 at 1:56-60, 7:37-43, 12:56-59; Ex. 1023 at ¶¶ 17-18, 22-24, 28. Prior to February 2000, one of ordinary skill in the art would have been motivated to use the domain name database described by RFC 1034 in the name servers of Provino to store domain names and corresponding IP addresses, because databases organize data in a manner that allows for fast and efficient storing and searching of the data relative to other storage structures, such as a flat text file. *See* Ex. 1023 at ¶¶ 26, 38. Because the number of domain names and IP addresses can be relatively large, having a fast and efficient storage would allow for a timely response to a query to resolve a domain name. Ex. 1023 at ¶¶ 36-38. It therefore would have been obvious to one of ordinary skill in the art to use the domain database of RFC 1034 in the nameservers of Provino and such a combination would meet all of the elements of claims 20, 21, 35, 44, 45, and 59. Accordingly, claims 20, 21, 39, 44, 45, and 59 should be rejected as obvious.

C. [GROUND 3] – Provino In View of Kosiur Renders Obvious Claims 29-32 and 53-56

As explained above, Provino discloses all of the limitations of claims 29-32 and 53-56 and 56. See §§ V.A.18-21, above. To the extent the Patent Owner contends Provino does not show different services or data types being sent through a secure tunnel, this distinction does not render claims 29-32 and 53-56 patentable.

Provino in view of Kosiur would have rendered obvious claims 29, 30, 31, 32, 53, 54, 55, and 56 to a person of ordinary skill in the art in February of 2000. Dependent claims 29, 30, 31, and 32 (from claim 1) and claims 53, 54, 55, and 56 (from claim 36) each specify that the process or system be able to support a plurality of services. Specifically: (i) **claims 29 and 53** specify that "*the secure communication link is capable of supporting a plurality of services*"; (ii) **claims 30 and 54** specify that "*the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof*"; (iii) **claims 31 and 55** specify that "*the plurality of application programs comprises items selected from a group consisting of the following: video conferencing, e-mail, a word processing program, and telephony*"; and (iv) **claims 32 and 56** specify that "*the plurality of services comprises audio, video, or a combination thereof.*"

A person of ordinary skill in the art prior to February 2000 would have found it obvious to configure Provino to transmit data representing different types of services and or data types (including multimedia) through a secure tunnel in view of Kosiur.

Kosiur provides information regarding the capabilities of VPNs at or before the time of the '211 patent. *See* Ex. 1023 at ¶ 39. In particular, Kosiur is "a book [that] aims to provide you with the background on VPN technologies and products that you need to make appropriate business decisions about the design of a VPN and expectations for its use." Ex. 1024, p. 9; Ex. 1023 at ¶ 39. Chapter 15 of Kosiur "covers the basics of network performance and related application requirements as well as methods for offering network services to your customers that can be differentiated on the basis of those application and/or user requirements." Ex. 1024, p. 243; Ex. 1023 at ¶ 39.

In chapter 15, Kosiur describes that "a wide variety of applications can run on networks." Ex. 1024, p. 244; Ex. 1023 at ¶ 40. In particular, Kosiur describes that, if they're configured for differentiated services, virtual private networks can support "newer applications, such as interactive multimedia and videoconferencing." Ex. 1024, p. 254; Ex. 1023 at ¶ 40. Kosiur describes that VPN traffic may include "file transfers, Web browsing, and e-mail," in which case the VPN "won't need to be concerned with QoS." Ex. 1024, p. 249; Ex. 1023 at ¶ 40. Conversely, Kosiur describes that VPN traffic may also include "transactional traffic, interactive multimedia, and IP telephony," in which case "you'll need to track developments in QoS technologies." *Id.* Therefore, Kosiur describes that VPNs could be configured to support a plurality of application programs, including application programs that support interactive multimedia, file transfers, Web browsing, and e-mail. Ex. 1023 at ¶ 40

Provino arguably does not provide many specific details about the types of applications and services that are supported by VPN 15. Ex. 1023 at ¶ 41. However, Provino notes that the device 12(m) may be operated by an "employee of a particular company or governmental agency." Ex. 1008, 3:54-56. It would have been obvious to one of ordinary skill in the art to configure the VPN 15 described by Provino to support the applications and services described by Kosiur, as these applications and services would increase the mobility and productivity of the employees operating devices 12(m). Ex. 1023 at ¶ 41

In particular, Kosiur recognizes the increasing mobility of the modern workforce in which businesspersons require productivity applications, such as videoconferencing. *See* Ex. 1024, p. 13; Ex. 1023 at ¶ 42. As of 1998, Kosiur tells us that VPNs were commonly configured to support various services and applications, such as videoconferencing. *See* Ex. 1024, p. 254; Ex. 1023 at ¶ 42. Provino provides no contrary position, as it does not explicitly or implicitly describe any limitations on the services or applications that Provino's VPN 15 may be configured to support. Ex. 1023 at ¶ 42. Indeed, Provino describes that the devices in its system are capable of supporting numerous applications and services using various transfer methods. *See* Ex. 1008, 6:10-50; Ex. 1023 at ¶ 42. Moreover, Provino describes the maintenance of its VPN 15 "by a company, governmental agency, organization or the like." Ex. 1008, 9:6-7; Ex. 1023 at ¶ 42. Prior to 2000, it was common for companies or similar organizations to have their employees use interactive multimedia, vide-

oconferencing, file transfers, Web browsing, and e-mail as part of their daily routine to increase the employees' productivity and mobility. *See* Ex. 1024, p. 13; Ex. 1023 at ¶ 42. A company or other similar organization would find it desirable to make those resources available to remotely located employees through the VPN 15 so as to similarly increase the productivity of those remote employees. *See* Ex. 1023 at ¶ 42.

D. [GROUND 4] – Provino In View of RFC 2660 Renders Obvious Claims 16, 27, 33, 40, 51, and 57

Claims 16, 27, 33, 40, 51 and 57 are anticipated by Provino for the reasons set forth in §§ V.A.8 and V.A.16, above. To the extent Patent Owner contends that Provino does not expressly show establishing (or establishment of) a secure communication link between a first location and a second location – a position that would be inconsistent with its prior interpretations of the limitation – claims 16, 27, 33, 40, 51, and 57 are still invalid as obvious. In particular, were the Patent Owner to contend that a secure communication link "between" a first location and a second location must be a secure communication link that starts at the first location and ends at the second location, rather than just an intermediate portion there-between, a person of ordinary skill in the art in February of 2000 would have considered these claims obvious based on Provino in view of, *inter alia*, the information in draft 01 of RFC 2660 (Ex. 1012).

In particular, a person of ordinary skill would have considered it obvious to configure Provino's client device 12(m) and the VPN server 31(s) to implement end-to-end encryption using the Secure HTTP (S-HTTP) protocol. Ex. 1023 at ¶ 44. A motivation for

encrypting communications within each VPN would be to screen certain communications from others within the private network. *See* Ex. 1023 at ¶ 44. For example, certain user information (e.g., confidential employment information) may need to be encrypted even within a private network, securing the communications from third parties without authorization to view the user information, such as network administrators. *See* Ex. 1023 at ¶ 44.

RFC 2660 discloses the use of encryption between clients and servers: "Secure HTTP (S-HTTP) provides secure communication mechanisms between an HTTP client-server pair in order to enable spontaneous commercial transactions for a wide range of applications." Ex. 1012 at § 1; *see* Ex. 1023 at ¶ 45. In particular, RFC 2660 describes that "Secure HTTP provides a variety of **security** mechanisms to **HTTP clients** and **servers**" and that "[s]everal **cryptographic** message format standards may be **incorporated** into S-HTTP **clients** and **servers**." Ex. 1012 at § 1.1. "S-HTTP provides full flexibility of cryptographic algorithms, modes and parameters." Ex. 1012 at § 1.1.

The combination of Provino and RFC 2660 would result in encrypted communications between the client device 12(m) and VPN server 31(s) using S-HTTP messages instead of standard HTTP messages. *See* Ex. 1023 at ¶ 46. In this way, the use of S-HTTP could simply replace HTTP within the secure tunneling scheme describe by Provino. Ex. 1023. Thus, the exchange of the S-HTTP messages would ensure end-to-end encryption between the client device 12(m) and VPN server 31(s). *See* Ex. 1023 at

¶ 46. If, on the other hand, the client device 12(m) is requesting information from a non-secure server outside the VPN that does not implement S-HTTP, the client device 12(m) would communicate using standard HTTP. *See* Ex. 1012 at § 1.1 ("S-HTTP supports interoperation among a variety of implementations, and is compatible with HTTP. S-HTTP aware clients can communicate with S-HTTP oblivious servers and vice-versa, although such transactions obviously would not use S-HTTP security features."); *see also* Ex. 1023 at ¶ 46.

Therefore, it would have been an obvious design choice to one of ordinary skill in the art to incorporate the cryptography provided by Secure HTTP, as taught by RFC 2660, into Provino's client device12(m) and VPN server 31(s), in order to provide end-to-end encryption. *See* Ex. 1023 at ¶ 47. Therefore, Provino (which discloses a secure tunnel between the client device 12(m) and the firewall 30) in view of RFC 2660 (which discloses encrypted/secure end-to-end communications between a client and server) discloses a secure communication link that starts at the client device 12(m) (a first location) and ends at the VPN server 31(s) (a second location). *See* Ex. 1023 at ¶ 47.

VI. REDUNDACY

This petition is being filed concurrently with two other petitions regarding the same '211 patent. Between these three petitions, Petitioner has presented only a limited number of grounds, yet in doing so, has demonstrated how various teachings address the claims divergently. The limited grounds presented in these petitions do not impede "the just,

speedy, and inexpensive resolution of [this] proceeding," as required by 37 C.F.R. § 42.1(b). As Petitioner has already limited its petitions to just a few grounds, Petitioner respectfully requests that the Board institute rejections on all grounds presented in these three petitions to avoid prejudicing Petitioner.

VII. CONCLUSION

The cited prior art references identified in this Petition contain pertinent technological teachings (both cited and uncited), either explicitly or inherently disclosed, which were not previously considered in the manner presented herein, or relied upon on the record during original examination of the '211 patent. In sum, these references provide new, non-cumulative technological teachings which indicate a reasonable likelihood of success as to Petitioner's assertion that the Challenged Claims of the '211 patent are not patentable pursuant to the grounds presented in this Petition. Accordingly, Petitioner respectfully requests institution of an IPR for those claims of the '211 patent for each of the grounds presented herein.

Respectfully submitted,

Dated: 4/11/14

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265
Fish & Richardson P.C.
P.O. Box 1022
Minneapolis, MN 55440-1022
T: 202-626-6447
F: 202-783-2331

Dated: 4/11/14

/Kevin E. Greene/

Kevin E. Greene, Reg. No. 46,031
Fish & Richardson P.C.
P.O. Box 1022
Minneapolis, MN 55440-1022
T: 202-626-6376
F: 202-783-2331

(Trial No. _____)

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on April 11, 2014, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided via FedEx, to the Patent Owner by serving the correspondence address of record as follows:

Finnegan, Henderson, Farabow
Garrett & Dunner LLP
901 New York Avenue, NW
Washington, DC 20001

/Edward G. Faeth/
Edward G. Faeth
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(202) 626-6420