

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC
Petitioner

v.

HEADWATER RESEARCH LLC
Patent Owner

Case No. IPR2026-00439
Patent 11,096,055

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,096,055**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. MANDATORY NOTICES PURSUANT TO 37 C.F.R. §42.8(a)(1)	3
A. Real Party-In-Interest	3
B. Identification of Related Matters Under 37 C.F.R. §42.8(b)(2)	5
C. Lead and Backup Counsel.....	7
D. Service Information Under 37 C.F.R. §42.8(b)(4).....	8
III. FEES	8
IV. REQUIREMENTS UNDER 37 C.F.R. §42.104.....	8
A. Grounds for Standing	8
B. Identification of Challenges and Precise Relief Requested	9
C. Prior Art Qualification of Asserted References	10
V. BACKGROUND	11
A. The '055 Patent	11
B. Examination History	13
C. Prior Art.....	15
1. Charas (EX1004) - US Equivalent of Charas EP	15
2. Olvera-Hernandez (EX1005)	17
3. Mottes (EX1007).....	17
4. Spencer (EX1008).....	18
5. Phillips (EX1009)	18
6. Brown (EX1010).....	18

7.	3GPP (EX1018-EX1019).....	18
D.	Person of Ordinary Skill in the Art (“POSITA”).....	19
VI.	CLAIM CONSTRUCTION	19
VII.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	20
A.	Claims 1-4, 8-10, and 12 are Anticipated and/or Obvious over Charas (EX1004) alone and/or in view of Olvera-Hernandez (EX1005) (Ground 1)	20
1.	Claim 1 (Preamble): “A wireless end-user device comprising:”	20
a.	[1.1]: “a Wireless Wide-Area Network (WWAN) modem;”	21
b.	[1.2]: “a secure memory to store a first service profile associated with a first service plan and a first wireless network accessible through the WWAN modem, the first service profile comprising a first set of network service policies, and”	26
c.	[1.3]: “a second service profile associated with a second service plan and a second wireless network accessible through the WWAN modem, the second service profile comprising a second set of network service policies;”	31
d.	[1.4]: “a connection manager to select an access network connection for the WWAN modem, based on a selected one of the first and second service profiles;”	35
e.	[1.5]: “at least one adaptive service policy control agent to enforce network service policies associated with the selected one of the first and second service profiles,”	37
f.	[1.6]: “the enforced network service policies including policies enforced at an application	

	service interface on network data connections for selected applications resident on the device.”	40
2.	Claim 2: “The wireless end-user device of claim 1, the first service profile further comprising first device credentials and the second service profile further comprising second device credentials, the wireless end-user device further comprising a device master agent credential that is independent of the first and second device credentials.”	43
3.	Claim 3: “The wireless end-user device of claim 1, further comprising a service monitor agent to record network service usage categorized by sub-account for different wireless networks, including separate service usage counts associated with each of the first service plan and the second service plan.”	46
4.	Claim 4: “The wireless end-user device of claim 3, wherein for at least one of the first and second service plans, the wireless end-user device synchronizes a local service usage count with a network-based service count.”	47
5.	Claim 8: “The wireless end-user device of claim 1, wherein the at least one adaptive service policy control agent applies network service policies from a superset profile that provides capabilities from each of the first and second service profiles.”	49
6.	Claim 9: “The wireless end-user device of claim 1, wherein the at least one adaptive service policy control agent detects network connection changes from the first wireless network to the second wireless network, and in response enforces the second set of network service policies.”	51
7.	Claim 10: “The wireless end-user device of claim 1, wherein the connection manager further comprises a modem selection and control layer that routes certain types of data traffic to the first wireless network and	

	other types of data traffic to the second wireless network.”	54
8.	Claim 12: “The wireless end-user device of claim 1, the connection manager configured to prompt the WWAN modem to connect to a selected access network and send credentials associated with the selected one of the first and second service profiles to the selected access network.”	56
B.	Claim 5 is Obvious over Charas alone or in Combination with Olvera-Hernandez in view of Mottes (Ground 2)	58
1.	Claim 5: “The wireless end-user device of claim 1, wherein the first service plan is associated with a central provider that operates a WWAN access network, and the second service plan is associated with a virtual network operator.”	58
C.	Claims 6 and 7 are Obvious over Charas alone or in Combination with Olvera-Hernandez in view of Spencer (Ground 3)	61
1.	Claim 6: “The wireless end-user device of claim 1, further comprising a user service interface to allow a user to make a user selection between the first and second service profiles, the connection manager to, responsive to the user selection, select an access network connection for the WWAN modem.”	61
2.	Claim 7: “The wireless end-user device of claim 1, further comprising a service notification and billing interface to display service usage options for each of the first and second service profiles.”	65
D.	Claim 11 is Obvious over Charas alone or in Combination with Olvera-Hernandez in view of Phillips (Ground 4)	68
1.	Claim 11: “The wireless end-user device of claim 1, further comprising a Subscriber Identity Module (SIM), the adaptive service policy control agent located at least in part on the SIM.”	68

E.	Claim 13 is Obvious over Charas alone or in Combination with Olvera-Hernandez in view of Brown (Ground 5)	72
1.	Claim 13: “The wireless end-user device of claim 2, configured to, when the second service plan is inactive, suspend the second device credentials, and when the second service plan is reactivated, reactivate the second device credentials”	72
VIII.	OTHER CONSIDERATIONS	75
IX.	CONCLUSION.....	75

APPENDIX A - LIST OF EXHIBITS

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. §42.24

CERTIFICATE OF SERVICE

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (<i>en banc</i>)	19
Statutes	
35 U.S.C. §102	9
35 U.S.C. §102(b)	10, 11
35 U.S.C. §102(e)	10
35 U.S.C. §103	9
35 U.S.C. §122(b)	10
35 U.S.C. §§311-319	1
Rules	
37 C.F.R. §42.8(a)(1)	3
37 C.F.R. §42.8(b)(2)	5
37 C.F.R. §42.8(b)(3)	7
37 C.F.R. §42.8(b)(4)	8
37 C.F.R. §42.10(a)	7
37 C.F.R. §42.10(b)	8
37 C.F.R. §42.100(b)	19
37 C.F.R. §42.100 <i>et seq.</i>	1
37 C.F.R. §42.104	8

Petition for *Inter Partes* Review of U.S. Patent No. 11,096,055

37 C.F.R. §42.104(a).....	8
---------------------------	---

I. INTRODUCTION

Google LLC respectfully requests *inter partes* review of Claims 1-13 (“Challenged Claims”) of U.S. Patent No. 11,096,055 (“’055 Patent”) (EX1001) under 35 U.S.C. §§311-319 and 37 C.F.R. §42.100 *et seq.*

The ’055 Patent claims a wireless end-user device (e.g., “user terminal”) that comprises a secure memory to store two service profiles (e.g., “policy blocks”) associated with two service plans (e.g., two service provider subscriptions) and two wireless networks, wherein the policies are enforced at an application service interface on the end-user device. The end-user device subscriptions are enforced on the end-user device rather than on the networks with which the device interacts. The end-user device includes a connection manager that selects an “access network connection” based on a selected service profile. An agent on the device (“adaptive service policy control agent”) enforces network service policies associated with the selected service profile.

The ’055 Patent should never have issued because the prior art cited herein (Charas, EX1004) discloses enforcing policies associated with first and second subscriptions/wireless networks on an end-user device. The European Patent Office recognized this in its rejection of European counterpart claims that were identical to the ’055 Patent claims (*see* prosecution of counterpart European Application No. 19219822.4 (EX1014) citing a European equivalent of Charas (EX1027)). Patent

Owner amended its European claims to distinguish the Charas equivalent but never informed the USPTO of Charas or its equivalent even though the EPO prosecution preceded allowance of the '055 Patent. Worse yet, the '055 Patent was granted based on a first Office Action allowance.

Charas anticipates and/or renders obvious the claims of the '055 Patent because it discloses enforcing service policies at an application service interface of an end-user device. Charas discloses “application programming interfaces (APIs) for the services” offered by service providers as part of fee-based subscriptions. EX1004, ¶¶[0051], [0056]. These APIs include an “applications interface” having Quality of Service (QoS) “parameters” (i.e., policies). *Id.*, ¶[0064]. Charas therefore discloses exactly the purported novelty on which the '055 Patent was granted.

Patent Owner deprived the USPTO of a full and fair examination in failing to disclose Charas (or its equivalent). The '055 Patent claims are unpatentable at least for reasons similar to those raised in the European counterpart.

All claims of the '055 Patent are unpatentable. *See* EX1004, EX1005, and EX1007-EX1010 each in their entirety.

II. MANDATORY NOTICES PURSUANT TO 37 C.F.R. §42.8(a)(1)

A. Real Party-In-Interest

Google LLC¹ is a real party-in-interest.

Out of an abundance of caution, Google identifies Apple Inc. (“Apple”) as a real party-in-interest. Apple and Headwater entered into “a worldwide settlement whereby Headwater licensed its patents to Apple.” Patent Owner’s Request for Discretionary Denial of Institution, *Google LLC v. Headwater Research LLC*, IPR2026-00048, Paper 8, 2 (PTAB Jan. 7, 2026).

As identified in the related matters below, the ’055 Patent is being asserted against multiple Carriers in E.D. Tex. Case Nos. 2:25-cv-00901, 2:25-cv-00902, 2:25-cv-00903, with Case No. 2:25-cv-00902 serving as the lead consolidated case for all pretrial issues. On December 1, 2025, the Carriers in those cases filed a joint opposed motion to stay the litigations under, among other things, the customer-suit exception. *See* Defendants’ Joint Opposed Motion to Stay, *Headwater Res. LLC v. Dish Network Corp. et al.*, Civ. Action No. 2:25-cv-00902 (Dec. 1, 2025), ECF No. 55. On December 8, 2025, a redacted version of that motion was made publicly available. *See id.* ECF No. 64. On December 19, 2025, Headwater filed a sealed

¹ Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc.

response to the motion. *See id.* ECF No. 75. On January 9, 2026, the Carriers filed a sealed reply. *See id.* ECF No. 84. Given these filings, Google names the following Carriers (the named defendants in these cases) as real parties-in-interest to this proceeding:

- DISH Network Corporation f/k/a EchoStar Communications Corporation
- DISH Network LLC
- Dish Wireless, LLC d/b/a Boost Mobile
- Charter Communications, Inc.
- Charter Communications, LLC
- Charter Communications Operating, LLC
- Comcast Cable Communications, LLC d/b/a Xfinity
- Comcast Cable Communications Management, LLC
- Comcast Corporation
- Comcast of Houston, LLC d/b/a Xfinity
- Spectrum Gulf Coast, LLC
- Spectrum Management Holding Company, LLC

Charter Communications, Inc., Charter Communications, LLC, Charter Communications Operating, LLC, Spectrum Gulf Coast, LLC, Spectrum Management Holding Company, LLC and Headwater Research LLC filed a Joint Motion to Stay All Deadlines and Notice of Settlement on August 5, 2026.

Headwater Res. LLC v. Dish Network Corp. et al., Civ. Action No. 2:25-cv-00902 (E.D. Tex.), ECF No. 114 (Aug. 5, 2026).

Comcast Cable Communications, LLC d/b/a Xfinity, Comcast Cable Communications Management, LLC, Comcast of Houston, LLC, and Headwater Research LLC filed a Joint Motion to Stay All Deadlines and Notice of Settlement on August 7, 2026. *See Headwater Res. LLC v. Dish Network Corp. et al.*, Civ. Action No. 2:25-cv-00902 (E.D. Tex.), ECF No. 117 (Aug. 7, 2025).

To be clear, none of these Carriers funded, directed, or controlled the filing or preparation of this petition, nor did Google prepare or file the petition at the Carriers' behest. Instead, Google makes this identification out of an abundance of caution and in the interest of over-disclosure.

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

The following is a list of any judicial or administrative matters that would affect, or be affected by, a decision in this proceeding:

Related District Court Matters

Headwater Research LLC v. Google LLC, Civ. Action No. 5:26-cv-07551 (N.D. Cal.) ("7551 Litigation") transferred from Civ. Action No. 7:25-cv-00369 (W.D. Tex.) ("369 Litigation") – Complaint filed Aug. 27, 2025 and ordered related to Civ. Action 5:26-cv-01460 (N.D. Cal.) Aug. 7, 2026;

Petition for *Inter Partes* Review of U.S. Patent No. 11,096,055

Headwater Research LLC v. Apple Inc., Civ. Action No. 7:25-cv-00370 (W.D. Tex.) – Complaint filed Aug. 27, 2025, Dismissed Oct. 31, 2025 (“’370 Litigation”);

Headwater Research LLC v. Charter Communications, Inc. et al., Civ. Action No. 2:25-cv-00901 (E.D. Tex.) – Complaint filed Aug. 27, 2025, Notice of Settlement and Motion to Stay Aug. 5, 2026, Stay granted Aug. 6 – Consolidated with 25-cv-00902 (E.D. Tex.) for all pre-trial issues;

Headwater Research LLC v. Dish Network Corp. et al., Civ. Action No. 2:25-cv-00902 (E.D. Tex.) – Complaint filed Aug. 27, 2025, Stayed July 6, 2026 due to Defendants’ bankruptcy filings;

Headwater Research LLC v. Comcast Cable Communications, LLC d/b/a Xfinity et al., Civ. Action No. 2:25-cv-00903 (E.D. Tex.) – Complaint filed Aug. 27, 2025, Notice of Settlement and Motion to Stay Aug. 7, 2026, Stay granted Aug. 11, 2026 – Consolidated with 25-cv-00902 (E.D. Tex.) for all pre-trial issues; and

Headwater Research LLC v. Samsung Electronics Co., Ltd. et al., Civ. Action No. 2:24-cv-00228 (E.D. Tex.) – Dismissed Sep. 29, 2025.

Related PTAB Matters

Samsung Electronics Co., Ltd. v. Headwater Research LLC, IPR2025-00481 – Petition filed Feb. 26, 2025 – Institution Denied August 4, 2025.

Related Applications

The '055 Patent issued from U.S. Patent App. No. 16/421,121, filed on May 23, 2019, which is a continuation of U.S. Patent App. No. 15/427,837, filed Feb. 8, 2017 (US Pat 10,321,318), which is a continuation of U.S. Patent App. No. 15/239,398, filed Aug. 17, 2016 (US Pat 9,641,957), which is a continuation of U.S. Patent App. No. 14/979,233, filed Dec. 22, 2015 (US Pat 9,532,161), which is a continuation of U.S. Patent App. No. 14/667,353, filed Mar. 24, 2015 (US Pat 9,232,403), which is a continuation of U.S. Patent App. No. 14/263,604, filed Apr. 28, 2014 (US Pat 9,037,127), which is a continuation of U.S. Patent App. No. 12/380,780, filed Mar. 2, 2009 (US Pat 8,839,388), which claims priority to U.S. Provisional App. No. 61/207,739, filed Feb. 13, 2009, U.S. Provisional App. No. 61/207,393, filed Feb. 10, 2009, U.S. Provisional App. No. 61/206,944, filed Feb. 4, 2009, and U.S. Provisional App. No. 61/206,354, filed Jan. 28, 2009.

U.S. Patent App. No. 17/401,635, filed Aug. 13, 2021 (US Pat 11,757,943) is a continuation of U.S. Patent App. No. 16/421,121.

C. Lead and Backup Counsel

Pursuant to 37 C.F.R. §42.8(b)(3) and §42.10(a), Petitioner hereby identifies lead and backup counsel as follows:

<u>Lead Counsel</u> Patrick C. Keane (Reg. No. 32,858) BUCHANAN INGERSOLL & ROONEY PC 1700 K Street, N.W., Suite 300 Washington, DC 20006 Telephone (703) 838-6522 Facsimile (202) 452-7989 patrick.keane@bipc.com	<u>Backup Counsel</u> Roger H. Lee (Reg. No. 46,317) BUCHANAN INGERSOLL & ROONEY PC 1700 K Street, N.W., Suite 300 Washington, DC 20006 Telephone (703) 838-6545 Facsimile (202) 452-7989 roger.lee@bipc.com
<u>Backup Counsel</u> Andrew J. Koopman (Reg. No. 65,537) BUCHANAN INGERSOLL & ROONEY PC 2200 Renaissance Blvd., Suite 350 King of Prussia, PA 19406 Telephone (610) 993-4217 Facsimile (610) 407-0701 andrew.koopman@bipc.com	<u>Backup Counsel</u> Samuel Harrod (Reg. No. 79,148) BUCHANAN INGERSOLL & ROONEY PC Union Trust Building 501 Grant Street Suite 200 Pittsburgh, PA 15219 Telephone (412) 562-8805 Facsimile (412) 562-1041 samuel.harrod@bipc.com

A Power of Attorney is being filed concurrently herewith in accordance with 37 C.F.R. §42.10(b).

D. Service Information Under 37 C.F.R. §42.8(b)(4)

Petitioner consents to electronic service at the email addresses listed above.

III. FEES

The Office is authorized to charge required fees to Deposit Account 02-4800.

IV. REQUIREMENTS UNDER 37 C.F.R. §42.104

A. Grounds for Standing

Petitioner certifies that the '055 Patent is available for IPR and Petitioner is not barred or estopped from requesting an IPR of the Challenged Claims on the grounds identified herein. 37 C.F.R. §42.104(a).

B. Identification of Challenges and Precise Relief Requested

Petitioner challenges Claims 1-13 of the '055 Patent and requests that these claims be found unpatentable for the reasons set forth in Petitioner's Grounds as follows:

Ground	Reference(s)	Basis	Claims
1	U.S. Pub. 2002/0056002 ("Charas") (EX1004) alone and/or in view of U.S. Pub. 2009/0170555 ("Olvera-Hernandez") (EX1005)	§102/103	1-4, 8-10, 12
2	Charas alone and/or in view of Olvera-Hernandez in view of U.S. Pub. 2004/0162058 ("Mottes") (EX1007)	§103	5
3	Charas alone and/or in view of Olvera-Hernandez in view of U.S. Pub. 2010/0107225 ("Spencer") (EX1008)	§103	6, 7
4	Charas alone and/or in view of Olvera-Hernandez in view of U.S. Pub. 2008/0096559 ("Phillips") (EX1009)	§103	11
5	Charas alone and/or in view of Olvera-Hernandez in view of U.S. Pub. 2005/0164737 ("Brown") (EX1010)	§103	13

Petitioner also relies upon the evidence listed in the Exhibit List (Appendix A), including the Declaration and *Curriculum Vitae* of David Williams (EX1012, ¶¶1-312; EX1013) and Declaration and *Curriculum Vitae* of Fred Rodermund (EX1020, ¶¶1-83; EX1021).

C. Prior Art Qualification of Asserted References

Petitioner assumes the earliest effective '055 Patent filing date as January 28, 2009, the filing date of U.S. Provisional Application No. 61/206,354.² The '055 Patent is subject to pre-AIA 35 U.S.C. §§102/103.

Charas (EX1004), published May 9, 2002 and filed January 15, 2001, is prior art at least under pre-AIA 35 U.S.C. §102(b), being published more than one year prior to the earliest claimed '055 Patent filing date.

Olvera-Hernandez (EX1005), published July 2, 2009 and filed December 23, 2008, is prior art at least under pre-AIA 35 U.S.C. §102(e), as an application published under 35 U.S.C. §122(b).

Mottes (EX1007), published August 19, 2004 and filed December 8, 2003, is prior art at least under pre-AIA 35 U.S.C. §102(b).

Spencer (EX1008), published April 29, 2010 and filed June 6, 2006, is prior art at least under pre-AIA 35 U.S.C. §102(e), as an application published under 35 U.S.C. §122(b).

Phillips (EX1009), published April 24, 2008 and filed December 21, 2007, is prior art at least under pre-AIA 35 U.S.C. §102(b).

² Petitioner does not concede that any challenged claim is entitled to an effective filing date of January 28, 2009.

Brown (EX1010), published July 28, 2005 and filed December 31, 2003, is prior art at least under pre-AIA 35 U.S.C. §102(b).

Mandato (EX1011), published August 22, 2002 and filed December 6, 2001, is prior art at least under pre-AIA 35 U.S.C. §102(b).

Brisebois (EX1017), published April 22, 2010 and filed October 20, 2008, is prior art at least under pre-AIA 35 U.S.C. §102(e), as an application published under 35 U.S.C. §122(b).

Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (3GPP TS 51.011 version 4.10.0 Release 4) (EX1018) constitutes prior art as of January 12, 2004 at least under §102(b). *See* EX1020, ¶¶21, 61.

Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (3GPP TS 51.011 version 4.2.0 of Release 4) (EX1019) constitutes prior art as of October 11, 2001 at least under §102(b). *See* EX1020, ¶¶20, 42.

V. BACKGROUND

A. The '055 Patent

The '055 Patent discloses a wireless end-user device storing multiple service profiles each associated with a service plan and wireless network and including a connection manager that selects a network associated with a selected profile. An adaptive service policy control agent enforces the appropriate

network service policies associated with a selected profile. EX1001, Claim 1. EX1012, ¶27.

Fig. 21 (shown below) illustrates an end-user device that includes a Wireless Wide-Area Network (WWAN) modem (orange, Element [1.1]), a secure memory storing first and second network profiles (not shown, Elements [1.2]/[1.3]), a connection manager (yellow, Element [1.4]), an adaptive service policy control agent (green, Element [1.5]) and an application service interface (purple, Element [1.6]) at which some policies are implemented/enforced on network connections for selected applications (light blue, Element [1.6]).

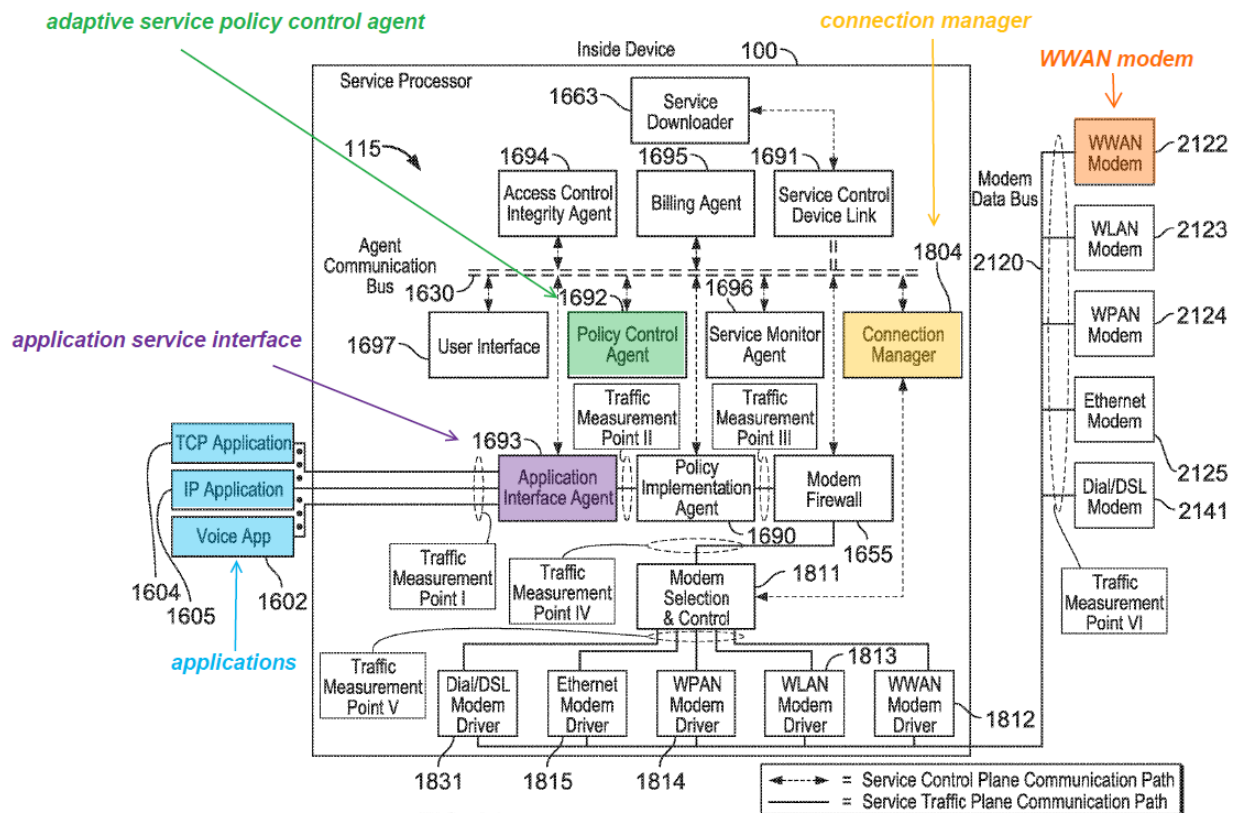


FIG. 21

EX1001, Fig. 21 (Annotated)

EX1012, ¶28.

B. Examination History

The '055 Patent's U.S. Application No. 16/421,121, filed on May 23, 2019 (“the '121 Application”, EX1002) claims priority to seven different continuation applications and four provisional applications, the earliest of which was filed January 28, 2009. EX1003. The '055 Patent was granted in a first action allowance.

1. Examination History of European Application

Before allowance of the '121 Application, Patent Owner filed European Application No. 19219822.4 (Pub No. 3,661,242, “the European counterpart”) on December 27, 2019 (EX1014) claiming priority via an international application number PCT/US2010/021302 that is substantively identical to the '121 application. EX1015.

The European counterpart's claims were rejected in a European search opinion dated April 17, 2020 — nine months before the '121 Application allowance — as lacking novelty based on EP 1,247,411 A2 (“Charas EP”, EX1027), a European equivalent of EX1004. EX1015, pp.780-789.

Patent Owner unsuccessfully argued that Charas EP did not disclose a “connection manager” selecting an access network connection for the WWAN modem based on a false assertion that Charas EP's “service policies are stored on a server.” EX1015, p.767. The European Examiner maintained the rejection citing

Charas’s “access selection function 690” of the user terminal as requesting access and presenting credentials to a “desired access network depending on the service requested” and preparing for interconnection “with the chosen access network.” EX1004, ¶[0052]; EX1015, pp.744, 782. Patent Owner conceded and amended the claims to recite the “application service interface” as a distinct element:

“an application service interface (1693) to interface with one or more applications (1602, 1604, 1605) resident on the wireless end-user device (100), characterized in that first policies included in the one or more network service policies are enforced at the application service interface (1693) on network data connections for the one or more applications (1602, 1604, 1605) interfacing with the application service interface (1693).”

However, Charas also discloses an application service interface (i.e., “applications interface 650”) in an end-user device at which quality of service “parameters” (i.e., policies defining the connection on which the “requested web-service”) are delivered/enforced. EX1004, ¶[0064]. Charas’s “applications interface 650” implements (i.e., enforces) quality of service “parameters” or policies for a network connection on which a “requested web-service” is delivered. EX1004, ¶[0064]; *see* §§I, V.B. *supra*.

2. Examination History of U.S. Application

None of this was brought before the US Examiner. In first action Notices of Allowance dated January 22, 2021 and February 23, 2021, the US Examiner stated

that “all the cited prior art alone or in combination does not disclose Applicant’s inventive claim language.” EX1002, p.16. The ’055 Patent was granted August 17, 2021, over a year after the European search opinion, but Patent Owner did not disclose Charas, its EP equivalent, or the European search opinion to the USPTO. Patent Owner did not amend the claims of the ’121 Application to include the limitations of the European counterpart.

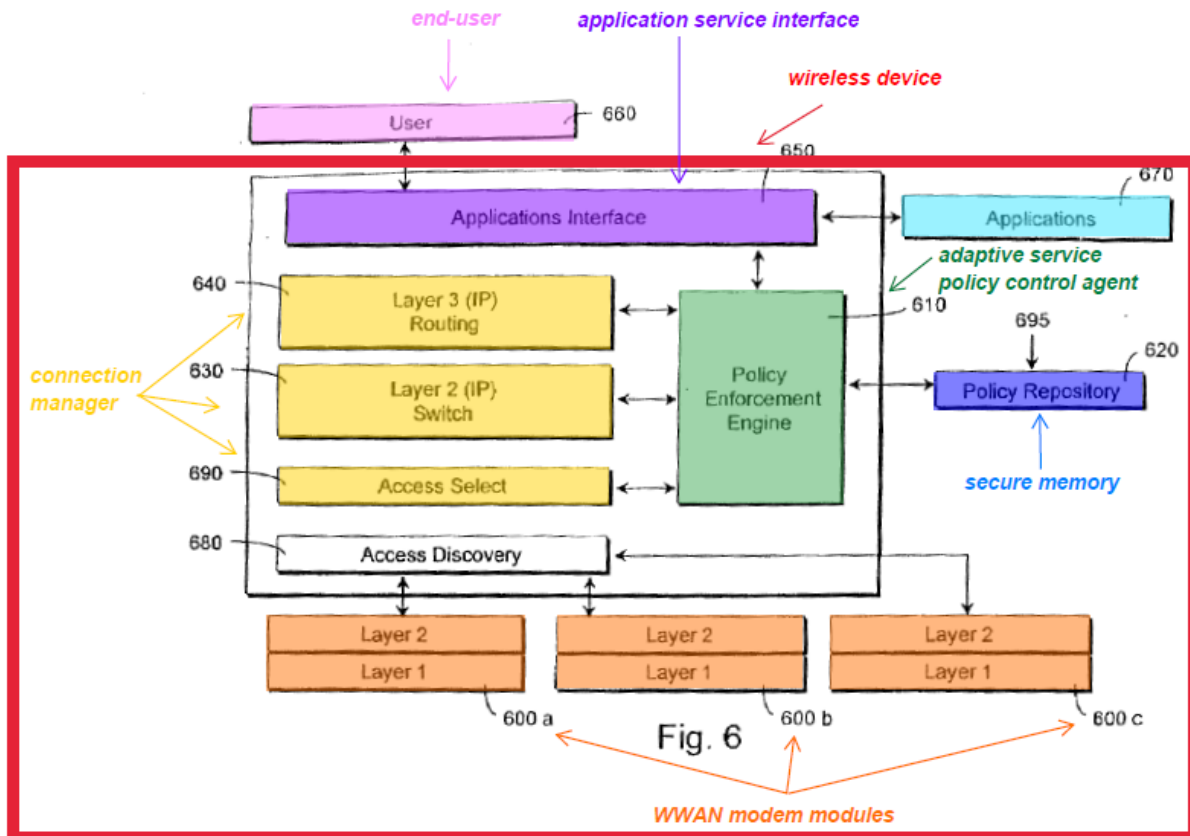
C. Prior Art

1. Charas (EX1004)

Charas (EX1004) is the U.S. equivalent of Charas EP relied upon by the EPO in the European counterpart and not considered by the USPTO, both sharing a common parent publication (EP 1,117,265 A1, App. No. 00850007.6, EX1016). EX1012, ¶43.

Charas’s Fig. 6 (annotated below) shows a *wireless end-user device* (i.e., red client/terminal block, with end-user in pink) including: a modem (orange) for first and second networks; a policy repository (i.e., blue *secure memory*) secured “by e.g. a personal identification code, a fingerprint reading or other means” for storing policy blocks for each subscription/relationship a user holds with a service provider; an access select function, layer 2 IP switch, and layer 3 IP router (i.e., yellow *connection manager*) that select an access network from those discovered by an access discovery function and route data flows to the appropriate modem; a policy

enforcement engine (i.e., green *adaptive service policy control agent*) that “enforces policies defined in policy repositories;” and an applications interface (i.e., purple *applications service interface*) interfacing with one or more *applications* (light blue).



EX1004, Fig. 6 (Annotated)

EX1012, ¶¶43-44.

Charas’s end-user device includes an access selection function “responsible for requesting access and presenting credentials to the desired access network depending on the service requested.” EX1004, ¶[0052]. Charas performs network

access selection in the same manner as the '055 Patent. *See* EX1001, 13:19-21 (“The network selection policy allows the selection of the network that corresponds to the most desirable service profile to meet the user’s service preferences.”). Charas’s policy enforcement engine “enforces policies defined in policy repositories.” EX1004, ¶[0059]. The policy enforcement engine “set[s] up a channel that complies with the agreed parameters” specified by the user “via the applications interface.” *Id.*, ¶[0064]. The channel facilitates the application’s access to the requested service thereby indicating that the policies defining the agreed parameters are enforced on the end-user device’s applications service interface (located in the end-user device at a position which exactly matches ‘055 Patent’s application services interface). EX1012, ¶¶45-49.

2. Olvera-Hernandez (EX1005)

Olvera-Hernandez discloses “various technology specific modems” that are combined within a single “multimode modem” (e.g., WWAN modem). EX1005, ¶[0024]. EX1012, ¶50.

3. Mottes (EX1007)

Mottes discloses a method “enabl[ing] an End User to use and or subscribe to several service providers and or Mobile Virtual Network Operators (MVNOs).” EX1007, Abstract. EX1012, ¶51.

4. Spencer (EX1008)

Spencer discloses as a “user service interface” a “user interface (UI)...send[ing] a web page displaying available service options” from which “[a] service profile is selected” from among multiple service profiles “stored in [a] database.” EX1008, ¶¶0166]. EX1012, ¶52.

5. Phillips (EX1009)

Phillips discloses a “Subscriber Identity Module (SIM)” as a type of “smart card” that enforces network policies by storing and executing “authentication settings” including “an authentication algorithm.” EX1009, ¶¶[0023], [0024]. Phillips’s SIM also maintains a “preferred network list” and implements “Enhanced Operator Named String (EONS) ... for automatic network selection.” *Id.*, ¶¶[0024], [0026]. EX1012, ¶53.

6. Brown (EX1010)

Brown discloses multiple sets of “subscription parameters” that can be selectively “activated, deactivated and reactivated as many times as desired.” EX1010, ¶¶[0008], [0015], [0018], [0033]. EX1012, ¶54.

7. 3GPP (EX1018-EX1019)

3GPP TS 51.011 version 4.10.0 (EX1018) and version 4.2.0 (EX1019) of Release 4 disclose identical user authentication procedures and algorithms performed by a Subscriber Identity Module (SIM). EX1018, §§7.1, 7.2, 9.2.16; EX1019, §§7.1, 7.2, 9.2.16. EX1018 represents the most recent version of 3GPP TS

51.011 as of the filing date of Phillips while EX1019 represents the earliest version of 3GPP TS 51.011 with which Phillips's SIM implementation complies. EX1009, ¶[0026]. EX1012, ¶55.

D. Person of Ordinary Skill in the Art (“POSITA”)

A person of ordinary skill in the art (“POSITA”) relating to the subject matter of the '055 Patent as of January 28, 2009 would have had (1) at least a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in wireless communication network applications and software. Additional graduate education could substitute for professional experience, and *vice versa*. EX1012, ¶36.

VI. CLAIM CONSTRUCTION

Petitioner interprets the claims “in accordance with the ordinary and customary meaning ... as understood by one of ordinary skill in the art.” 37 C.F.R. §42.100(b). *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*).

In the Related Litigation, Petitioner proposes “subscriber identity module (SIM)” should be construed as:

Subscriber Identity Module as described in the ETSI/3GPP standards in existence at the time of the claimed invention.

EX1022, 3; EX1026, 2. Patent Owner proposes that the term be given its plain and ordinary meaning. *Id.* See also EX1023, EX1024, and EX1025. The prior art cited

herein discloses the noted term under Petitioner's and Patent Owner's proposed constructions and any other constructions, as demonstrated herein. EX1012, ¶41.

VII. THE CHALLENGED CLAIMS ARE UNPATENTABLE

The Challenged Claims are unpatentable over the prior art. EX1012, ¶¶56-57.

A. Claims 1-4, 8-10, and 12 are Anticipated and/or Obvious over Charas (EX1004) alone and/or in view of Olvera-Hernandez (EX1005) (Ground 1)

1. Claim 1 (Preamble): "A wireless end-user device comprising:"

To the extent the Preamble is limiting, Charas discloses/suggests a wireless end-user device as a "client" or "mobile terminal" including a transport domain "preferably implemented as interchangeable modules (modems) for different access standards." EX1004, ¶¶[0012], [0041], [0051], [0068] (emphasis added). EX1012, ¶58.

Charas's Fig. 6 (*see*, §V.C.1., *supra*) illustrates a client/terminal as a "user terminal" having "interchangeable modules (modems)" supporting access to, for example, a "W-CDMA" network; Charas's Fig. 1 illustrates an example of a global network technology for "global roaming" between wireless wide-area networks (WWANs) of different standards. EX1004, Abstract, ¶¶[0012], [0041], [0066], Figs. 1, 6. A POSITA would have understood that the different W-CDMA, EDGE, CDMA 2000, and W-LAN standards referenced by Charas are wireless network standards.

Id., ¶[0041]. Charas’s Fig. 6 illustrates a “user” and an exemplary embodiment of a user terminal. EX1004, ¶[0025], Fig. 6. EX1012, ¶¶59-61.

Charas’s user client/terminal is a wireless end-user device. EX1012, ¶62.

a. [1.1]: “a Wireless Wide-Area Network (WWAN) modem;”

Charas discloses/suggests Element [1.1]. Charas’s wireless end-user device (i.e., client/terminal in annotated Fig. 6, §V.C.1., *supra*) includes a WWAN modem to access a first wireless network (e.g., the Fig. 1 “W-CDMA network”) and a second wireless network (e.g., the Fig. 1 “GPRS network”). EX1012, ¶¶63-64.

Charas’s wireless end-user device includes “interchangeable modules (*modems*) for different access standards such as *W-CDMA, EDGE, CDMA2000*, ... etc.” *See* VII.A.1, *supra*; EX1004, ¶[0041] (emphasis added). The module that connects to the W-CDMA network and the module that connects to the GPRS network are contained within the same “terminal” constituting a WWAN modem. EX1004, Fig. 6 (*see* §V.C.1., *supra*). Figure 6 illustrates the WWAN modem modules “physically located in the terminal itself...” (i.e., on the wireless end-user device). EX1004, ¶[0050]. EX1012, ¶¶65-67.

Patent Owner did not distinguish the WWAN modem of the European counterpart claims over Charas’s WWAN modem configuration. *See* §V.B.1. Patent Owner tacitly conceded Charas’s disclosure of this Element in amending the EP counterpart claims. EX1012, ¶68.

A POSITA would have understood that “WWAN” encompasses different cellular telecommunication technologies that cover large geographical areas. W-CDMA (wideband code-division multiple access), EDGE (enhanced data rates for GSM evolution), and CDMA2000 are WWAN communication technologies (i.e., standards). The '055 Patent explicitly identifies W-CDMA as a WWAN technology. EX1001, 158:11-17. EX1012, ¶¶69-70.

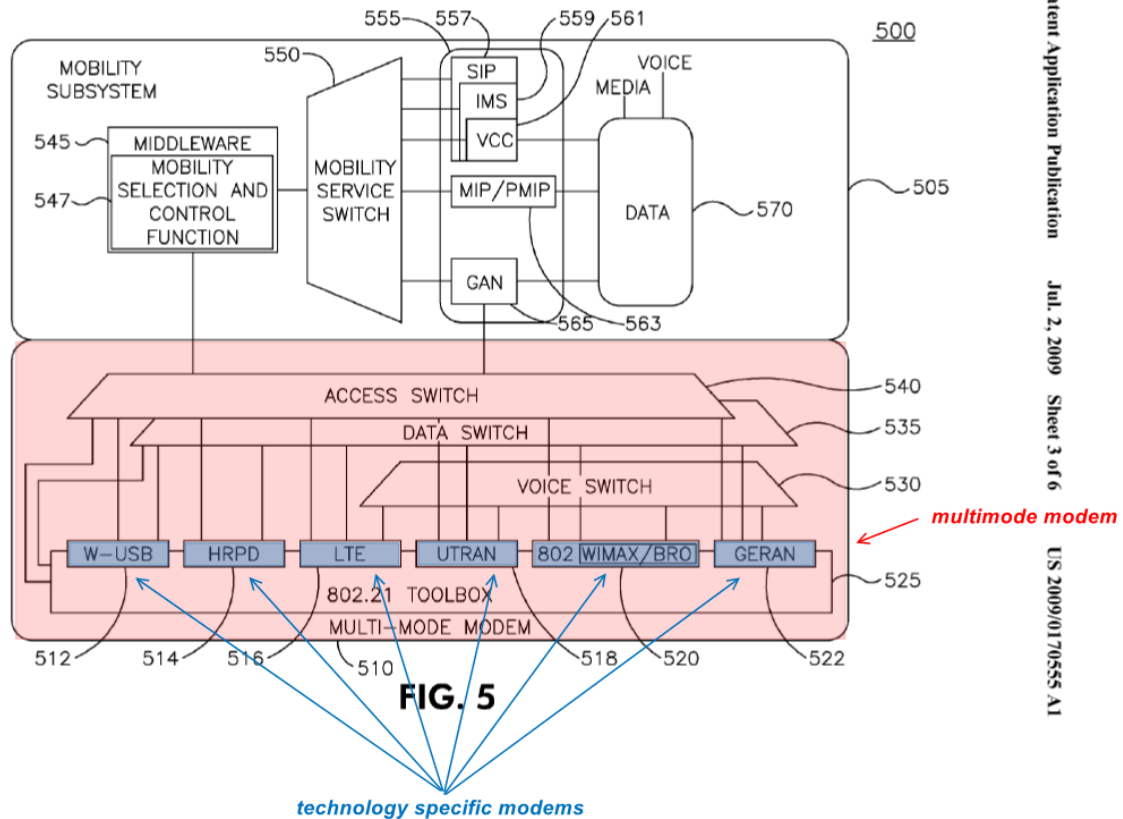
Olvera-Hernandez

Charas’s interchangeable modem modules contained within a single terminal provide a multimode capability. To the extent it is argued that Charas’s multimode capability is not within a single WWAN modem, Olvera-Hernandez discloses multimode capability supporting multiple access standards in a single multimode WWAN modem. Olvera-Hernandez’s WWAN “multimode modem 510” combines “various technology specific modems” to support similar access standards as disclosed by Charas (e.g., 2G, 3G standards). EX1001, 12:52-59; EX1005, ¶[0024], Fig. 5. Element [1.1] is therefore satisfied by Charas alone or in combination with Olvera-Hernandez. EX1012, ¶¶71-73.

Charas enables “access independent global roaming between heterogeneous networks.” EX1004, ¶[0029]. Charas’s terminal includes an access discovery function 680 that “continuously” scans for available access networks and an access selection function 690 that dynamically selects the best network for a requested

service. *Id.*, ¶[0052]. This architecture contemplates that multiple supported access technologies—W-CDMA, EDGE, CDMA2000, GPRS, and others—are simultaneously available on the terminal. *Id.*, ¶[0051]. A POSITA implementing Charas would have been motivated to integrate the terminal’s various technology-specific modules as a single multimode WWAN modem. EX1012, ¶¶74-76.

Olvera-Hernandez addresses the same problem of mobility between “heterogeneous access networks,” and every terminal it depicts includes a multimode modem as a baseline architecture. EX1004, ¶¶[0029], [0063]; EX1005, ¶¶[0005]-[0006], [0010], Fig. 6. Olvera-Hernandez’s multimode modem 510 houses “various technology specific modems” and specifically multiple WWAN technologies (e.g., LTE modem 516, UTRAN modem 518, WiMAX modem 520, GERAN modem 522) that correspond directly to Charas’s interchangeable modules for “different access standards such as W-CDMA, EDGE, CDMA 2000.” EX1005, ¶[0024], Fig. 5; EX1004, ¶[0041].



Patent Application Publication Jul. 2, 2009 Sheet 3 of 6 US 2009/0170555 A1

EX1005, Fig. 5 (Annotated)

EX1012, ¶¶77-78.

A POSITA would have been motivated to implement the interchangeable modules of Charas’s single multimode terminal as an integrated multimode modem as disclosed by Olvera-Hernandez. First, a POSITA would have been motivated to facilitate access to a selected group of heterogeneous network standards through a singular, centralized multimode WWAN modem. EX1005, ¶[0003], ¶[0008] (“mobility functions” (which enable switching between access standards) are

“supported by the various interface technologies of the multimode modem 420.”). EX1012, ¶¶79-80.

Second, implementing Charas’s interchangeable modules as a single integrated multimode modem would have involved simply consolidating Charas’s modules into a single platform on the terminal or substituting Charas’s modules with a single multimode modem as taught by Olvera-Hernandez. Both Charas and Olvera-Hernandez are directed to facilitating access and switching between heterogeneous network standards. Such a consolidation/substitution would have merely involved grouping the technology specific WWAN modems of Charas’s device into a single multimode WWAN modem as disclosed by Olvera-Hernandez to facilitate access to heterogeneous network standards. EX1012, ¶¶81-82.

Third, the combination would have been straightforward/predictable. Consolidating Charas’s separate interchangeable modules into a single multimode modem as disclosed by Olvera-Hernandez or simply substituting Olvera-Hernandez’s multimode modem into Charas, would have preserved Charas’s control and traffic-flow architecture. Charas’s higher-layer control functions operate above the Fig. 6 modem layer. Olvera-Hernandez’s architecture similarly places higher layer control functions such as “mobility selection and control function (MSCF)” in an application layer above its multimode modem. EX1005, ¶[0011]. Charas’s traffic flows would also have been preserved among the interchangeable modules via the

“layer 2 IP switch 630 and a layer 3 IP router 640” (EX1004, ¶[0008]). A POSITA would have recognized Charas’s layer 2 IP switch 630 and layer 3 IP router 640 function similarly to Olvera-Hernandez’s access switch 540 and would therefore manage transitions between access standards in a multimode modem as disclosed by Olvera-Hernandez. EX1005, ¶¶[0024], [0027]. A POSITA would have had a reasonable expectation of success in combining Charas’s modules into a single WWAN multimode modem as disclosed by Olvera-Hernandez without disturbing the higher-layer functionality and traffic flows of Charas. EX1012, ¶¶83-87.

Charas, either alone or in combination with Olvera-Hernandez, discloses a WWAN modem. EX1012, ¶88.

b. [1.2]: “a secure memory to store a first service profile associated with a first service plan and a first wireless network accessible through the WWAN modem, the first service profile comprising a first set of network service policies, and”

Charas discloses/suggests Element [1.2]. Charas discloses a secure memory (“policy repository 620”; *see* annotated Fig.6, §V.C.1., *supra*) to store a first service profile (e.g., a first of “several policy blocks”) associated with a first service plan (e.g., a first “subscription” relationship) and a first wireless network (e.g., the Fig. 1 “W-CDMA network”) accessible through the WWAN modem, the first service profile comprising a first set of network service policies (e.g., policy block “rights”). EX1004, ¶¶[0052], [0054], [0056]-[0058]. EX1012, ¶¶89-90.

Secure memory to store a first service profile

Charas's "***policy repository 620***" is a secure memory on the terminal and is responsible for storing service profiles (i.e., "policy blocks defining the relationships that exists [sic] between the user 660 and different service providers as well as individuals."). EX1004, ¶[0057]. *See also* §V.C.1. (annotated Fig. 6), *supra*. Charas's policy repository is secure because outside access is achieved via "a personal identification code, a fingerprint reading or other means," similar to the '055 Patent's use of "pass keys and/or other security mechanisms." EX1001, 28:30-39; EX1004, ¶[0058]. EX1012, ¶¶91-92.

First service profile comprising a first set of network service policies

Charas's "policy block" stored in policy repository 620 constitutes a first service profile. EX1004, ¶[0057]. Charas's policy repository "contains several policy blocks defining the relationships that exist[] between the user 660 and different service providers as well as individuals." *Id.* EX1012, ¶¶93-94.

The policy blocks comprise "network service policies" as claimed at least because they contain policies for network service in relation to the "different service providers" and other "individuals" with which the user 660 has a defined relationship. Charas specifies that "policies" refer to, "among others, a set of ***rights and obligations pertaining to authentication of users, authorization to access and services...***" EX1004, ¶[0014]. EX1012, ¶¶95-96.

Charas's policy blocks comprise a set of parameters "defin[ing] the relationships that exist between the user 660 and different service providers" and include "rights, obligations, shared secret, and address to a credential verifier or SMP." EX1004, ¶[0057]. These parameters include Quality of Service (QoS) parameters agreed upon by the user and the service provider via "applications interface 650." To initiate a web-service, a user and provider "agree on parameters, i.e. some Quality of Service value for the session, e.g. the transmission rate." *Id.*, ¶[0064]. *See also id.*, ¶¶[0031], [0042], [0057]-[0058] ("[S]ervers" (i.e., "providers") and "clients" (e.g., "a user") are connected on "a Quality of Service basis."). These parameters correspond to the service policies (i.e., "access control settings, traffic control settings" and "authentication settings") that the '055 Patent discloses are part of its service profile. EX1001, 8:49-55. A POSITA would have understood that the "rights" and "obligations" of Charas's policy blocks define the set of services and features to which a user has access, thereby constituting access control settings. EX1004, ¶[0057]; EX1012, ¶¶97-100.

A POSITA would have also understood that Charas's "Quality of Service" policies constitute traffic control settings. EX1001 56: 46-51 ("traffic shaping QoS control"); EX1004, ¶[0064]. The "rights," "shared secret," and "address to a credential verifier or SMP" constitute exemplary authentication settings. *Id.* ¶[0014].

Charas's first service profile comprises a first set of network policies. EX1012, ¶¶101-103.

First service profile associated with a first service plan

Charas's policy block is associated with a service plan as recited in Element [1.2]. Charas's policy blocks "defin[e] the relationships"—e.g., subscriptions—"that exist[] between the user 660 and different service providers." EX1004, ¶[0057]; *see also id.*, ¶[0056] (describing the "relationship" between subscriber A and provider X as a "private subscription"). Charas's "subscription with provider X for voice and web browsing" providing services that are "paid for...per invoice from a service provider" constitutes a first service plan. *Id.*, ¶¶[0014], [0056]. Because Charas's relationships (i.e., subscriptions) are "defin[ed]" by policies within a "policy block," they are associated with a service profile. *Id.*, ¶[0057]. EX1012, ¶104.

First service profile associated with a first wireless network accessible through the WWAN modem

Charas's service profiles (i.e., "policy blocks") are associated with a first wireless network as recited in Element [1.2]. Charas discloses that service providers can tie their service to a specific wireless access network. EX1004, ¶[0055] ("[A] special access network or a special gateway might need to be used or passed before a particular service can be executed."). A policy block defining a subscription with a service provider is therefore associated with the wireless network that the service provider requires. EX1012, ¶¶105-106.

Charas discloses that a requested service is associated with a “desired access network” (e.g., a “W-CDMA network”). *See* EX1004, ¶[0052] (“access selection function 690” is “responsible for requesting access and presenting credentials to the *desired access network depending on the service requested* from the service layers.”) (emphasis added). The requested services are provided based on a subscription defined by the policy block and are associated with specific networks. Charas’s policy enforcement engine 610 “enact[s] the requested web-service” specified by “the applications interface 650” by “collect[ing] data from the policy repository 620 and the access selection function 690 to set up a channel that complies with the agreed parameters...The policy enforcement engine 610 then *launches the requested web-service according to the policies in the policy repository.*” *Id.*, ¶¶[0064]-[0065] (emphasis added). The policies of a given policy block define a specific relationship (i.e., subscription) a user has with a respective service provider. *See id.*, ¶¶[0057]-[0058]. The access selection function then selects the “chosen access network” according to the policies received from the policy repository via the policy enforcement engine (e.g., “depending on the service requested”). *Id.*, ¶[0052]. As explained in Element [1.1], the access networks are accessible through a WWAN modem. EX1012, ¶¶107-110.

Combining the interchangeable modules of Charas’s single terminal unit into a multimode modem as disclosed by Olvera-Hernandez would not have disrupted

Charas’s disclosure of a first service profile associated with a first wireless network accessible through a WWAN modem. *See* §VII.A.1.a., *supra*. Olvera-Hernandez’s MSCF can package a “collection” of “mobility services” (i.e., a first service profile) and “select[] an optimum air interface technology” for those services. EX1005, ¶[0027]. These mobility services require (i.e., are associated with) “specific air interface technologies” which are in turn associated with specific “access networks” (i.e., first wireless network, e.g., E-UTRAN network 810 as shown in Fig. 8) accessible by Olvera-Hernandez’s multimode modem (i.e., WWAN modem). *Id.*, ¶¶[0030]-[0031], Fig. 8. *See also id.*, ¶[0031] (“certain mobility service 555, such as GAN 565, require specific air interface technologies”). Olvera-Hernandez also discloses a first service profile associated with a first wireless network accessible through a WWAN modem. Consolidating/replacing Charas’s interchangeable modules into/with a multimode modem as taught by Olvera-Hernandez would not have disrupted Charas’s disclosed functionality and would have been obvious. EX1012, ¶¶111-113.

Thus, Charas discloses and renders obvious Element [1.2]. EX1012, ¶114.

- c. [1.3]: “a second service profile associated with a second service plan and a second wireless network accessible through the WWAN modem, the second service profile comprising a second set of network service policies;”**

Charas discloses/suggests Element [1.3]. Charas discloses a secure memory (“policy repository 620”) to store a second service profile (e.g., a second of the

“several policy blocks”) associated with a second service plan (a second “subscription” relationship) and a second wireless network (e.g., the Fig. 1 “GPRS network”) accessible through the WWAN modem, the second service profile comprising a second set of network service policies (e.g., policy block “rights”). EX1004, ¶¶[0052], [0054], [0056]-[0058]. EX1012, ¶¶115-116.

Charas discloses “*several policy blocks* defining the relationships that exist[] between the user 660 and *different* service providers” or “access providers.” EX1004, ¶¶[0054], [0057]. A second policy block therefore corresponds to a second access provider and a second wireless network. Charas expressly indicates that access providers have different networks by: (1) noting that a “requested network” is associated with an “appropriate access supplier” (i.e., access provider); and (2) specifying that “access providers can accept different types of payment methods...for access to *their networks*.” EX1004, ¶¶[0042], [0065]. EX1012, ¶¶117-119.

Each of Charas’s subscriptions (i.e., service plans), defined by their own “policy blocks” (i.e., service profiles), can be “hierarchical” and can therefore be associated with a “*special access network*” (wireless network). *See* §VII.A.1.b., *supra*; EX1004, ¶¶[0055-57] (emphasis added). The “specific policy” defining the relationship a “subscriber A” has with “provider X” for, e.g., a “voice service” and the “policy” defining the relationship “subscriber A” has to another service provider

(e.g., “bank at which [they] have an account”) correspond to first and second policy blocks (i.e., service profiles) associated with first and second “special access network[s]” (i.e., first and second wireless networks). *Id.*, ¶¶[0056]-[0057]. EX1012, ¶¶120-121.

It would have been obvious to a POSITA for the first wireless network (e.g., the Fig. 1 “W-CDMA network”) and the second wireless network (e.g., the Fig. 1 “GPRS network”) to be accessible through “the WWAN modem” as recited in Element [1.3]. Charas’s interchangeable modules are contained within the same “terminal” constituting a WWAN modem and correspond to access *standards* (e.g., W-CDMA, GPRS, etc.) that are not limited to any particular *network*. See EX1004, ¶[0041]; see §VII.A.1.a., *supra*. Where two policy blocks are associated with two networks using a same standard (e.g., where first wireless network and second wireless network are both GPRS networks)—a well-known and common occurrence—their networks would both be accessible through the same WWAN modem Charas contemplates this occurrence as “different services” (e.g., of first and second policy blocks) provided by “non-hierarchical” service providers can be “enacted at the same level, e.g. in that *any access network may be used.*” EX1004, ¶[0055] (emphasis added). A POSITA would have used the single GPRS module of Charas to access both networks as there would be no need for a second WWAN modem. EX1012, ¶¶122-126. At the time of the ’055 Patent, for example, AT&T

and T-Mobile each operated GPRS networks, and GPRS modems were compatible with both networks. Patent Owner did not distinguish the WWAN modem of the European counterpart claims over Charas's WWAN modem configuration. *See* §§V.B.1. and VII.A.1.a., *supra*. EX1012, ¶¶127-128.

To the extent it is argued that Charas's multimode capability of its terminal does not constitute a single WWAN modem, Olvera-Hernandez discloses multimode capability supporting multiple access standards in a single multimode WWAN modem. *See* §VII.A.1.a., *supra*, EX1001, 12:52-55; EX1005, ¶[0024], Fig. 5. Olvera-Hernandez also discloses a second service profile (i.e., a second "combination[] of mobility services") associated with a second wireless network (i.e., a second "access network", e.g., GERAN network 820 as shown in Fig. 8) accessible by the multimode modem (i.e., WWAN modem). EX1005, ¶¶[0030]-[0031], Fig. 8. Because Olvera-Hernandez also discloses a second service profile associated with a second wireless network accessible through a WWAN modem, consolidating/replacing Charas's interchangeable modules into/with a multimode modem as taught by Olvera-Hernandez would not have disrupted Charas's disclosed functionality and would have been obvious. EX1012, ¶¶129-131.

Charas either alone or in combination with Olvera-Hernandez discloses and renders obvious Element [1.3]. EX1012, ¶132.

d. [1.4]: “a connection manager to select an access network connection for the WWAN modem, based on a selected one of the first and second service profiles;”

Charas discloses/suggests Element [1.4]. Charas discloses a connection manager (i.e., “access selection function 690” and “layer 2 IP switch 630” and “layer 3 IP router 640” (*see* annotated Fig.6, §V.C.1., *supra*) to select an access network connection (i.e., for a “desired access network”) for the WWAN modem, based on a selected one of the first and second service profiles (i.e., policy blocks). EX1004, ¶¶[0052], [0057]. EX1012, ¶¶133-134.

Charas’s access selection function is “responsible for requesting access and presenting credentials to the *desired access network depending on the service requested* from the service layers and also for preparing to interconnect with the *chosen access network.*” EX1004, ¶[0052] (emphasis added). Because the “requested web-service” is launched “according to the policies in the policy repository 620”, the “desired access network” is selected based on the policies of a subscriber’s service profile (i.e., policy block). *Id.*, ¶[0065]. EX1012, ¶¶135-136.

Where the first and second service profiles are associated with first and second networks accessed by a common standard (e.g., GPRS), the access selection function 690 selects the access network “for the WWAN modem.” *See* §VII.A.1.c., *supra*. Charas therefore discloses a connection manager to select a network connection based on the selected service profile. Charas’s layer 2 switch and layer 3 router

constitute components of the connection manager to the extent that they route data between access networks. *See* EX1004, ¶[0051]; *see infra* §VII.A.7 (Claim 10). EX1012, ¶¶137-139.

Consolidating/replacing Charas’s interchangeable modules into/with a multimode modem as taught by Olvera-Hernandez would not disrupt Charas’s disclosure of a connection manager to select an access network connection for the WWAN modem based on a selected one of the first and second service profiles. Olvera-Hernandez’s architecture also enables routing functionality through a MSCF and various switches (i.e., connection manager). EX1005, ¶¶[0027]-[0028], [0030]-[0031]. Olvera-Hernandez’s MSCF “selects and controls a mobility service 555 [or combinations of mobility services (i.e., first and second service profiles)] and a lower layer air interface technology ... that is capable of carrying the mobility service 555 independently via the mobility service switch 550 and the access switch 540,” where each air interface technology is associated with an access network (i.e., first and second wireless networks) accessible through the multimode modem. *Id.*, ¶[0030]. *See* §VII.A.1.c., *supra*. Because Olvera-Hernandez also discloses a connection manager configured to select an access network connection for the WWAN modem based on a selected one of first and second service profiles, consolidating/replacing Charas’s interchangeable modules into/with a multimode

modem as taught by Olvera-Hernandez would not have disrupted Charas's disclosed functionality and would have been obvious. EX1012, ¶¶140-142.

e. [1.5]: “at least one adaptive service policy control agent to enforce network service policies associated with the selected one of the first and second service profiles,”

Charas discloses/suggests Element [1.5]. Charas discloses at least one adaptive service policy control agent (i.e., “policy enforcement engine 610”; *see* annotated Fig. 6, §V.C.1., *supra*) to enforce network service policies (e.g., rights, obligations, etc.) associated with the selected one of the first and second service profiles (i.e., policy blocks). EX1004, ¶¶[0059], [0064]-[0065]. EX1012, ¶¶143-144.

Charas's policy enforcement engine “*enforces policies* defined in policy repositories 620” and “launches the requested web-service *according to the policies* in the policy repository 620.” EX1004, ¶¶[0065] (emphasis added). These policies are network service policies associated with the selected one of the first or second service profiles as discussed above for Element [1.2]. *See* §VII.A.1.b, *supra*; *see* EX1004, ¶[0057]. Charas's policy enforcement engine therefore enforces network service policies associated with a selected service profile. EX1012, ¶¶145-146.

Policies enforced by Charas's policy enforcement engine are the same as policies enforced by the adaptive service policy control agent of the '055 Patent. The “set[s] of rights and obligations” stored as policy blocks in Charas's policy

repository and subsequently enforced by Charas's policy enforcement engine include those "*pertaining to authentication of users.*" EX1004, ¶¶[0014], [0057], [0059] (emphasis added). Charas's policy enforcement engine also enforces Quality of Service parameters (i.e., policies) agreed upon by the user (i.e., subscriber) corresponding to the selected one of the first and second profiles. *See* §VII.1.A.b, *supra*; *see also* EX1004, ¶[0064] (to initiate a web-service, a user 660 will "agree on parameters, i.e. some Quality of Service value for the session ... policy enforcement engine 610 then collects data from the policy repository 620 [i.e., policy block] to set up a channel that complies with the agreed parameters and the requested web-service"). The '055 Patent similarly discloses service policies enforced by the adaptive service policy control agent as including "access control settings, traffic control settings, ... *authentication settings* and admission control settings." EX1001, 8:49-55 (emphasis added). EX1012, ¶¶147-150.

Charas's policy enforcement engine is "adaptive" because it adapts to network conditions, including Quality of Service requirements and network access technology. When a user requests a service, there is an agreement on "parameters, i.e. some Quality of Service value for the session." EX1004, ¶[0064]. The policy enforcement engine "collects data from the policy repository 620 and the access selection function 690 to set up a channel that *complies with the agreed*

parameters”—e.g., the Quality of Service—“and the requested service and thereafter activates the connection.” *Id.*, ¶[0064]. EX1012, ¶¶151-152.

By collecting data from the access selection function when selecting access networks, Charas’s policy enforcement engine adapts to the selected network. EX1004, ¶¶[0052], [0064]. For example, policy blocks in the repository can be organized into hierarchical relationships in which “a special access network or a special gateway might need to be used or passed before a particular service can be executed.” *Id.*, ¶[0055]; *see* §VII.1.A.b., *supra*. When changing between first and second networks under this hierarchy, policy blocks depending on the first network would no longer be enforced, and those depending on the second network would be enforced. *Id.*, Fig. 7. EX1012, ¶¶153-154.

Charas’s policy enforcement engine adapts its enforcement by consulting the policy repository and applying the policy blocks corresponding to the selected network and requested service. This is consistent with the ’055 Patent’s description of adaptive policy control as adjusting “service policy based on one or more other service policy settings, the service profile and/or the service plan associated with the device.” EX1001, 49:51-56; *see also id.*, 50:33-44 (policy control agent performs a “service control algorithm to assist in managing overall network capacity or application QoS (Quality of Service)” and “an access network selection algorithm to determine which access network to connect to based on connection options and

determine strengths of available wireless networks...”). *See infra.*, §VII.A.6 (Claim 9). EX1012, ¶¶155-156.

Charas’s policy enforcement engine constitutes at least one adaptive service policy control agent to enforce network service policies associated with the selected one of the first and second service profiles. EX1012, ¶157.

f. [1.6]: “the enforced network service policies including policies enforced at an application service interface on network data connections for selected applications resident on the device.”

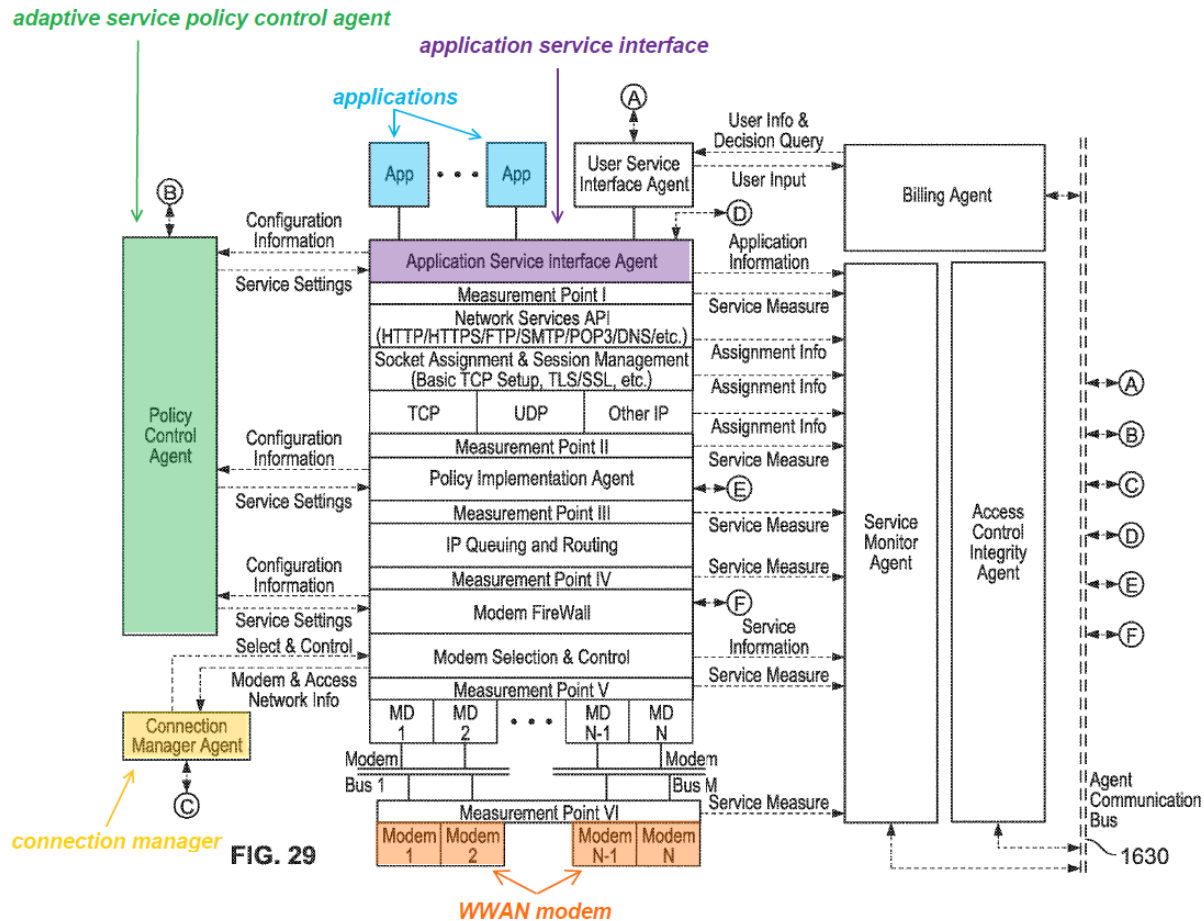
Charas discloses/suggests Element [1.6]. Charas’s adaptive service policy control agent (i.e., policy enforcement engine 610; *see* annotated Fig. 6, §V.C.1., *supra*) enforces network service policies at an “applications interface 650” (i.e., application service interface) for selected applications (e.g., “applications 670”) resident on the device. *See* §VII.A.1.e., *supra*, EX1004, ¶¶[0031], [0050]-[0051], [0053], [0064]-[0065]. EX1012, ¶¶158-159.

Charas’s applications interface is between “applications 670” resident on the device and the network layer stack (i.e., elements 610, 630, 640, 680, and 690 in Fig. 6) which establishes the network data connections. *See* EX1004, Fig. 6 (§V.C.1., *supra*). Charas’s applications are “selected” applications because they are associated with “requested web-service[s],” and can be selectively disconnected by the policy enforcement engine after data associated with the requested web-service has been received. EX1004, ¶[0064] (“the policy enforcement engine 610

disconnects the application 670 and assembles accounting data” for the “requested web-service”). Charas’s end-user device (i.e., terminal) includes applications 670. *See* §V.C.1., *supra* (annotated Fig. 6). Charas therefore discloses enforcing service policies over network data connections for selected applications resident on the device. EX1012, ¶¶160-163.

Charas’s applications interface is located between applications resident on the device and the adaptive service policy control agent (i.e., policy enforcement engine 610). EX1004, ¶¶[0050], [0053], [0064], Fig. 6 (*see* §V.C.1., *supra*). EX1012, ¶164.

Charas’s applications interface performs the functions of the applications service interface disclosed in the ’055 Patent. The ’055 Patent discloses an “application interface agent 1693” or “application service interface layer” located “above the standard networking stack API.” EX1001, 95:62-66, Fig. 29 (annotated below).



EX1001, Fig. 29 (Annotated)

EX1012, ¶165.

The enforced network service policies include at least Quality of Service policies. *See* §VII.A.1.e, *supra*. Charas enforces Quality of Service policies at the applications interface 650 on network data connections established by the network layer stack for selected applications resident on the device. *See* EX1004, ¶[0064] (“Quality of Service (QoS) value for the session, e.g. the transmission rate” is agreed upon “via the applications interface 650”; applications interface 650 uses the policy enforcement engine 610 to enact a requested web-service by setting up “a **channel**

that complies with the agreed [QoS] parameters.”) (emphasis added). Charas’s QoS policy enforcement is similar to “traffic shaping QoS control,” of the ’055 Patent. EX1001, 56:46-51. Charas’s network data connection (i.e., channel) “complies with the agreed [QoS] parameters.” EX1004, ¶¶[0064]. Therefore, a POSITA would have understood that Charas’s QoS policies are enforced at an applications service interface on network data connections for selected applications resident on the device. *See also* Mandato (EX1011), ¶¶[0025], [0152]. EX1012, ¶¶166-168.

2. **Claim 2: “The wireless end-user device of claim 1, the first service profile further comprising first device credentials and the second service profile further comprising second device credentials, the wireless end-user device further comprising a device master agent credential that is independent of the first and second device credentials.”**

Claim 2 is anticipated and/or obvious over Charas alone and/or in view of Olvera-Hernandez. *See* §VII.A.1., *supra*. Charas’s first and second service profiles (i.e., policy blocks) respectively comprise first and second device credentials (i.e., “shared secrets”) and its wireless end-user device (i.e., “terminal”) comprises a device master agent credential (i.e., “LPEP (local policy enforcement point) key 350”) independent of the first and second device credentials. EX1004, ¶¶[0039], [0054], [0057]. EX1012, ¶¶169-170.

Each of Charas’s service profiles (i.e., “policy blocks”) includes its own “shared secrets” used to generate encryption keys (which are also shared secrets) authenticating the subscriber with the service provider. EX1004, ¶¶[0039], [0054].

This corresponds to embodiments of credentials in the '055 Patent, which include “parameters that the network and/or device uses (e.g. requires) to admit the device onto the network and associate it with the appropriate service profile and/or service plan.” EX1001, 136:46-50. Because each policy block contains such shared secrets, Charas discloses a first service profile further comprising first device credentials and a second service profile further comprising second device credentials. EX1012, ¶¶171-172.

Charas discloses as “a device master agent credential” an “LPEP (Local Policy Enforcement Point) key...used for identifying the LPEP 110” of the wireless end-user device to a server cluster or “SMP (Secure Mobile Portal) 100.” EX1004, ¶[0046]. Thus, where the shared secrets within the policy block (first and second device credentials) authenticate the subscriber with the provider, the LPEP key authenticates the LPEP (e.g., policy enforcement engine) to the server. EX1012, ¶173.

Charas’s SMP is a server cluster that “acts as a Policy Definition Point (PDP) for the LPEP 110” and “[e]ach LPEP 110 has a set of policies associated with it and the relationship between the PDP and the LPEP 110 i.e. between the SMP 100 and the subscriber is uniquely defined by these policies.” The master agent of the '055 Patent is likewise a “service owner” or “service distributor” consisting of “multiple activation servers 160.” EX1001, 142:38-46, 143:26-41, 148:32-39. Like Charas’s

LPEP key, the device master agent credential of the '055 Patent is “a unique credential in the device that ... can be recognized and recorded by the network ... or other service entity at time of activation.” EX1001, 120:24-40. Charas’s LPEP key therefore constitutes a device master agent credential that is independent of the first and second device credentials. Figure 3 illustrates the LPEP Key 350 as independent from the “Secret” stored in the Authorisation Database 300 for each policy block.

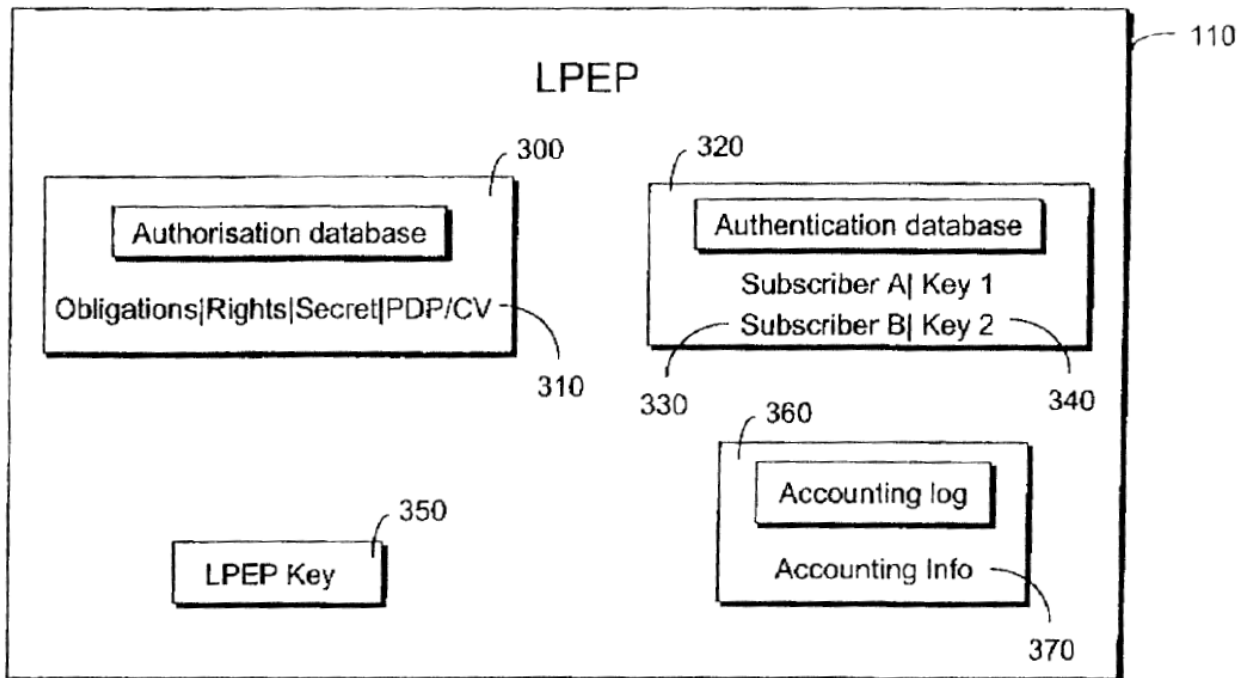


Fig. 3

EX1004, Fig. 3

EX1012, ¶¶174-176.

Maintaining the Charas/Olvera-Hernandez combination would have been obvious as Charas's device and master agent credentials satisfying claim 2 would not have been disrupted. *See* Claim 1, §VII.A.1., *supra*. EX1012, ¶177.

3. Claim 3: “The wireless end-user device of claim 1, further comprising a service monitor agent to record network service usage categorized by sub-account for different wireless networks, including separate service usage counts associated with each of the first service plan and the second service plan.”

Claim 3 is obvious over Charas alone or in combination with Olvera-Hernandez. *See* §VII.A.1., *supra*. Charas discloses a service monitor agent (i.e., “LPEP”) to record network service usage (i.e., “transactions”) categorized by sub-account for different wireless networks (i.e., subscriber-initiated “session”), including service usage counts associated with first and second service plans (i.e., Charas's multiple subscriptions). EX1001, ¶¶[0049], [0051], [0056]. EX1012, ¶¶178-179.

The “service monitor agent 1696” of the '055 Patent “records and reports device service usage or service activities of device 100.” EX1001, 53:10-12. After “enact[ing] [] the requested service” for the subscriber, Charas's LPEP similarly “monitors [] all transactions between the LPEP 110 and the SMP 100,” and “maintains an accounting log 360 containing accounting information 310 pertaining to a session, such as start time, stop time and service utilised.” EX1004, ¶[0047]. Because this accounting is done on a per-session basis, a POSITA would have

understood that it would include separate service usage counts associated with the respective subscriptions associated with each policy block—i.e., with the first and second service plans – into individual sub-accounts. EX1012, ¶¶180-181.

A POSITA would have understood that Charas’s disclosure teaches monitoring service usage by sub-account as such techniques were widely recognized in the prior art. *See also* Swanburg which creates a sub-account as a subscriber “sub-profile” based on service usage. EX1006, 3:1, 5:47-59. Charas’s policy blocks can be associated with specific wireless networks via, e.g., hierarchical relationships between policy blocks and “special access network[s]” (*see infra*, §VII.A.6, Claim 9) to categorize usage by sub-accounts for different wireless networks). EX1012, ¶¶182-183.

Maintaining the Charas/Olvera-Hernandez combination would have been obvious as Charas’s service monitor agent satisfying claim 3 would not have been disrupted. *See* Claim 1, §VII.A.1., *supra*. EX1012, ¶184.

4. **Claim 4: “The wireless end-user device of claim 3, wherein for at least one of the first and second service plans, the wireless end-user device synchronizes a local service usage count with a network-based service count.”**

Claim 4 is obvious over Charas alone or in combination with Olvera-Hernandez. *See* §VII.A.3., *supra*. Charas discloses that, for at least one of its first and second service plans (i.e., subscriptions), its wireless end-user device (i.e., “terminal”) synchronizes a local service usage count (i.e., “accounting information

570” generated by the LPEP) with a network-based service count (i.e., “accounting information generated in the SMP 100”). EX1004, ¶¶[0047], [0049]. EX1012, ¶¶185-186.

The “accounting information 570” generated by the LPEP of Charas includes an elapsed time a service was utilized (i.e., local service usage count). Charas’s LPEP synchronizes its local service usage count with a network-based service count generated by “a server cluster called Secure Mobile Portal (SMP).” *See* §VII.A.3., *supra*; EX1004, ¶¶[0039], [0047], [0049]. When the SMP receives the accounting information from the LPEP, it “compares it with the accounting information generated in the SMP 100 and sends a positive or negative accounting confirmation 575 back to the LPEP 110,” thus synchronizing the local and network-based service counts. EX1004, ¶[0049]; *see also id.* ¶[0047] (“SMP 100 replies in agreement or disagreement, i.e. compare the accounting log in the SMP 100 with the one generated in the LPEP 110.”). EX1012, ¶¶187-189.

Maintaining the Charas/Olvera-Hernandez combination would have been obvious as Charas’s service count synchronization functionality satisfying claim 4 would not have been disrupted. *See* Claims 1 and 3, §VII.A.1., VII.A.3., *supra*. EX1012, ¶190.

5. **Claim 8: “The wireless end-user device of claim 1, wherein the at least one adaptive service policy control agent applies network service policies from a superset profile that provides capabilities from each of the first and second service profiles.”**

Claim 8 is obvious over Charas alone or in combination with Olvera-Hernandez. *See* §VII.A.1., *supra*. Charas’s adaptive service policy control agent applies network service policies (e.g., rights, obligations, etc.) from a superset profile (i.e., “policy sub-domain”) that provides capabilities from first and second service profiles (i.e., “policy blocks”). *See* §VII.A.1.e., *supra*. EX1004, ¶[0060]. EX1012, ¶¶191-192.

Charas discloses Fig. 7 policy “sub-domains” each containing “multiple policy blocks 625” (e.g., first and second service profiles) having “specific relationships” between a user and service providers. EX1004, ¶[0060], Fig. 7.

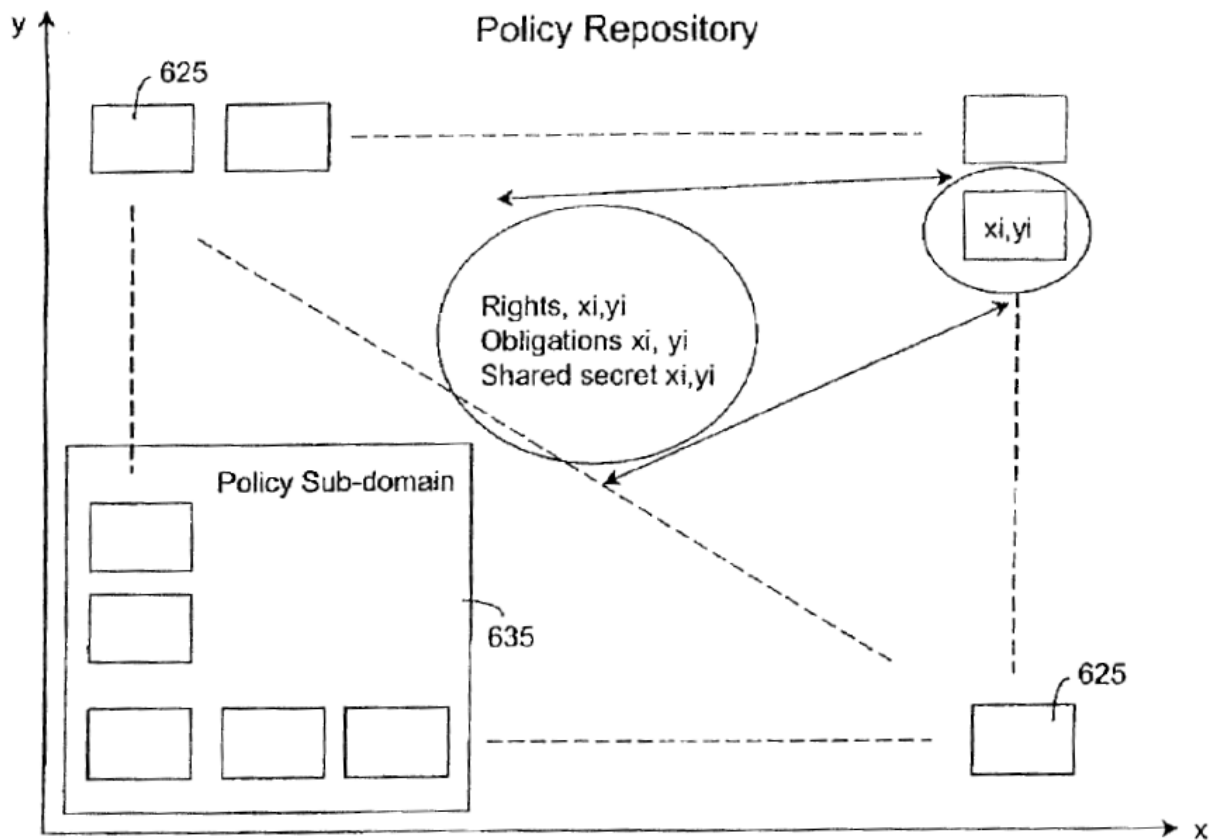


Fig. 7

EX1004, Fig. 7

EX1012, ¶193.

Each sub-domain constitutes a superset profile that provides capabilities from each of its constituent policy blocks (i.e., service profiles). A sub-domain is a “reserved domain space for a particular application” that groups relevant policy blocks for the application thereby providing combined capabilities from those constituent policy blocks. EX1004, ¶[0060]; EX1012, ¶194.

Charas’s policy enforcement engine (i.e., adaptive service policy control agent) enforces policies drawn from the policy repository including from sub-

domains for certain applications. EX1004, ¶[0059]-[0060]. When the user requests a service, “the policy enforcement engine 610 then collects data from the policy repository 620 and the access selection function 690 to set up a channel that complies with the agreed parameters and the requested service.” EX1004, ¶[0064]. Charas’s policy enforcement engine can concurrently enforce policies from first and second policy blocks (i.e., service profiles) because Charas’s terminal supports several simultaneous, independent data flows (e.g., VoIP via W-CDMA and multimedia via W-LAN). EX1004, ¶[0051]. EX1012, ¶¶195-196.

Maintaining the Charas/Olvera-Hernandez combination would have been obvious as Charas’s adaptive service policy control agent and superset profiles satisfying claim 8 would not have been disrupted. *See* Claim 1, §VII.A.1., *supra*. EX1012, ¶197.

6. **Claim 9: “The wireless end-user device of claim 1, wherein the at least one adaptive service policy control agent detects network connection changes from the first wireless network to the second wireless network, and in response enforces the second set of network service policies.”**

Claim 9 is anticipated and/or obvious over Charas alone and/or in view of Olvera-Hernandez. *See* §VII.A.1., *supra*. Charas’s adaptive service policy control agent (i.e., “policy enforcement engine 610”) detects network connection changes from the first wireless network (e.g., “W-CDMA network”) to the second wireless network (e.g., “GPRS” network), and in response enforces the second set of network

service policies (i.e., network service policies of Charas's second "policy block").
See supra §VII.A.1.e, EX1004, ¶¶[0051], [0055]. EX1012, ¶¶198-199.

Charas expressly discloses that the second wireless network has a corresponding set of network policies that are enforced in response to a network connection change. Charas's first and second service profiles (i.e., first and second "policy blocks") possess hierarchical dependencies to access networks such that a network connection change to a second wireless network would require service policies of the second service profile to be enforced. EX1004, ¶[0055]. EX1012, ¶200.

Charas discloses that "the terminal [can] hand over a communication session from one communications network to another, by re-routing the data flow from one modem port to another." EX1004, ¶[0051]. Charas's policy enforcement engine (i.e., adaptive service policy control agent) is responsible for setting up a channel and enforcing the policies of the requested web-service. *See* §VII.A.1.e., *supra*. EX1012, ¶¶201-202.

Charas alone or in combination with Olvera-Hernandez discloses an adaptive service policy control agent detecting network connection changes from the first wireless network to the second wireless network, and in response enforcing the second set of network service policies. A POSITA would have understood, and it would have been obvious, that Charas's policy enforcement engine would have

known what access network(s) are connected in order to enforce policies that depend on such connection. The policy enforcement engine would thereby detect network connection changes from the first network to the second network and enforce policies based on that change. This detection of connection changes is enabled by the access selection function, layer 2 IP switch, and the layer 3 IP router coupled to the policy enforcement engine. EX1004, Fig. 6 (*see* §V.C.1., *supra.*); EX1012, ¶¶203-205.

A POSITA would have been motivated to accommodate Olvera-Hernandez's multimode modem as it can similarly route traffic flows between "various technology specific modems" in response to network changes. *See* §VII.A.1.d., *supra.* *See also e.g.*, EX1005, ¶¶[0024], [0027] (Olvera-Hernandez's "MSCF 547" manages "transitions among various mobility services" of different "interface technologies" via an "access switch 540"). This modification would have predictably yielded a device configured to support and detect network changes because Charas's interchangeable modules and Olvera-Hernandez's multimode modem are enabled with switching functionality. EX1004, ¶[0051], EX1005, ¶[0024], Consolidating/replacing Charas's interchangeable modules into/with a multimode modem as taught by Olvera-Hernandez would have been obvious. *See* Claim 1, §VII.A.1., *supra.* EX1012, ¶¶206-208.

7. **Claim 10: “The wireless end-user device of claim 1, wherein the connection manager further comprises a modem selection and control layer that routes certain types of data traffic to the first wireless network and other types of data traffic to the second wireless network.”**

Claim 10 is anticipated and/or obvious over Charas alone and/or in view of Olvera-Hernandez. *See* §VII.A.1., *supra*. Charas’s connection manager includes a modem selection and control layer (i.e., “a layer 2 IP switch 630 and a layer 3 IP router 640”) that routes certain types of data traffic (i.e., information flows) to a first wireless network (e.g., “W-CDMA network”) and other types of data traffic to a second wireless network (e.g., “GPRS network”). *See* §VII.A.1.d., *supra*, EX1004, ¶[0051]. EX1012, ¶¶209-210.

Charas’s “layer 2 IP switch 630 and a layer 3 IP router 640... enable[] the user 660 the possibility to have several information flows ... active at the same time. For example [] a voice over IP data flow [can] be maintained through a W-CDMA network, at the same time as a multimedia flow is maintained through a W-LAN network.” EX1004, ¶[0051]. A POSITA would have understood that Charas’s disclosure is not limited to routing between W-LAN and W-CDMA networks because Charas broadly teaches routing flows between any available networks. Network connections are established by selecting among Charas’s “interchangeable modules (modems) for different access standards such as W-CDMA, EDGE, CDMA 2000, W-LAN etc.” Olvera-Hernandez’s multimode modem similarly groups

multiple technology specific modems (e.g., LTE modem 516, UTRAN modem 518, IEEE 802 modem 520, etc.). EX1004, ¶¶[0041], EX1005, ¶[0024]. Charas's access selection function, layer 2 IP switch, and layer 3 IP router, constitute a connection manager including a modem selection and control layer that routes certain types of data traffic to the first wireless network and other types of data traffic to the second wireless network. EX1012, ¶¶211-215.

The Charas/Olvera-Hernandez combination would not have disrupted Charas's disclosure of a connection manager comprising a modem selection and control layer routing certain types of data traffic to the first wireless network and other types of data traffic to the second wireless network. Olvera-Hernandez discloses as a connection manager a "mobility selection and control function (MSCF) 547" and various switches (e.g., "voice switch 530", "data switch 535", "access switch 540"). EX1005, ¶¶[0024-25], Fig. 5. *See* §VII.A.1.d., *supra*. Just as the claim 10 modem selection and control layer routes "certain network traffic" to a first network and "some or all of the data traffic" to another network, Olvera-Hernandez's MCSF "manag[es] transitions among various mobility services in response to changing scenarios (for example, changing from GAN (Generic Access Network) to IMS (Internet protocol (IP) Multimedia subsystem...)" by dynamically selecting "air interface technologies and associated access networks" that support selected mobility services. EX1001, 94:58-95:9, EX1005, ¶¶[0027], [0030]-[0031].

A POSITA would have understood that Olvera-Hernandez's mobility services (e.g., "session initiation protocol (SIP) 557, IMS 559, voice call continuity (VCC) 561, as well as other services including Mobile IP (MIP)/proxy MIP (PMIP) 563, and GAN 565") generate unique traffic flows. Olvera-Hernandez's MSCF therefore routes certain data traffic (i.e., of a first mobility service or collection of mobility services) to a first wireless network and other data traffic (i.e., of a second mobility service or collection of mobility services) to a second wireless network. EX1012, ¶216-220.

Maintaining the Charas/Olvera-Hernandez combination would have been obvious as the connection manager functionality of Charas satisfying claim 10 would not have been disrupted. *See* Claim 1, §VII.A.1., *supra*. EX1012, ¶221.

8. Claim 12: "The wireless end-user device of claim 1, the connection manager configured to prompt the WWAN modem to connect to a selected access network and send credentials associated with the selected one of the first and second service profiles to the selected access network."

Claim 12 is anticipated and/or obvious over Charas alone and/or in view of Olvera-Hernandez. *See* §VII.A.1., *supra*. Charas's connection manager (i.e., "access selection function 690", "layer 2 IP switch 630" and "layer 3 IP router 640," *see* VII.A.1.d., *supra*) is configured to prompt the WWAN modem to connect to a selected (i.e., "chosen") access network and send credentials associated with the selected one of the first and second service profiles (i.e., "policy blocks") to the

selected access network. *See* §VII.A.1.c., *supra*, EX1004, ¶[0052]. EX1012, ¶¶222-223.

The “access selection function 690” of Charas’s connection manager “is responsible for requesting access and *presenting credentials to the desired access network depending on the service requested* from the service layers and also for *preparing to interconnect with the chosen access network*.”. EX1004, ¶[0052] (emphasis added). Access to the “chosen access network” networks is facilitated through Charas’s interchangeable modules. EX1004, ¶¶[0041], [0053]; *see* §VII.A.1.a., *supra*. EX1012, ¶¶224-225.

To the extent it is argued that Charas’s multimode modem capability does not constitute a single modem, Olvera-Hernandez discloses a single multimode WWAN modem. *See* §VII.A.1.a., *supra*. A POSITA would have been motivated to use a multimode modem as disclosed by Olvera-Hernandez to connect to an access network selected by its “MSCF 547” just as Charas’s interchangeable modules connect to an access network selected by its “access selection function 690.” EX1004, ¶[0052], EX1005, ¶[0024]. *See* §VII.A.1.d., *supra*. EX1012, ¶¶226-227.

Because Olvera-Hernandez’s multimode modem connects to an access network selected by a connection manager (i.e., MSCF 547 and various switches), consolidating/replacing Charas’s interchangeable modules into/with a multimode modem as taught by Olvera-Hernandez would not have disrupted Charas’s disclosed

functionality and would have been obvious. *See* Claim 1, §VII.A.1., *supra*. EX1012, ¶228.

Each of Charas’s service profiles (i.e., “policy blocks”) defines a relationship between a subscriber and a service provider (i.e., service plan or “subscription”). EX1004, ¶[0057]. These profiles include device credentials (i.e., “shared secrets”) which encrypt each packet sent “between the service provider and the service buyer” (i.e., “subscriber”), the service provider operating the selected access network (i.e., “chosen access network”). *See* §VII.A.2., *supra*, EX1004, ¶¶[0039], [0051]; *see also* EX1004, ¶[0039] (“each packet received by the SMP 100 will be seen as de facto authentication of the service buyer or subscriber by the service provider.”). Charas’s access selection function is therefore responsible for prompting a WWAN modem to connect to a selected access network and for sending credentials associated with the selected one of a first and second service profiles to a selected access network. EX1012, ¶¶229-230.

B. Claim 5 is Obvious over Charas alone or in Combination with Olvera-Hernandez in view of Mottes (Ground 2)

- 1. Claim 5: “The wireless end-user device of claim 1, wherein the first service plan is associated with a central provider that operates a WWAN access network, and the second service plan is associated with a virtual network operator.”**

Claim 5 is obvious over Charas alone or in combination with Olvera-Hernandez in view of Mottes. *See* §VII.A.1., *supra*. Charas discloses first and second

service plans (i.e., subscriptions) that are associated with access providers operating WWAN access networks. *See* §VII.A.1.b., *supra*; *see also* EX1004, ¶[0054]. Charas discloses “subscriber A [that] has a private subscription with provider X for voice and web browsing,” maintained through a W-CDMA network. EX1004, ¶¶[0051], [0056]. Although Charas does not expressly distinguish between central providers operating physical access networks and virtual network operators providing services over another operator’s infrastructure, virtual network operators were well-known in the art as demonstrated by Mottes. EX1012, ¶¶231-233.

Mottes discloses a system enabling an end user “to use and or subscribe to several service providers and or Mobile Virtual Network Operators (MVNOs)” from a single device. EX1007, Abstract. Service providers can be MVNOs or mobile network operators (MNOs). EX1007, ¶[0007]. Mottes defines an MVNO as “an organization that offers mobile subscription and call services to customers but does not have an allocation of spectrum,” and distinguishes MVNOs from non-virtual MNOs . EX1007, ¶¶[0008], [0040]. An MNO therefore corresponds to the claimed “central provider that operates a WWAN access network.” EX1012, ¶¶234-235.

Mottes discloses that a single end user can maintain relationships with both types of providers (MNOs and MVNOs) simultaneously, enabling them “to use and or subscribe to several service providers and or Mobile Virtual Network Operators (MVNOs)” from a single device. EX1007, Abstract. A POSITA reading Mottes

would have understood it was well-known for the wireless ecosystem to include both central providers operating physical WWAN access networks (MNOs) and virtual network operators leveraging that infrastructure (MVNOs), and for a user to have relationships (e.g., subscriptions) to both. EX1012, ¶¶236-237.

It would have been obvious to accommodate one virtual network operator within Charas's policy repository 620 and this would have predictably yielded a first service plan associated with a central provider operating a WWAN access network (an MNO) and a second service plan associated with a virtual network operator (an MVNO). Charas's policy repository already supports multiple, discrete policy blocks for different provider relationships, each with its own rights, obligations, and credentials. EX1004, ¶[0054]. Adding an MVNO policy block alongside an existing MNO policy block would have been a natural, predictable extension of Charas's existing architecture based on the existing access networks and providers at the time of Charas. A POSITA would have combined Charas and Mottes to include a virtual network operator, thereby expanding service provider options. EX1007, ¶¶[0002], [0009-11]. EX1012, ¶¶238-241.

The combination of Charas, Olvera-Hernandez, and Mottes would have been obvious as Mottes's central provider and virtual network operator relied upon for claim 5 would not have disrupted the Charas/Olvera-Hernandez combination. *See* Claim 1, §VII.A.1., *supra*. EX1012, ¶242.

C. Claims 6 and 7 are Obvious over Charas alone or in Combination with Olvera-Hernandez in view of Spencer (Ground 3)

- 1. Claim 6: “The wireless end-user device of claim 1, further comprising a user service interface to allow a user to make a user selection between the first and second service profiles, the connection manager to, responsive to the user selection, select an access network connection for the WWAN modem.”**

Claim 6 is obvious over Charas alone or in combination with Olvera-Hernandez in view of Spencer. *See* §VII.A.1., *supra*. Charas’s user service interface is a “user interface and application programming interfaces (API’s)” for user-initiated services. EX1004, ¶[0050]. *See also, e.g.*, EX1004, ¶[0064] (the user “wants to initiate a web-service”), ¶[0068] (“user wishes to make a call”), Fig. 5 (showing “Subscriber” sending “service request (510)” to LPEP). Charas does not disclose details about how these service requests are made, e.g., the user interface enables service profile selection. A POSITA would therefore have looked to existing solutions for user-initiated services in mobile devices, such as Spencer’s disclosed teachings of wireless service access in the technical field of Charas. *See* EX1008, Abstract; EX1004, Abstract; EX1012, ¶¶243-246.

Spencer discloses as a user service interface a “user interface (UI)...send[ing] a web page displaying available service options” from which “[t]he user selects the required services.” EX1008, ¶[0166]. An “Access Management Module determines what service profile the user has access to through the current remote device” and “sends the available service options to the remote device through an appropriate UI.”

EX1008, ¶[0165]. The user is therefore presented with service profiles and selects between them. *See* EX1008, ¶[0166] (service profile selected after cross-referencing user selection to profiles in database), EX1012, ¶247.

Charas and Spencer both define the parameters and permissions governing a user's access to network services: Spencer's service profiles define "allowed or restricted services, resources or applications to be provided" (EX1008, ¶[0045]), and Charas's policy blocks similarly define "rights" and "obligations" associated with each service provider relationship (EX1004, ¶[0056]). Spencer teaches configuring a user interface, such as that of Charas, to allow a user to make a selection between first and second service profiles (i.e., Charas's policy blocks). The "service profile rules are sent to the Access Management Module (step 534)" and used to "establish a connection to the network 508 (step 548)." *Id.*, EX1008, Fig. 5. Charas's access selection function 690 responds to a user-selected policy block (e.g., via a user interface as taught by Spencer) by selecting the appropriate access network and interconnecting with the chosen network. EX1004, ¶[0052]. EX1012, ¶¶248-250.

Charas's connection manager includes an "access selection function 690 [] responsible for...interconnect[ing] with [a] chosen access network" via interchangeable modules supporting multiple WWAN network technologies (e.g., W-CDMA, EDGE, etc.). EX1004, ¶[0052]; *see* §VII.A.1.d., *supra*. This access network selection within Charas would have been responsive to the user's service

profile selection, as the access selection function selects the appropriate network based on the service requested by the subscriber. EX1004, ¶[0043]. EX1012, ¶¶251-252.

To the extent it is argued that Charas's multimode modem capability does not constitute a single modem, Olvera-Hernandez discloses a single multimode WWAN modem. *See* §VII.A.1.a., *supra*. Olvera-Hernandez also discloses a connection manager that selects an access network for its multimode modem. *See* §VII.A.1.d., *supra*. EX1012, ¶¶253-254.

Because Olvera-Hernandez's multimode modem can also connect to an access network selected by a connection manager (i.e., MSCF 547 and various switches), consolidating/replacing Charas's interchangeable modules into/with a multimode modem as taught by Olvera-Hernandez would not have disrupted Charas's disclosed functionality. *See* §VII.A.1.a., *supra*. EX1012, ¶255.

A POSITA would have been motivated to combine Charas's access selection function and Spencer's service profile selection to provide a user interface via the applications interface 650 that would have facilitated Charas's service initiation. Both Charas and Spencer are directed to managing user access to wireless network services through the application of service profiles. Spencer teaches that users benefit from the ability to select among service offerings, disclosing that "a user can

select and pre-pay for a service profile based on price and desired functionality.” EX1008, ¶[0049]. EX1012, ¶¶256-258.

A POSITA would have recognized that incorporating Spencer’s technique of presenting available service profiles to the user for selection into Charas’s existing user interface would have improved user engagement and ease-of-use. EX1012, ¶259. Charas’s terminal architecture separates the service part (containing the user interface and API’s) from the access part (containing the modem modules) and the control part (containing the policy enforcement engine, policy repository, and access selection function), making it architecturally amenable to adding an explicit user selection step before the policy enforcement engine and access selection function respond by selecting the appropriate access network. EX1012, ¶260.

The combination of Spencer’s user-interface in Charas’s system involves simply applying a user-driven service profile selection through a UI as taught by Spencer to Charas’s multi-access terminal with its existing user interface to yield the predictable result of allowing a user to select between multiple service profiles through the user interface. The terminal’s access selection function thereafter selects the appropriate access network connection. EX1012, ¶261.

The combination of Charas, Olvera-Hernandez, and Spencer would have been obvious as Charas’s connection manager functionality and Spencer’s user service

interface relied upon for claim 6 would not have disrupted the Charas/Olvera-Hernandez combination. *See* Claim 1, §VII.A.1., *supra*. EX1012, ¶262.

2. Claim 7: “The wireless end-user device of claim 1, further comprising a service notification and billing interface to display service usage options for each of the first and second service profiles.”

Claim 7 is obvious over Charas alone or in combination with Olvera-Hernandez in view of Spencer. *See* §VII.A.1., *supra*. Charas discloses a “user interface and application programming interfaces (API’s) for the services.” EX1004, ¶[0050]. Charas discloses multiple (e.g., first and second) service profiles defining a user’s relationship with a service provider, which charges the user via an “invoice.” *Id.*, ¶¶[0014], [0056]-[0057]. Charas also discloses accounting/billing functionality. *Id.*, ¶[0047]. Charas, however, does not explicitly describe how the user is informed of, or consents to, charges. A POSITA would have used known prior art techniques to present charging information to users in a multi-network, multi-profile mobile device context, such as those disclosed by Spencer. EX1012, ¶¶263-267.

Spencer discloses as a “service notification and billing interface” a “User Interface (UI)” responsible for “displaying available *service options*...to the user so the user can select the required services” and “payment options.” EX1008, ¶[0166] (emphasis added). Spencer’s UI displays billing information and service usage options in the form of “service options” and the corresponding “payment options.” *Id.* Spencer indicates that these service options can be selected in order to “pre-pay”

for or to “upgrade a service profile.” *Id.*, ¶[0049]; *see id.*, ¶[0096] (“when a user of a given remote device having restrictive access ... may be redirected to an interactive interface providing the user the option of upgrading or enhancing their service profile, for example, for an additional fee”). The service notification and billing interface of the ’055 Patent likewise allows “service plan options/changes ... [to be] configured/updated” and “provides options for automatic pre-buy.” EX1001, 66:9-25. EX1012, ¶¶268-269.

Spencer indicates that service options correspond to a “user’s current service profile” representing a single service profile from among multiple “service profiles stored in a knowledge base” or “established for the [user’s] account” (i.e., first and second service profiles in a secure memory). EX1008, ¶¶[0096]-[0097], [0166]-[0067]. Spencer’s service profiles constitute “subscription packages that enable subscribed users access to certain network-based functions and services.” *Id.*, ¶[0091]. Charas’s policy blocks and Spencer’s service profiles define distinct relationships with different service providers, each one involving its own rights, obligations, and charges. EX1004, ¶[0056]. Because Spencer’s UI displays service options for a current service profile selected from a number of different packages, a POSITA would have understood that the UI would display service options for each of Charas’s profiles (including the first and second service profiles) depending on which was selected. *Id.* Spencer’s UI therefore constitutes a service notification and

billing interface to display service usage options for each of the first and second service profiles. EX1012, ¶¶270-274.

Charas alone or in combination with Olvera-Hernandez in view of Spencer discloses a service notification and billing interface to display service usage options for each of the first and second service profiles. A POSITA would have been motivated to implement Spencer's UI on Charas's terminal as the combination would have predictably yielded a simple, transparent interface that would promote customer satisfaction and ease-of-use. Spencer's UI gives the user an opportunity to pre-pay for services or to upgrade or enhance an existing service profile upfront for an additional fee before charges are incurred. This protects the user from unintended charges and would have been desirable in Charas's system where the user has relationships with multiple service providers. EX1008, ¶¶[0049], [0096]. EX1012, ¶¶275-277.

The combination would have been predictable/straightforward. Both references involve packaging and selling network services within subscription-based profiles. Implementing service charging in Charas's existing UI/API layer would have involved a well-known UI modification. The ability to notify and bill users for services incurred under their given subscriber profile was within the knowledge/skill of a POSITA. *See* Brisebois, EX1017, ¶[0076]. EX1012, ¶¶278-279.

The combination of Charas, Olvera-Hernandez, and Spencer would have been obvious as Spencer's service notification and billing interface relied upon for claim 7 would not have disrupted the Charas/Olvera-Hernandez combination. *See* Claim 1, §VII.A.1., *supra*. EX1012, ¶280.

D. Claim 11 is Obvious over Charas alone or in Combination with Olvera-Hernandez in view of Phillips (Ground 4)

- 1. Claim 11: “The wireless end-user device of claim 1, further comprising a Subscriber Identity Module (SIM), the adaptive service policy control agent located at least in part on the SIM.”**

Claim 11 is obvious over Charas alone or in combination with Olvera-Hernandez in view of Phillips. *See* §VII.A.1., *supra*. The parties have proposed constructions of the term “Subscriber Identity Module” in the related litigation. Under any proposed construction, the prior art cited herein discloses embodiments that align with embodiments of the '055 Patent which are encompassed by claim 11. EX1012, ¶¶281-282.

Charas discloses an adaptive service policy control agent (i.e., policy enforcement engine 610). *See* §VII.A.1.e., *supra*; EX1004, ¶[0014]. While Charas discloses storing its policy enforcement engine and policy repository on a smart card (*see* EX1004, ¶[0059]), Charas does not expressly disclose that the smart card is a SIM. EX1012, ¶¶283-284.

However, Phillips discloses the well-known use of a SIM/smart card for storing mobile device policy enforcement functions. *See, e.g.*, EX1009, ¶[0006] (a “Subscriber Identity Module (SIM)... is one type of ‘smart card’ ... connected to the mobile station for customization and for identifying the end user.”), ¶¶[0023]-[0024]. Policy enforcement functions disclosed by Phillips (e.g., user authentication/identification) include the exact functions performed by the adaptive service policy control agent of the ’055 Patent (*see* EX1001, 8:49-55) and Charas’s policy enforcement engine (*see* §VII.A.1.e., *supra.*). *See also* EX1004, ¶¶[0014], [0059]. *See also* EX1018, §§7.1, 7.2, and 9.2.16; EX1019, §§7.1, 7.2, and 9.2.16. Under any construction of “Subscriber Identity Module,” locating Charas’s policy enforcement engine at least in part on Phillips’s SIM satisfies claim 11. EX1012, ¶¶285-286.

The adaptive service policy control agent of the ’055 Patent enforces “access control settings, ... authentication settings, and admission control settings.” EX1001, 8:49-55 (emphasis added). Phillips’s SIM uses key generating and authentication algorithms stored on the SIM to implement user authentication/identification procedures, just like the adaptive service policy control agent of the ’055 Patent. EX1009, ¶[0024]. The SIM is used for subscriber-specific policy/profile storage and for “identifying [an] end user.” *Id.*, ¶[0006]. Phillips discloses that to perform user authentication, the SIM “stores” authentication

settings including “(3) a ciphering key generating algorithm (A8)—with Ki and RAND it generates a 64-bit key (Kc); [and] (4) an authentication algorithm (A3)—with Ki and RAND it generates a 32-bit signed response (SRED).” *Id.*, ¶[0024]; *see* EX1018, §§7.1, 7.2, and 9.2.16; EX1019, §§7.1, 7.2, and 9.2.16. EX1012, ¶¶287-289.

Phillips also teaches implementing a SIM in accordance with the “3GPP 51.001 Specifications of the SIM-ME interface R4 (v4.2.0 or later)” per Petitioner/Defendant’s construction proposed in related litigation.³ EX1009, ¶[0026]. Phillips implements certain elements of its SIM in accordance with 3GPP (EX1018, EX1019); *see e.g.*, the EONS procedure and the other functionalities of its SIM. *Id.*, [0024], [0026]. 3GPP also teaches storing elements associated with user authentication/identification on a SIM. EX1018, §§7.1, 7.2, 9.2.16; EX1019 §§7.1, 7.2, and 9.2.16. It would have been obvious in view of Phillips to implement user authentication/identification on a SIM in accordance with 3GPP. EX1012, ¶¶290-292.

³ A POSITA in reading Phillips would have recognized that the citation to “3GPP 51.001 Specifications” was intended to be a reference to the 3GPP 51.011 specification which includes EX1018 and EX1019 discussed herein. EX1020, ¶¶77-81.

A POSITA would have been motivated to implement at least a portion of Charas’s policy enforcement engine (i.e., adaptive service policy control agent) on Phillips’s SIM to leverage the SIM’s portability and built-in authentication functionality. A SIM card provides a user with secure access to their subscribed services from multiple wireless devices. *See* EX1009, ¶[0023] (“An advantage of using SIM 140 is that end users are not necessarily bound by any single physical wireless device” and a SIM card “personalizes a wireless device terminal.”). *See also* Phillips whose SIM discloses additional identical functionality to that performed by Charas’s policy enforcement engine and the adaptive service policy control agent of the ’055 Patent. *See* EX1001, 50:38-41 (“the policy control agent ... performs an access network selection algorithm to determine which access network to connect to ***based on connection options ... network preference ...*** and/or any other criteria”); EX1004, ¶[0052] “[t]he ***access selection function*** is responsible for requesting access and presenting credentials to the ***desired access network*** depending on the service requested”); EX1009, ¶[0024] (“A typical SIM 140 stores ... a preferred network list,”); *id.*, ¶[0026] (Phillips’s SIM includes files for “Enhanced Operator Named String (EONS) ... for automatic network selection”). EX1012, ¶¶293-294.

Implementing at least part of Charas’s policy enforcement engine on a removable SIM would have been a straightforward application of known techniques (implementing policy enforcement logic on a SIM smart card capable of storing files

and hosting applications as Charas contemplates) to yield the predictable result of portable, secure, subscriber-specific policy enforcement across devices. Storing service profiles and their subscriber-specific policies and network preferences on a portable SIM was within the skill and knowledge of a POSITA. *See* EX1017, ¶[0072] (“memory 675 can retain subscriber-specific network selection profile(s) 679 and display profile(s) 677 ... memory 675 is at least in part a subscriber-specific removable computer-readable storage medium such as for example a SIM.”). EX1012, ¶¶295-296.

The combination of Charas, Olvera-Hernandez, and Phillips would have been obvious as Phillips’s SIM relied upon for claim 11 would not have disrupted the Charas/Olvera-Hernandez combination. *See* Claim 1, §VII.A.1., *supra*. EX1012, ¶297.

E. Claim 13 is Obvious over Charas alone or in Combination with Olvera-Hernandez in view of Brown (Ground 5)

- 1. Claim 13: “The wireless end-user device of claim 2, configured to, when the second service plan is inactive, suspend the second device credentials, and when the second service plan is reactivated, reactivate the second device credentials”**

Claim 13 is obvious over Charas alone or in combination with Olvera-Hernandez in view of Brown. *See* §VII.A.2., *supra*. Charas’s wireless end-user device (i.e., “terminal”) is configured to identify when a service plan is inactive (i.e., when a “subscriber does not pay the invoice for a particular service”). Charas also

discloses multiple device credentials (i.e., “shared secrets”) used to authorize a subscriber (i.e., their subscription or “service plan”) to a given service. EX1004, ¶¶[0046], [0048]; *see* §VII.A.2., *supra*. Charas does not disclose details of how a service is barred or how credentials are suspended. A POSITA would have looked to the prior art for details of barring services such as Brown. EX1012, ¶¶298-300.

Brown’s “subscription parameters” (IMSI, ICCID, and other parameters needed for operation in a given network/region) “saved in a portion of [a] SIM memory” can be selectively “activated, deactivated and reactivated as many times as desired.” EX1010, ¶¶[0032]-[0033]; *see also id.* ¶¶[0008], [0015], [0018]. These subscription parameters constitute “device credentials” because they are (1) stored on Brown’s SIM (and are thus “activated, deactivated and reactivated” on the device itself) and (2) represent information the network uses to admit the device and associate it with a desired service (e.g., “identity of the user and/or account, and the network in which the user account is activated”). EX1010, ¶¶[0005], [0032]-[0033]; *cf.* EX1001, 19:38-39. Brown therefore discloses suspending credentials associated with a given service profile (i.e., the shared secrets of an inactive subscription in Charas). Brown also discloses “reactivat[ing]” credentials associated with a given service profile. EX1010, ¶[0033]. Just as Charas discloses deactivating an inactive subscription, Brown reactivates credentials, for example, when a SIM travels to a “market[] or region[] in which a service provider provides service” or to a “network

in which the user account [i.e., subscription] is activated.” EX1010, ¶¶[0005], [0033]. EX1012, ¶¶301-304.

A POSITA would have been motivated to implement Brown’s method of deactivating and reactivating subscription parameters (e.g., device credentials) with Charas’s subscription identification keys. Charas’s architecture involves multiple service provider relationships, each with its own credentials. EX1004, ¶[0057]. Charas expressly discloses barring service when a user fails to pay, and Brown provides an identical mechanism. Suspending credentials associated with a barred service would prevent the policy enforcement engine from attempting to use inactive or unauthorized credentials, improving security. This reactivation capability also allows a user to deactivate and reactivate service plans when roaming between different markets or regions, as taught in Brown. EX1010, ¶¶[0008], [0015], [0018]-[0020]. The combination would have yielded the predictable result of a device that efficiently manages active and inactive service provider relationships at the credential level, allowing an SMP to deactivate unpaid plans, and allowing a user to reactivate, or switch between service plans. EX1012, ¶¶305-307.

The combination of Charas, Olvera-Hernandez, and Brown would have been obvious as Brown’s credential suspension/activation functionality relied upon for claim 13 would not have disrupted the Charas/Olvera-Hernandez combination. *See* Claims 1 and 2, §VII.A.1., VII.A.2., *supra*. EX1012, ¶308.

VIII. OTHER CONSIDERATIONS

Petitioner is not aware of any secondary considerations evidence bearing any nexus to the purported claimed invention. Any purported evidence of secondary considerations that Patent Owner may present in this proceeding would be insufficient to overcome the strong evidence of obviousness of the Challenged Claims. EX1012, ¶¶309-311.

IX. CONCLUSION

Petitioner has shown a reasonable likelihood of success. Therefore, this Petition should be granted and the Board should institute trial.

Date: August 27, 2026

Respectfully submitted,

/Patrick C. Keane/

Patrick C. Keane, Esq.

Registration No. 32,858

BUCHANAN INGERSOLL & ROONEY PC

1700 K Street, N.W., Suite 300

Washington, DC 20006

Telephone (703) 838-6522

Facsimile (202) 452-7989

patrick.keane@bipc.com

Counsel for Petitioner

APPENDIX A - LIST OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 11,096,055, issued August 17, 2021 to G. Raleigh (“’055 Patent”)
1002	File History of U.S. Patent Application No. 16/421,121 through September 22, 2025
1003	U.S. Provisional Application No. 61/206,354, filed January 28, 2009
1004	U.S. Patent Application Publication No. 2002/0056002, published May 9, 2002 to P. Charas (“Charas”)
1005	U.S. Patent Application Publication No. 2009/0170555, published July 2, 2009 to U. Olvera-Hernandez et al. (“Olvera-Hernandez”)
1006	U.S. Patent No. 10,127,530, issued November 13, 2018 to S. Swanburg et al. (“Swanburg”)
1007	U.S. Patent Application Publication No. 2004/0162058, published August 19, 2004 to D. Mottes (“Mottes”)
1008	US Patent Application Publication No. 2010/0107225, published April 29, 2010 to R. Spencer et al. (“Spencer”)
1009	U.S. Patent Application Publication No. 2008/0096559, published April 24, 2008 to C. Phillips et al. (“Phillips”)
1010	U.S. Patent Application Publication No. 2005/0164737, published July 28, 2005 to J. Brown (“Brown”)
1011	U.S. Patent Application Publication No. 2002/0116545, published August 22, 2002 to D. Mandato et al. (“Mandato”)
1012	Declaration of David Williams
1013	<i>Curriculum Vitae</i> of David Williams

Petition for *Inter Partes* Review of U.S. Patent No. 11,096,055

Exhibit No.	Description
1014	European Patent Application Publication No. 3,661,242, published June 3, 2020 (“European counterpart”)
1015	File History of European counterpart
1016	European Patent Application Publication No. 1,117,265, published July 18, 2001 to Charas (“Charas”)
1017	U.S. Patent Application Publication No. 2010/0099405, published April 22, 2010 to A. Brisebois et al. (“Brisebois”)
1018	Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (3GPP TS 51.011 version 4.10.0 Release 4)
1019	Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (3GPP TS 51.011 version 4.2.0 Release 4)
1020	Declaration of Friedhelm Rodermund
1021	<i>Curriculum Vitae</i> of Friedhelm Rodermund
1022	Defendant Google LLC’s Opening Claim Construction Brief, filed May 13, 2026 in <i>Headwater Research LLC v. Google LLC</i> , Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1023	Plaintiff Headwater Research LLC’s Responsive Claim Construction Brief, filed June 8, 2026 in <i>Headwater Research LLC v. Google LLC</i> , Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1024	Defendant Google LLC’s Reply to Plaintiff’s Responsive Claim Construction Brief, filed June 22, 2026 in <i>Headwater Research LLC v. Google LLC</i> , Civ. Action No. 7:25-cv-00369 (W.D. Tex.)

Petition for *Inter Partes* Review of U.S. Patent No. 11,096,055

Exhibit No.	Description
1025	Plaintiff Headwater Research LLC’s Sur-Reply to Defendant’s Reply to Plaintiff’s Responsive Claim Construction Brief, filed July 7, 2026 in <i>Headwater Research LLC v. Google LLC</i> , Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1026	Joint Claim Construction Statement, filed July 10, 2026 in <i>Headwater Research LLC v. Google LLC</i> , Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1027	European Patent Publication No. EP 1247411 B1 (“Charas EP”)

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. §42.24

The undersigned hereby certifies that the foregoing Petition totals 13,921 words, excluding the parts which are exempted by 37 C.F.R. §42.24(a)(1).

Date: August 27, 2026

/Patrick C. Keane/

Patrick C. Keane, Esq.

Registration No. 32,858

BUCHANAN INGERSOLL & ROONEY PC

1700 K Street, N.W., Suite 300

Washington, DC 20006

Telephone (703) 838-6522

Facsimile (202) 452-7989

patrick.keane@bipc.com

Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 27th day of August, 2026, a true and correct copy of the foregoing **PETITION FOR *INTER PARTES* REVIEW FOR U.S. PATENT NO. 11,096,055 and EXHIBITS 1001-1027 and Petitioner's Power of Attorney** are being served upon the Patent Owner at the following correspondence address of record via FedEx:

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

and courtesy copies are being served on litigation counsel for Patent Owner via electronic mail to:

RUSS AUGUST & KABAT
Marc Fenster (mfenster@raklaw.com)
Reza Mirzaie (rmirzaie@raklaw.com)
Brian Ledahl (bledahl@raklaw.com)
Ben Wang (bwang@raklaw.com)
Dale Chang (dchang@raklaw.com)
Kristopher Davis (kdavis@raklaw.com)
Paul Kroeger (pkroeger@raklaw.com)
James S. Tsuei (jtsuei@raklaw.com)
Philip Wang (pwang@raklaw.com)
James Pickens (jpickens@raklaw.com)
Jason Wietholter (jwietholter@raklaw.com)
Qi (Peter) Tong (ptong@raklaw.com)
Minna Jay (mjay@raklaw.com)

Date: August 27, 2026

/Patrick C. Keane/
Patrick C. Keane, Esq.
Registration No. 32,858
BUCHANAN INGERSOLL & ROONEY PC
1700 K Street, N.W., Suite 300
Washington, DC 20006
Telephone (703) 838-6522
Facsimile (202) 452-7989
patrick.keane@bipc.com
Counsel for Petitioner