

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Gregory G. Raleigh, et al.
U.S. Patent No.: 9,277,445 Attorney Docket No.: 39843-0162IP1
Issue Date: March 1, 2016
Appl. Serial No.: 14/684,033
Filing Date: April 10, 2015
Title: WIRELESS END-USER DEVICE WITH DIFFERENTIAL TRAF-
FIC CONTROL POLICY LIST AND APPLYING FOREGROUND
CLASSIFICATION TO WIRELESS DATA SERVICE

Mail Stop Patent Board

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

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES

PATENT NO. 9,277,445 PURSUANT TO 35 U.S.C. §§ 311–319,

37 C.F.R. § 42

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR	1
A.	Grounds for Standing.....	1
B.	Challenge and Relief Requested.....	1
C.	Claim Construction	2
D.	Level of Ordinary Skill in the Art.....	3
II.	THE '445 PATENT.....	3
A.	Brief Description.....	3
B.	Prosecution History.....	4
III.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	4
A.	[GROUND 1] – Claims 1, 2, 4-9, 14, 16, 19, 20, 23, and 26 are rendered obvious by Rao, Oestvall, and Montemurro.....	4
1.	Overview of Rao	4
2.	Overview of Oestvall.....	7
3.	Overview of Montemurro.....	9
4.	Combination of Rao, Oestvall, and Montemurro.....	11
(a)	Both Rao’s system and Oestvall’s system selectively allow and block network traffic from applications based on certain criteria.....	12
(b)	A POSITA would have been led to modify Rao’s system to allow/block an application’s network traffic based on the application’s “trusted/untrusted” status as taught by Oestvall to thereby reduce battery drain.....	13
(c)	Like Rao, Montemurro’s system selectively regulates network traffic from applications based on certain criteria.....	16
(d)	A POSITA would have been led to additionally modify the Rao-Oestvall system to apply different policies depending on which network is selected to handle an application’s network traffic as taught by Montemurro.....	18
5.	Analysis	24
B.	[GROUND 2] – Claims 10-12, 15, 17, 18, 22, and 25 are rendered obvious by Rao, Oestvall, Montemurro, and Araujo.....	52
1.	Overview of Araujo.....	52
2.	Combination of Rao-Oestvall-Montemurro and Araujo	54
3.	Analysis	58
C.	[GROUND 3] – Claims 3, 13, 21, and 24 are rendered obvious by Rao, Oestvall, Montemurro, and Freund.....	67
1.	Overview of Freund.....	67

2.	Combination of Rao-Oestvall-Montemurro and Freund.....	68
3.	Analysis	70
D.	PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION...	75
1.	35 U.S.C. §325(d) – Discretionary Denial under 325(d) is not warranted	75
2.	35 U.S.C. §314(a) – Discretionary Denial is not Merited in view of Petitioner’s <i>Sotera</i> Stipulation	76
IV.	CONCLUSION AND FEES	78
V.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	78
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	78
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	78
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	79
D.	Service Information	79

EXHIBITS

- SAMSUNG-1001 U.S. Patent No. 9,277,445 to Raleigh, et al. (“the ’445 Patent”)
- SAMSUNG-1002 Excerpts from the Prosecution History of the ’445 Patent (“the Prosecution History”)
- SAMSUNG-1003 Declaration and Curriculum Vitae of Dr. Kevin Butler
- SAMSUNG-1004 Complaint, Headwater Research LLC v. Samsung Electronics Co., Ltd. et al., 2:22-cv-00422, E.D. Tex., October 26, 2022
- SAMSUNG-1005 U.S. Patent Publication No. 2006/0039354 A1 (“Rao”)
- SAMSUNG-1006 U.S. Patent Publication No. 2007/0038763 A1 (“Oestvall”)
- SAMSUNG-1007 U.S. Patent Publication No. 2009/0207817 A1 (“Montemurro”)
- SAMSUNG-1008 U.S. Patent Publication No. 2009/0217065 A1 (“Araujo”)
- SAMSUNG-1009 U.S. Patent No. 5,987,611 (“Freund”)
- SAMSUNG-1010 M. V. Pedersen, F. H. P. Fitzek, and T. Larsen, “Implementation and Performance Evaluation of Network Coding for Cooperative Mobile Devices,” ICC Workshops - 2008 IEEE International Conference on Communications Workshops, Beijing, China: IEEE, May 2008, pp. 91–96. doi: 10.1109/ICCW.2008.22 (“Pedersen”)
- SAMSUNG-1011 U.S. Patent Publication No. No. 2008/0080458 (“Cole”)
- SAMSUNG-1012 U.S. Patent No. 8,381,127 (“Singh”)
- SAMSUNG-1013 W. R. Stevens, “TCP/IP Illustrated, Volume 1,” 2003, ISBN: 0-13-141155-1 (“Stevens”)
- SAMSUNG-1014 D. P. Bovet, “Understanding the Linux Kernel,” 2000, ISBN: 0-596-00002-2 (“Bovet”)
- SAMSUNG-1015 Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (USPTO June 21, 2022) (“Director’s Guidance”)

SAMSUNG-1016 Samsung Stipulation letter regarding IPR grounds in District court litigation

SAMSUNG-1017 First Amended Complaint, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:22-cv-00422, E.D. Tex., November 30, 2022

SAMSUNG-1018 First Amended Docket Control Order, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:22-cv-00422, E.D. Tex., April 21, 2023

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1pre]	A wireless end-user device, comprising:
[1a]	a wireless wide area network (WWAN) modem to communicate data for Internet service activities between the device and at least one WWAN, when configured for and connected to the WWAN;
[1b]	a wireless local area network (WLAN) modem to communicate data for Internet service activities between the device and at least one WLAN, when configured for and connected to the WLAN; and
[1c]	one or more processors configured to
[1d]	classify, as a first classification, whether data for Internet service activities is to be communicated through the WWAN modem or the WLAN modem, and
[1e]	classify, as a second classification, whether a particular application associated with an Internet service access request, and capable of both interacting with a user in a user interface foreground of the device, and at least some Internet service activities when not interacting with a user in the device user interface foreground,

	is interacting with the user in the device user interface foreground, and
[1f]	apply a differential traffic control policy to the Internet service access request, based on (i) the first and second classifications performed by the one or more processors, and (ii) a differential traffic control policy list distinguishing between a first one or more applications resident on the device and a second one or more applications resident on the device,
[1g]	such that, when the particular application is one of the first one or more applications, the one or more processors are operable to block the Internet service access request in a first state of the first and second classifications, wherein data for Internet service activities is classified as to be provided through the WWAN modem, and the particular application is not classified as interacting with a user in the device user interface foreground, and
[1h]	allow the Internet service access request under at least one different state of the first and second classifications.
Claim 2	

[2]	The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is interacting with the user in the device user interface foreground when the user of the device is directly interacting with that application or perceiving any benefit from that application.
Claim 3	
[3]	The wireless end-user device of claim 1, further comprising the user interface, wherein the user interface is to provide the user of the device with information regarding why the differential traffic control policy is applied to the particular end-user application.
Claim 4	
[4]	The wireless end-user device of claim 1, further comprising the user interface, wherein the user interface is to inform a user of the wireless end-user device when there are options to set, control, override, or modify service usage controls that affect the differential traffic control policy and/or the differential traffic control policy list.
Claim 5	
[5]	The wireless end-user device of claim 1, wherein the differential traffic control policy is part of a multimode profile having different policies for different networks.

Claim 6

[6]	The wireless end-user device of claim 5, wherein the one or more processors are further configured to select a traffic control policy from the multimode profile based at least in part on a network type of a network connection currently in use by the wireless end-user device.
-----	---

Claim 7

[7]	The wireless end-user device of claim 6, wherein the one or more processors are further configured to, when the network type of a network connection is at least one type of WLAN connection, select a traffic control policy from the multimode profile based at least in part on a type of network connection from the WLAN to the Internet.
-----	--

Claim 8

[8]	The wireless end-user device of claim 1, wherein the one or more processors are further to apply the differential traffic control policy such that, when the particular application is one of the second one or more applications, the one or more processors are operable to allow the Internet service access request when data for Internet service activities is classified as to be provided through the WWAN modem,
-----	---

	and the particular application is not classified as interacting with a user in the device user interface foreground.
Claim 9	
[9]	The wireless end-user device of claim 1, wherein the one or more processors are to apply the differential traffic control policy to one of but not both of a WWAN modem connection to a roaming WWAN network and a WWAN modem connection to a home WWAN network.
Claim 10	
[10]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the differential traffic control policy based on a power state of the device.
Claim 11	
[11]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the differential traffic control policy based on a device usage state.
Claim 12	

[12]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the differential traffic control policy based on power control state changes for one or more of the modems.
Claim 13	
[13]	The wireless end-user device of claim 1, wherein the differential traffic control policy defines that the first one or more applications can only have WWAN network access events during particular time windows.
Claim 14	
[14]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to update the differential traffic control policy and/or the differential traffic control policy list based on information received from a network element.
Claim 15	
[15]	The wireless end-user device of claim 1, further comprising an agent to block, modify, remove, or replace user interface messages generated by the particular application based on the applied differential traffic control policy.

Claim 16	
[16]	The wireless end-user device of claim 1, wherein the one or more processors operable to block the Internet service access request are configured to selectively block the Internet service access request by intercepting open, connect, and/or write requests by the particular application to a network stack.
Claim 17	
[17]	The wireless end-user device of claim 16, wherein the one or more processors are configured to respond to an intercepted request by the particular application by emulating network messaging.
Claim 18	
[18]	The wireless end-user device of claim 17, wherein emulating network messaging comprises responding to a network request from the particular application by blocking the request from passing to a network stack and returning to the particular application a message indicating the network request was not successful.
Claim 19	
[19]	The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the particular application is

	interacting with a user in the device user interface foreground based on a state of user interface priority for the application.
Claim 20	
[20]	The wireless end-user device of claim 1, wherein the second one or more applications are not subject to a differential network access control that is applicable to the first one or more applications.
Claim 21	
[21]	The wireless end-user device of claim 1, further comprising a policy agent to: monitor Internet service activity usage for a third application that is neither one of the first one or more applications nor one of the second one or more applications; and to report the activity usage to a network element when Internet service activity usage by the third application exceeds a data usage threshold.
Claim 22	
[22]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to classify between: user applications; system applications, utilities, functions, or processes; and operating system application, utilities, functions, or processes.

Claim 23	
[23]	The wireless end-user device of claim 1, wherein the second one or more applications comprises foreground services.
Claim 24	
[24]	The wireless end-user device of claim 1, wherein block comprises intermittently block when the Internet service access request occurs during selected time windows.
Claim 25	
[25]	The wireless end-user device of claim 1, wherein the one or more processors are configured to prevent the first one or more applications from changing the power state of the modem, and to not prevent the second one or more applications from changing the power state of the modem.
Claim 26	
[26]	The wireless end-user device of claim 1, wherein the at least one different classification state comprises a state wherein data for Internet service activities is classified as to be provided through the WWAN modem, and the particular application is classified as interacting with a user in the device user interface foreground.

Samsung Electronics Co., Ltd. (“**Petitioner**” or “**Samsung**”) petitions for *Inter Partes* Review (“**IPR**”) of claims 1-26 (“**the Challenged Claims**”) of U.S. Patent No. 9,277,445 (“**the ’445 Patent**”). Compelling evidence presented in this Petition demonstrates at least a reasonable likelihood that Samsung will prevail with respect to at least one of the Challenged Claims.

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the ’445 Patent is available for IPR. This petition is being filed within one year of service of a complaint against Samsung. SAMSUNG-1004; SAMSUNG-1017. Samsung is not barred or estopped from requesting review of the Challenged Claims on the below-identified grounds.

B. Challenge and Relief Requested

Samsung requests an IPR of the Challenged Claims on the below grounds. Dr. Kevin Butler provides supporting testimony in his Declaration. SAMSUNG-1003, ¶¶1-298.

Ground	Claim(s)	35 U.S.C. § 103
1	1, 2, 4-9, 14, 16, 19, 20, 23, 26	Rao in view of Oestvall and Montemurro
2	10-12, 15, 17, 18, 22, 25	Rao in view of Oestvall, Montemurro, and Araujo

Ground	Claim(s)	35 U.S.C. § 103
3	3, 13, 21, 24	Rao in view of Oestvall, Montemurro, and Freund

The '445 Patent claims priority to several provisional applications, the earliest of which was filed 1/28/2009. SAMSUNG-1001, Cover. While Samsung does not concede that 1/28/2009 is the priority date that should be afforded to the '445 Patent, for the purposes of this proceeding, each of the references asserted in this Petition qualifies as prior art under 35 USC § 102(b) and/or § 102(e) (as shown in the table below) even if the 1/28/2009 date of the provisional application is used as the priority date of the '445 Patent.

Reference	Filing Date	Publication Date
Rao	7/22/2005	2/23/2006
Oestvall	7/2/2004	2/15/2007
Montemurro	2/15/2008	8/20/2009
Araujo	2/26/2008	8/27/2009
Freund	5/6/1997	11/16/1999

C. Claim Construction

Petitioner submits that no formal claim constructions are necessary because “claim terms need only be construed to the extent necessary to resolve the controversy.” *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); SAMSUNG-1003, ¶19. Petitioner reserves the right to respond to any constructions offered by Patent Owner or adopted by the Board. Petitioner is not conceding that each challenged claim satisfies all statutory requirements, nor is Petitioner waiving any arguments concerning claim scope or grounds that can only be raised in district court. For this petition, Petitioner applies prior art in a manner consistent with Patent Owner’s allegations of infringement before the district court.

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art (“POSITA”) relating to the subject matter of the ’445 Patent as of 1/28/2009 would have had (1) at least a bachelor’s degree in computer science, electrical engineering, or a related field, and (2) three to five years of experience with networking, power consumption of networked computing devices, and/or wireless digital communications systems. SAMSUNG-1003, ¶¶15-17. Additional graduate education could substitute for professional experience, and *vice versa*. *Id.*

II. THE ’445 PATENT

A. Brief Description

The '445 Patent is directed to selectively “apply[ing] a differential traffic control policy to an application requesting Internet service access” through a “system 2700 for application-specific differential network access control.” SAMSUNG-1001, Abstract, 100:28-102:56, FIG. 27; SAMSUNG-1003, ¶¶32-34.

B. Prosecution History

In allowing the claims, the Examiner noted that the cited references did not render obvious the [1a]-[1h] limitations. SAMSUNG-1002, 23-31; SAMSUNG-1003, ¶¶36-37. However, the Examiner did not consider any of Rao, Oestvall, Montemurro, Araujo, and Freund. SAMSUNG, 23-131; SAMSUNG-1003, ¶¶36-37. As discussed below, these references render obvious the Challenged Claims, including the [1a]-[1h] limitations. SAMSUNG-1003, ¶¶36-37.

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. [GROUND 1] – Claims 1, 2, 4-9, 14, 16, 19, 20, 23, and 26 are rendered obvious by Rao, Oestvall, and Montemurro

1. Overview of Rao¹

Rao describes a system for performing “intelligent and client centric prioritization of application network communications on a client based on the type and/or

¹ Descriptions of the references and combinations thereof are incorporated into each mapping that includes citations to these references. All emphasis is added unless otherwise indicated.

priority of an application.” SAMSUNG-1005, [0179], FIG. 5A; SAMSUNG-1003, ¶¶39-53.

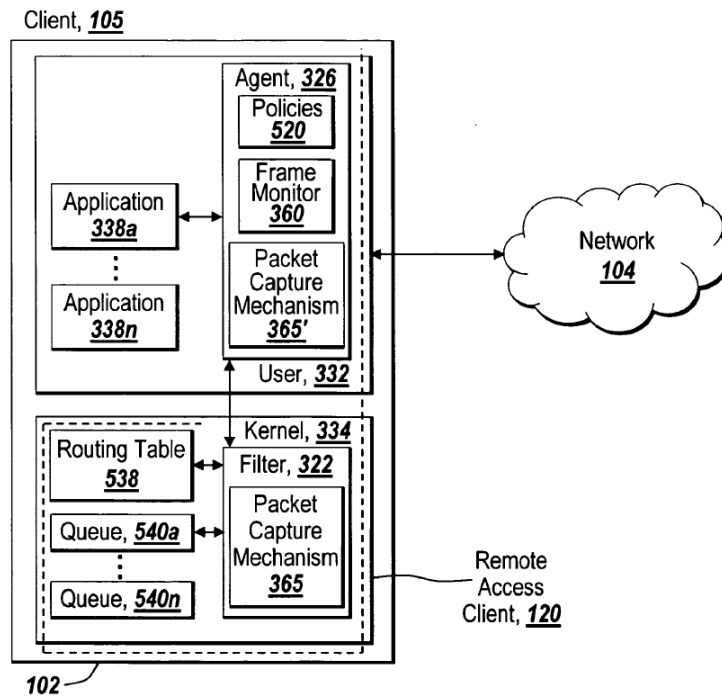


Fig. 5A

SAMSUNG-1005, FIG. 5A²

A “remote access client 105 of computing device 102 is connected to network 104” through one or more “LAN or WAN links” and/or “wireless connections,” and “may execute one or more applications 338 a-338 n, which access the network 104.” SAMSUNG-1005, [0179].

² Annotations to the figures throughout this Petition are shown in color.

Further, Rao's system implements "one or more policies 520 for specifying client-side prioritization of network communications related to applications 338 a-338 n." *Id.*, [0182]. Rao deploys these policies by intercepting packets of network traffic by the applications, determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network based on the determined priority. *Id.*, [0080], [0184]-[0190], FIGS. 5A-5B.

Further, Rao's system "determine[es] how to route network packets" based on a "routing table 538" that "identif[ies] a communication path or connection between a source and destination communication points." *Id.*, [0181].

In some cases, Rao's system prioritizes the captured packets by allowing certain packets to be transmitted to the network (e.g., by using "[a] filter 322 [to] place, arrange, or coordinate network packets into queues 540 a-540 n in support of the priorities"). *Id.*, [0143], [0180], [0191].

In some cases, Rao's system prioritizes the captured packets by blocking network packets from being transmitted to the network, either permanently or temporarily (e.g., by "drop[ping] or accept[ing] the network packets," or "holding" a packet in a queue and "releasing" the packet upon communication of packets from higher priority applications). *Id.*, [0102], [0207], [0040], [0194]; SAMSUNG-1003, ¶¶50-53.

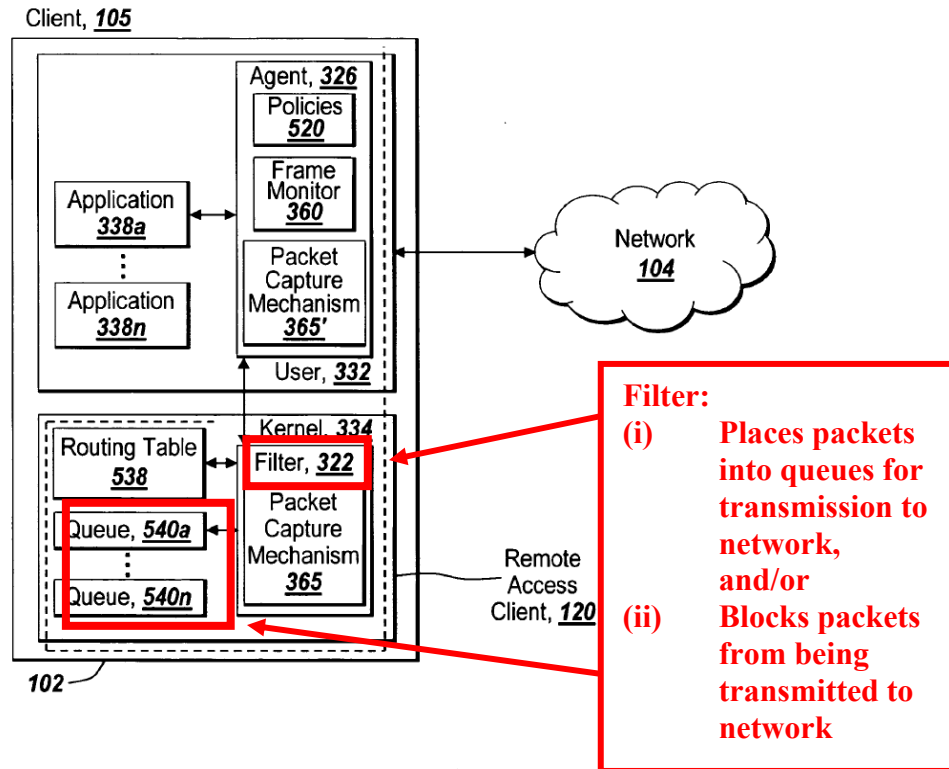


Fig. 5A

SAMSUNG-1005, FIG. 5A (annotated)

2. Overview of Oestvall

Oestvall describes “a method of enabling a multitasking computing device to preserve or conserve resources, such as battery power.” SAMSUNG-1006, [0002]; SAMSUNG-1003, ¶¶54-61. According to Oestvall’s method, a device classifies applications with respect to various criteria, and selectively provides resources to the applications based on their classifications. SAMSUNG-1006, [0008]-[0017], [0019]-[0025].

For instance, applications can be classified based on “‘trust’ or certification criteria” as (i) “untrusted” applications and (ii) “trusted” applications. *Id.*, [0010],

[0015], FIG. 1.

Applications also can be classified as “in the background or foreground on [a] display,” and can switch between these states. *Id.*, [0014], [0021], [0023], [0025].

Further, the device can provide resources to the applications differently, based on these classifications. *Id.*, [0010]-[0017], [0021]-[0025]. For example, the device can selectively:

- (i) Prevent an “untrusted” application in the background from running (e.g., by preventing the application from “being given any services or consuming any resources”) (*id.*, [0023]),
- (ii) Allow an “untrusted” application in the foreground to run (*id.*, [0021], [0025]), and
- (iii) Allow a “trusted” application to run, regardless of whether it is in the foreground or background (*id.*, [0015]).

That is, Oestvall’s device selectively provides resources to applications that it deems sufficiently important to consume resources (e.g., “trusted” applications and “untrusted” applications in the foreground), while selectively denying resources to applications that it deems not sufficiently important to consume resources (e.g., “untrusted” applications in the background). SAMSUNG-1003, ¶60.

As Oestvall describes, this method “is a valuable addition to power conservation strategies, especially (although without limitation) to battery operated devices.” SAMSUNG-1006, [0024]. For example, the method can “prevent background untrusted applications from ‘polling’ for data over a wireless network, an activity that can potentially drain a battery quickly.” *Id.* Accordingly, the “battery life” of the device is “increased.” *Id.*, [0009].

3. Overview of Montemurro

Montemurro describes “a policy-based mechanism to configure connections and routes” for “[c]ommunication devices capable of at least two communication modes (e.g. WLAN, WMAN and WWAN and/or wired modes).” SAMSUNG-1007, Abstract; SAMSUNG-1003, ¶¶62-66.

Montemurro’s system includes a “TCP/IP network stack 206A” having a “routing table 210” that specifies “which network interface 208 will be used for transmission of [a] packet” (e.g., WLAN 208A, WMAN 208B, and/or WWAN 208C managed by the connection table 206C). SAMSUNG-1007, [0030], FIG. 2.

Further, Montemurro’s system includes “a rules engine 206A ... as a policy-based mechanism using rules to configure TCP/IP network stack 206B and connection table 206C to coordinate communications for applications 204 using communications interfaces (also referenced as network interfaces) 208.” *Id.*, [0027]. Specifically, the “rules engine 206A configures (i.e. modifies, periodically in response

to changes of state and the evaluation of its rules) connection table 206C and routing table 210 to optimize the flow of communications over multiple communications modes (e.g. interfaces 208 and respective networks 104 and 106) ... to ensure that data goes out [sic] the most appropriate network (via respective interface 208).” *Id.*, [0034]-[0035].

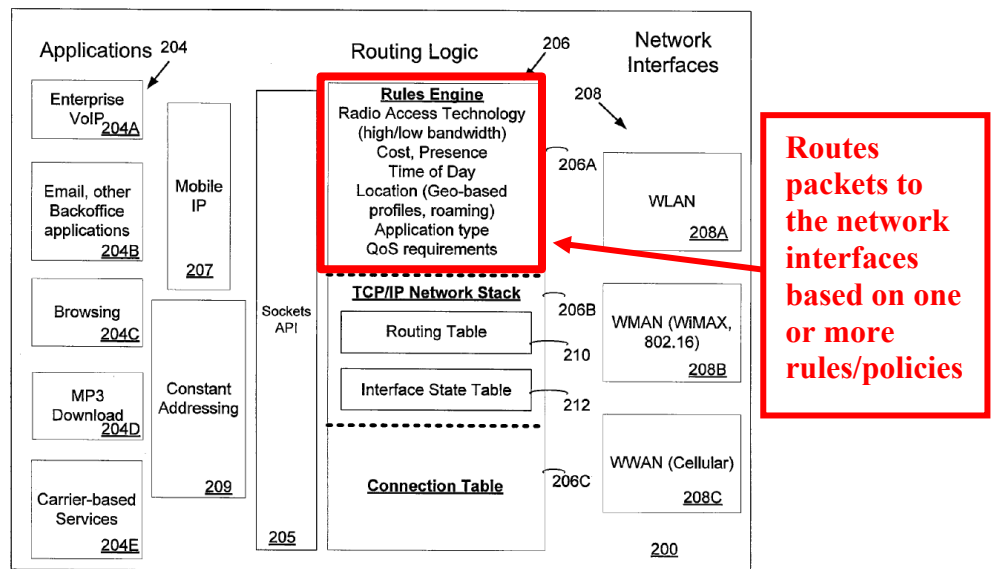


Figure 2

SAMSUNG-1007, FIG. 2 (annotated)

In general, the “[r]ules engine 206A configures the communication operations with a set of rules/policies,” which can “include various factors such as radio access technology (e.g. for high/low bandwidth properties), cost, presence, time of day, location (e.g. geo-based policies, network roaming), destination IP address, application type, and Quality of Service (QoS) requirements, among others.” *Id.* Further, these “rules/policies” can specify that certain applications use certain

types of networks under certain conditions. *Id.*, [0019].

As Montemurro describes, these “rules/policies” can be used “to optimize communications for multi-mode capable devices” by accounting for “different radio access technologies,” each of which may have “different properties ... such as bandwidth, range, cost, and power consumption, among other considerations.” *Id.*, [0030].

4. Combination of Rao, Oestvall, and Montemurro

A POSITA would have found it obvious to modify Rao’s system of prioritizing network packets based on the specific application classification criteria taught by Oestvall and Montemurro. SAMSUNG-1003, ¶¶67-102; §III.A.1-3. Combining Rao, Oestvall, and Montemurro would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of a known technique to improve similar devices (methods, or products) in the same way. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 415-421, 82 USPQ2d 1385, 1395-97 (2007); MPEP 2143; SAMSUNG-1003, ¶¶67-102.

Specifically, a POSITA would have recognized that (i) Rao, Oestvall, and Montemurro are directed to similar operations having similar purposes (e.g., controlling an application’s access to a network to preserve limited system resources), and (ii) Oestvall and Montemurro provide specific classification criteria for achiev-

ing specific technical benefits (e.g., reducing battery consumption in a network-enabled device and optimizing communications using multiple different networks, respectively). SAMSUNG-1003, ¶¶67-102.

(a) Both Rao's system and Oestvall's system selectively allow and block network traffic from applications based on certain criteria

Rao's system includes several applications configured to transmit network packets to a network (e.g., the Internet via one or more wireless connections). SAMSUNG-1005, [0095],[0125], [0179]; §III.A.1. Rao's system controls each of the applications' access to the network by intercepting packets of network traffic by the applications, determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network based on the determined priority. SAMSUNG-1005, [0184]-[0190], FIG. 5B; SAMSUNG-1003, ¶¶69-74.

Specifically, Rao's system prioritizes network packets by implementing one or more policies 520 for controlling network traffic. SAMSUNG-1005, [0182]. Based on these policies, Rao's system can selectively use a filter to (i) allow network packets to be transmitted to the network or (ii) block the network packets from being transmitted to the network. SAMSUNG-1005, [0191], [0194], [0207]; SAMSUNG-1003, ¶¶69-74; §III.A.1.

Like Rao, Oestvall describes an application-based priority system for controlling access to resources. SAMSUNG-1006, [0008]-[0017], [0019]-[0025]; SAMSUNG-1003, ¶¶75-78. Further, Oestvall contemplates similar criteria as Rao, and teaches that specific combinations of these criteria can be selected to achieve a specific technical benefit. SAMSUNG-1006, [0008]-[0017], [0019]-[0025]; SAMSUNG-1003, ¶¶75-78.

Specifically, Oestvall teaches that certain types of applications (e.g., “untrusted” applications) that are running in the background of the client should be assigned a low priority, such that they cannot access a network. SAMSUNG-1006, [0008], [0014]-[0017], [0021], [0023], [0024]; SAMSUNG-1003, ¶76.

Further, Oestvall teaches that certain other types of applications (e.g., “trusted” applications) should be assigned a high priority, such that they can continue to access a network. SAMSUNG-1006, [0008], [0014]-[0017], [0021], [0023], [0024]; SAMSUNG-1003, ¶77.

As Oestvall describes, these combinations of criteria can be used to “prevent background untrusted applications from ‘polling’ for data over a wireless network, an activity that can potentially drain a battery quickly.” SAMSUNG-1006,[0024]; SAMSUNG-1003, ¶78.

- (b) A POSITA would have been led to modify Rao’s system to allow/block an application’s network traffic based on the application’s**

**“trusted/untrusted” status as taught by Oestvall
to thereby reduce battery drain**

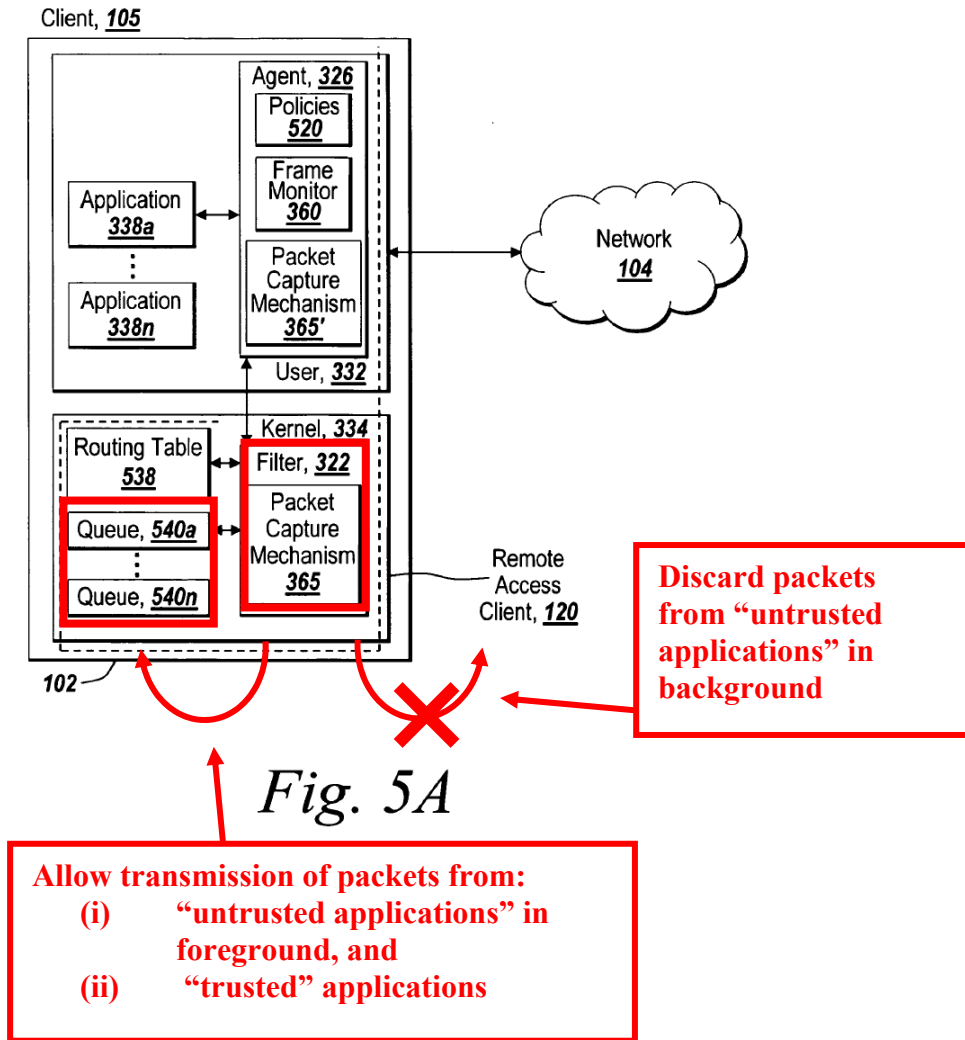
A POSITA would have readily recognized that Rao’s remote access client 120 could use a filter to discard packets from background untrusted applications to thereby prevent them from being communicated over network 104. SAMSUNG-1003, ¶¶79-87. As a consequence, the battery life of a mobile device client 105 would be increased, as taught by Oestvall. *Id.*, ¶¶79-87. Indeed, while Oestvall teaches increasing battery life by preventing such applications from running and thereby engaging in any network communications, a POSITA would have recognized that the power usage associated with using a wireless modem to transmit network packets to a network far exceeds the power usage associated with an application generating those network packets. *Id.*, ¶79. *Also see, generally*, SAMSUNG-1010. Accordingly, a POSITA would have readily recognized that Rao’s system could be used to enable a similar increase in battery life by specifically preventing the battery draining activity identified by Oestvall (i.e., preventing the network/packet communications that result in excessive battery drain). SAMSUNG-1003, ¶¶79-80.

As an example of this modification, a POSITA would have configured Rao’s “filter 322” to selectively block network packets and/or transmit network packets to the network, based on the criteria specified by Oestvall. SAMSUNG-1003, ¶81. Specifically, the “filter 322” would selectively “discard[]” network packets from

applications that are “untrusted” and running in the background (e.g., a classification of applications that should be assigned a low priority, as taught by Oestvall). *Id.*, ¶81. Accordingly, these applications can no longer poll for data over a wireless network (i.e., an activity that Oestvall teaches as being particularly burdensome on a battery). *Id.*

Further, the “filter 322” would selectively allow the transmission of network packets from applications that are either (i) “untrusted” and running in the foreground or (ii) “trusted,” regardless of whether they are running in the foreground or the background (e.g., classifications of applications that should be assigned a high priority, as taught by Oestvall). *Id.*, ¶¶82-87. Accordingly, applications that are sufficiently important can continue to exchange data in accordance with one or more Internet services. *Id.*, ¶¶82-87.

An example modification to Rao’s system in view of Oestvall’s teachings (“Rao-Oestvall system”) is shown below.



SAMSUNG-1005, FIG. 5A (annotated)

- (c) Like Rao, Montemurro's system selectively regulates network traffic from applications based on certain criteria

Like Rao, Montemurro describes an application-based priority system for controlling access to resources. SAMSUNG-1007, Abstract, [0011], [0027]-[0036]; SAMSUNG-1003, ¶¶88-91. Further, Montemurro contemplates similar criteria as Rao, and teaches that specific combinations of these criteria can be selected to achieve a specific technical benefit. SAMSUNG-1007, Abstract, [0011],

[0027]-[0036]; SAMSUNG-1003, ¶¶88-91.

Like Rao, Montemurro describes that controlling an application's access to a network based at least in part on (i) the "application type," (ii) the "destination IP address" of the traffic, and (iii) the protocol for transmitting data (e.g., wireless protocols for transmitting data over the WLAN, WWAN, etc.). SAMSUNG-1007, [0029], [0054]; SAMSUNG-1003, ¶¶88-89. Regarding network protocols specifically, Rao describes that its system can "be used in any other types of networking environments with other networking protocols" (SAMSUNG-1005, [0182], [0082]), of which Montemurro's wireless protocols are an example. SAMSUNG-1003, ¶89.

Based on these factors (among others), Montemurro's system selects a particular network interface for transmitting packets by that application. For instance, a "rules engine 206A executes and modifies, as applicable, the routing table 210 to ensure that data goes out [sic] the most appropriate network (via respective interface 208)." SAMSUNG-1007, [0035]; SAMSUNG-1003, ¶90. Further, various "rules/policies" can be deployed to selectively allow certain types of applications to access certain networks, while preventing those applications from accessing other networks. SAMSUNG-1007, [0029].

As Montemurro explains, these "rules/policies" can be used "to optimize

communications for multi-mode capable devices” by accounting for “different radio access technologies,” each of which may have “different properties ... such as bandwidth, range, cost, and power consumption, among other considerations.”

SAMSUNG-1007, [0030]; SAMSUNG-1003, ¶91.

(d) A POSITA would have been led to additionally modify the Rao-Oestvall system to apply different policies depending on which network is selected to handle an application’s network traffic as taught by Montemurro

A POSITA would have further modified the Rao-Oestvall system to apply different policies to an application’s network traffic based on which network is selected to handle an application’s network traffic, as taught by Montemurro. SAMSUNG-1003, ¶¶92-102. Specifically, a POSITA would have recognized that Montemurro teaches considering at least some of the same factors as Rao when selecting a network for an application’s network traffic (e.g., the “application type,” the “destination IP address” of the traffic, and the protocol for transmitting data). *See* §IIIA.1, §IIIA.3; SAMSUNG-1003, ¶¶92-102. Further, in view of Montemurro, a POSITA would have recognized that using these factors (among others) to select an appropriate type of network for transmitting the data would optimize “multi-mode capable devices” (e.g., by accounting for “different radio access technologies.”) SAMSUNG-1007, [0030]; SAMSUNG-1003, ¶¶92-102.

Specifically, in Rao’s system, a remote access client 120 includes a “routing

table 538 compris[ing] information about a source computing device and a destination computing device to identify a communication path or connection between a source and destination communication points” on the network. SAMSUNG-1005, [0181]. Further, Rao describes that a system can be connected to a network using “one or more “LAN or WAN links” and/or “wireless connections. *Id.*, [0179]. To the extent that Rao does not expressly describe using the “routing table 538” to select between different “communication paths” that include a wireless LAN link or a wireless WAN link, a POSITA nevertheless would have found it obvious to modify the “routing table 538” to make such a selection in view of Montemurro.

SAMSUNG-1003, ¶93.

As an example of this modification, in at least some implementations, a POSITA would have configured Rao’s system to include multiple sets of queues, where each set corresponds to a different network interface (e.g., network interfaces for accessing a WWAN, WLAN, etc.). *Id.*, ¶94. This is because a POSITA would have understood or recognized that Rao’s single set of queues is used to prioritize network traffic for a *single* network at a time (e.g., the “network 104” which is described as being one of “a local-area network (LAN), such as a company Intranet, a metropolitan area network (MAN), or a wide area network (WAN), such as the Internet or the World Wide Web,” SAMSUNG-1005, [0095]), and that in situations in which the device is connected to *multiple* networks concurrently (e.g.,

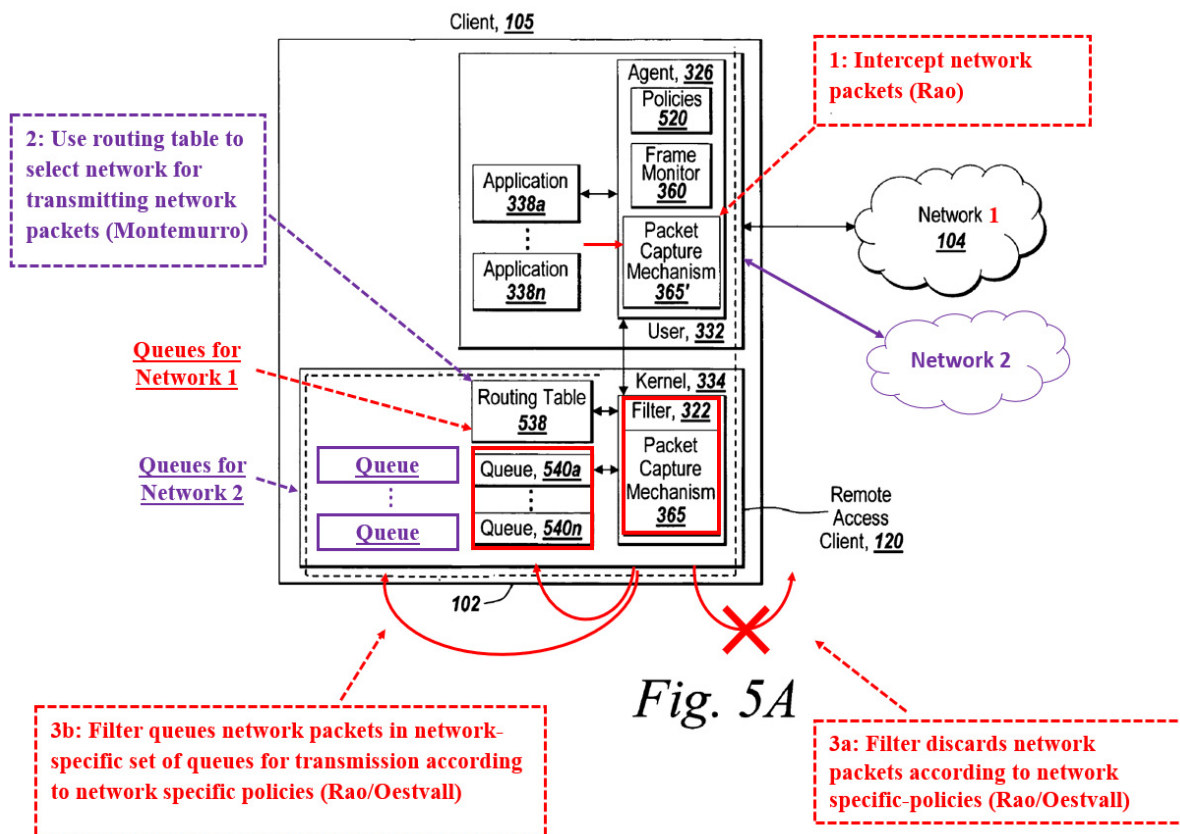
WWAN, WLAN, etc., as described by Montemurro), a different respective set of queues could be used to prioritize network traffic for each network specifically.

SAMSUNG-1003, ¶94. For instance, a POSITA would have recognized that this would allow the system to prioritize data in a manner that is specifically tailored to the properties of each network and/or the usage conditions of each network (e.g., the degree of which each network is congested). *Id.*, ¶94.

Further, in view of Montemurro, a POSITA would have configured Rao's routing table 538 in at least some implementations such that a given communication generated by an application (e.g., one or more packets) would be selectively routed by the remote access client 120 to a certain network (e.g., WWAN, WLAN, etc.) or blocked from a network based on criteria such as (i) the "application type," (ii) the "destination IP address" of the traffic, and (iii) the protocol for transmitting data. *Id.*, ¶95. According to this configuration, the "packet capture mechanism 365, 365'" would intercept network packets generated by the applications (step 1 below). *Id.* Upon the system selecting a particular network that is appropriate for one or more packets (step 2 below), those packets would be selectively provided to the set of queues corresponding to the selected network for prioritization and transmission (e.g., in accordance with the Rao-Oestvall combination, as described above) (see steps 3a, and 3b below). *Id.* Conversely, upon determining that a particular network is not appropriate for the one or more packets, the packets would

not be provided to the set of queues corresponding to that network and that network's policies would not be applied. *Id.*

An example modification to the Rao-Oestvall system in view of Montemurro's teachings ("Rao-Oestvall- Montemurro combination" or "ROMC") is shown below.



SAMSUNG-1005, FIG. 5A (revised and annotated)

In doing so, a POSITA would have been led to apply Montemurro's techniques to thereby enable Rao's system to intelligently select among the various networks to optimize "multi-mode capable devices," such as by accounting for "different radio access technologies." SAMSUNG-1007, [0030]; SAMSUNG-

1003, ¶¶97-102. Further, by modifying Rao’s system to first perform Montemurro’s network selection prior to prioritizing network traffic according to the Rao-Oestvall combination, the combined system would enjoy both the “multi-mode” optimization benefits taught by Montemurro and the application-specific network prioritization benefits as taught by Rao and Oestvall. SAMSUNG-1003, ¶¶97-102.

For instance, in view of Montemurro, if a first network (e.g., WWAN) is selected from among multiple networks to transmit an application’s network traffic, a POSITA would have found it obvious to apply a first policy specific to the first network to the network traffic. SAMSUNG-1003, ¶98. As an example first policy, the device would selectively place network packets in a set of queues that are *specific to the first network* to selectively allow or block an application’s network traffic with respect to the first network. *Id.*, ¶98. For instance, a POSITA would have found it obvious to allow or block network traffic from applications based on the application’s “trusted/untrusted” status and whether the application is running in the foreground or the background) (e.g., according to the Rao-Oestvall combination) See §III.A.3. SAMSUNG-1003, ¶98.

Further, if a second network (e.g., a WLAN) is selected from among multiple networks to transmit an application’s network traffic instead, a POSITA would

have found it obvious to apply a second *different* policy *specific to the second network* to selectively allow or block an application's network traffic with respect to the second network. SAMSUNG-1003, ¶99. As an example second policy, the device would selectively place network packets in a set of queues that are *specific to the second network* to selectively allow or block an application's network traffic with respect to the second network. *Id.*, ¶99. That is, the first and second policies would differ at least because the first and second policies selectively place network packets in different respective sets of queues. *Id.*, ¶99.

A POSITA would have found it obvious, in some cases, to configure the second policy in a similar manner as the first policy (i.e., with the exception that the policies selectively place network packets in different respective sets of queues). *Id.*, ¶100. For example, a POSITA would have recognized or understood that if the characteristics of the first and second networks are similar to another, the second policy could likewise be configured to allow or block network traffic from applications based on the Rao-Oestvall combination, as with the first policy. *See* §III.A.3.c; SAMSUNG-1003, ¶100.

A POSITA also would have found it obvious, in some cases, to configure the second policy in a different manner as the first policy. *Id.*, ¶101. For example, a POSITA would have found it obvious to modify the second policy (e.g., relative to

the first policy) to account for any differences in the bandwidth and/or cost between using the first and second networks to transmit data (e.g., as taught by Montemurro). *Id.*, ¶101. This is because a POSITA would have understood or recognized that policies for prioritizing network traffic are used to make better use of limited resources, and that if those resource limitations were less for a particular network, the policies could be modified to adapt the device's usage of that network to account for that difference. *Id.*, ¶101.

5. Analysis

[1pre]

Rao describes a device that is configured to communicate data wirelessly with a network (*wireless end-user device*). SAMSUNG-1005, [0090], [0125]; §III.A.1. SAMSUNG-1003, ¶¶103-104.

[1a], [1b]

Rao describes a device that is configured to communicate data wirelessly with a WWAN, a WLAN, and the Internet (e.g., using “wireless network adapter[s]” and/or “modem[s]”) (*WWAN modem [1a], WLAN modem [1b]*). SAMSUNG-1005, [0125]. SAMSUNG-1003, ¶¶105-114.

Further, Rao describes that the device is configured to communicate data for Internet service activities via the WWAN and/or the WLAN, such as to obtain email services, access a web or Internet service, access a desktop sharing server,

and/or access a collaboration server (*communicate data for Internet service activities between the device and at least one WWAN, when configured for and connected to the WWAN [1a], communicate data for Internet service activities between the device and at least one WLAN, when configured for and connected to the at least one WLAN [1b]*). SAMSUNG-1005, [0090]; SAMSUNG-1003, ¶¶105-114.

To the extent that Rao does not expressly describe a “WWAN modem” or “WLAN modem,” a POSITA would have understood or found it obvious to implement a WWAN modem or WLAN modem in Rao’s system in view of Rao’s teaching that (i) a device can access a WAN or LAN wirelessly, and (ii) a “modem” can be used to interface the device with “any type of network.” SAMSUNG-1005, [0125]; SAMSUNG-1003, ¶108, ¶112. Further, network configurations for mobile devices that enabled WWAN and/or WLAN connectivity via modems were conventional by the Critical Date. *Id.*, ¶108, ¶114. SAMSUNG-1011, [0035], FIG. 2.

Further, Montemurro also describes that “[c]ommunication devices [are] capable of at least two communication modes (e.g. WLAN ... and WWAN).” SAMSUNG-1007, Abstract. In view of Montemurro, a POSITA would have found it obvious to include both a “WWAN modem” and “WLAN modem” to allow the device to connect to multiple types of networks. SAMSUNG-1003, ¶113.

[1c]

Rao describes “a computing device useful for practicing an embodiment of the [subject matter described by Rao].” SAMSUNG-1005, [0118], FIG. 1D.

As Rao describes, “[e]ach computing device 102 includes a central processing unit [121]”³ (*one or more processors*) that includes “any logic circuitry that responds to and processes instructions fetched from the main memory unit 104.” *Id.*, [0118]. *See also id.*, [0121] (“main processor 100”); FIG. 1E; SAMSUNG-1003, ¶¶115-118.

³ Rao [0118] erroneously refers to the “central processing unit” as “102,” rather than “121” as depicted in FIG. 1D.

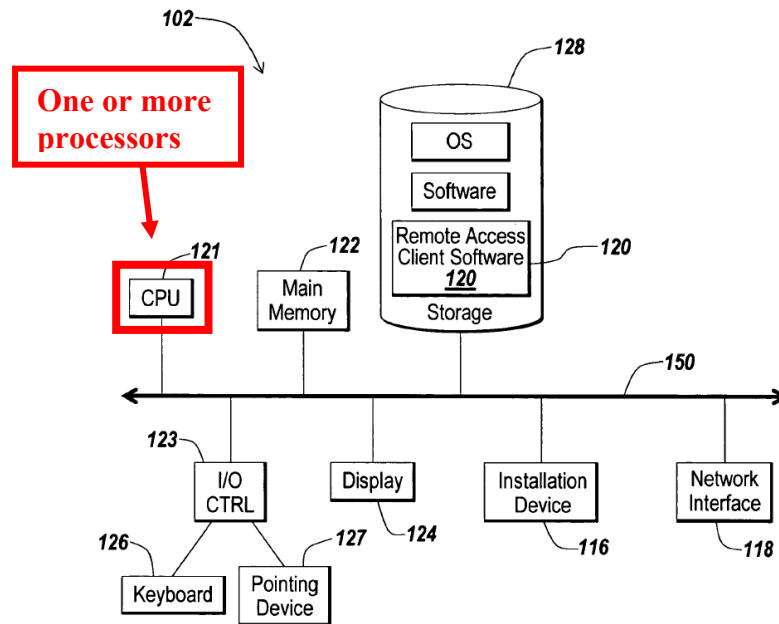


Fig. 1D

SAMSUNG-1005, FIG. 1D (annotated)

Further, as described below, a POSITA would have found it obvious to perform various operations using the processors. *See* [1d]-[1h], [2], [6]-[12], [14], [16]-[17], [19], [22], [26]; SAMSUNG-1003, ¶118.

[1d]

In view of Montemurro, a POSITA would have configured Rao's routing table 538 in at least some implementations such that a given communication generated by an application (e.g., one or more packets, constituting *data for Internet service activities*) would be selectively routed by the remote access client 120 to a

certain network (e.g., WWAN, WLAN, etc.). §III.A.4; SAMSUNG-1003, ¶¶119-

120. In doing so, the ROMC system would *classify, as a first classification, whether data for Internet service activities is to be communicated through the WWAN modem or the WLAN modem*. See also [1a], [1b].

[1e]

Regarding [1e(i)], a POSITA would have understood or found it obvious that Rao's applications can be *associated with an Internet service access request* based on Rao's teachings of its applications communicating over the Internet (e.g., in the form of network packets) and receiving service from Internet servers. SAMSUNG-1003, ¶¶121-124.

For example, Rao describes that an application can communicate with one or more servers on the network 104, such as the Internet. SAMSUNG-1005, [0090], [0095], [0125]. Further, Rao describes that an application can access services provided by a server 102e connected to the network 104, such as those provided by “an application server providing email services such as Microsoft Exchange,” “a web or Internet server,” “a desktop sharing server,” or “a collaboration server” (*a particular application associated with an Internet service access request*). *Id.*, [0090]; FIG. 1A. Further, in Rao, an application may attempt to access an Internet service by transmitting packets to that Internet service. See, e.g., *id.*, [0090], [0179], [0184]; SAMSUNG-1003, ¶123.

Regarding [1e(ii)], as discussed above, Rao describes that applications can request access to Internet services. SAMSUNG-1005, [0090]; SAMSUNG-1003, ¶¶122-130. Further, Rao describes that an application may be “running in the foreground or the background of the client.” SAMSUNG-1005, [0182]. *See also id.*, [0188]-[0189]. A POSITA would have understood or found it obvious that Rao’s applications envision interactions with users in the foreground (e.g., such that the user can engage in email, web, desktop sharing, and/or collaboration activities) ***(capable of ... interacting with a user in a user interface foreground of the device)***. SAMSUNG-1003, ¶125.

Further, Rao contemplates that applications that are running in the background may perform at least some Internet service activities, such as by generating network packets ***(capable of ... at least some Internet service activities when not interacting with a user in the device user interface foreground)***. SAMSUNG-1005, [0003]. For example, a POSITA would have understood or found it obvious that Rao’s email application can perform Internet service activities in the background (e.g., polling an email server for updates and/or retrieving emails in the background). SAMSUNG-1005, [0003], [0090]; SAMSUNG-1003, ¶126.

To the extent that Rao does not expressly describe that an application would be capable of both (i) interacting with a user in a user interface foreground of the device, and (ii) at least some Internet service activities when not interacting with a

user in the device user interface foreground, this feature would have been obvious in view of Oestvall. SAMSUNG-1003, ¶127. For example, Oestvall describes that a device includes applications that are capable of both:

- (i) Running the “foreground” and “present[ing] a user interface with which a user can interact,”, and
- (ii) Running in the “background” and “not being interacted with by an end-user and ... present[ing] no user interface with which a user could interact.” SAMSUNG-1006, [0006], [0015].

Further, Oestvall describes that an application may be capable of consuming “resources” (e.g., by performing network service activities such as “‘polling’ for data over a wireless network”) when in the background (*capable of ... at least some ... activities when not interacting with a user in the device user interface foreground*). SAMSUNG-1006, [0023]-[0024]; SAMSUNG-1003, ¶128.

In view of Oestvall, a POSITA would have understood or found it obvious that Rao’s applications can interact with users in the foreground by “present[ing] a user interface with which a user can interact” to allow users to engage in activities such as email, web, desktop sharing, and/or collaboration) (*capable of ... interacting with a user in a user interface foreground of the device*). SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶129.

Further, in view of Oestvall, a POSITA would have understood or found it

obvious that Rao's applications can perform Internet service activities (e.g., an email application polling an email server for updates and/or retrieving emails), even if the user is not interacting with the application and/or the application is not presenting a user interface with which a user could interact (*capable of ... at least some Internet service activities when not interacting with a user in the device user interface foreground*). SAMSUNG-1006, [0024]; SAMSUNG-1003, ¶130.

Regarding [1e(iii)], Rao describes that the device classifies “whether an application is running in the foreground or the background of the client 105” (*classify, as a second classification, whether a particular application ... is interacting with the user in the device user interface foreground*). SAMSUNG-1005, [0182], [0188]-[0189]; SAMSUNG-1003, ¶131.

Oestvall also describes that the device uses a “window server component 2 ... to determine if an application is in the background or foreground on display” (*classify, as a second classification, whether a particular application ... is interacting with the user in the device user interface foreground*). SAMSUNG-1006, [0008], [0016]-[0017], [0022]-[0023]; SAMSUNG-1003, ¶132.

[1f]

Rao describes that an application is associated with an *Internet service access request*. [1e]; SAMSUNG-1003, ¶¶133-134.

Further, a POSITA would have found it obvious to select a particular network to transmit an application's network traffic in accordance with the Internet service access request, and apply a particular differential traffic control policy to the Internet service access request based on the selected network (*apply a differential traffic control policy to the Internet service access request based on the first classification performed by the one or more processors*). §III.A.4; [1d]; SAMSUNG-1003, ¶¶135-136.

As an example, in view of Montemurro, if a first network (e.g., WWAN) is selected to transmit an application's network traffic, a POSITA would have found it obvious to apply a first policy specific to the first network to the network traffic. SAMSUNG-1003, ¶136. Further, if a second network (e.g., a WLAN) is selected to transmit an application's network traffic instead, a POSITA would have found it obvious to apply a second different policy specific to the second network instead. SAMSUNG-1003, ¶137.

Further, upon selecting a network and a corresponding policy, a POSITA would have found it obvious, in at least some implementations, to apply the selected policy by allowing or blocking an applications' network traffic (*applying a differential traffic control policy to the Internet service access request*) based on whether the application is running in the foreground or the background (... *based on the second classification performed by the one or more processors*) (e.g., as

taught by both Oestvall and Rao) and the application's "trusted/untrusted" status

(...and distinguishing between a first one or more applications resident on the device and a second one or more applications resident on the device) (e.g., as taught by Oestvall). See §III.A.4.c; SAMSUNG-1003, ¶¶137-140.

For example, a POSITA would have found it obvious to configure the ROMC system to prioritize network packets according to one or more policies for controlling network traffic, as taught by Rao. SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶138. These policies can "define prioritization" based on various criteria, including:

- (i) "the name of the application,"
- (ii) "the type of application,"
- (iii) "the type of one or more protocols used by the application[s],"
- (iv) "the size of the payload of the network packet"
- (v) "whether an application is running in the foreground or the background of the client," and/or
- (vi) "the destination network address, such as host name or IP address, and/or destination port number." SAMSUNG-1005, [0182].

Specifically, in applying Rao's policies to differentially distinguish how the network traffic of distinct applications will be handled, Rao's system considers any one or more of the above criteria, including "whether an application is running in

the foreground or the background of the client” (... *based on the second classification performed by the one or more processors*). SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶139.

Further, by also considering the “type[s]” of applications and/or differently named applications, among other criteria, the application of Rao’s policies for handling application traffic is further based on *distinguishing between a first one or more applications resident on the device and a second one or more applications resident on the device*. SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶140.

Rao describes that “[t]he policies ... may comprise any type and format of syntax and/or language for specifying a policy, and may be provided via any type and/or form of medium,” which a POSITA would have understood would encompass one or more lists (*a differential traffic control policy list*). SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶141. However, to the extent that Rao does not expressly describe representing these applications in the form of a list, a POSITA nevertheless would have found it obvious to implement such a list, as they would have recognized that a list is a commonplace “format of syntax and/or language” for enumerating data. SAMSUNG-1003, ¶141.

Further, in accordance with its policies, Rao’s system selectively uses a filter to (i) allow network packets to be transmitted to the network or (ii) block the network packets from being transmitted to the network, thereby applying the policies

to the Internet service access request embodied by those network packets. SAMSUNG-1005, [0191], [0194], [0207]; SAMSUNG-1003, ¶142. *See also* [1e]; §III.A.4.

To the extent that Rao alone does not expressly describe applying a differential traffic control policy based on the second classification and the differential traffic control policy list, these features nevertheless would have been obvious further in view of Oestvall. SAMSUNG-1003, ¶¶143-148.

Like Rao, Oestvall describes an application-based priority system for controlling access to resources. SAMSUNG-1006, [0008]-[0017], [0019]-[0025]; SAMSUNG-1003, ¶144. Further, Oestvall contemplates at least some of the same criteria as Rao, and teaches that specific combinations of these criteria can be selected to achieve a specific technical benefit. SAMSUNG-1006, [0008]-[0017], [0019]-[0025]; SAMSUNG-1003, ¶144.

Specifically, Oestvall describes that applications can be classified based on “‘trust’ or certification criteria” (*a differential traffic control policy list*) as (i) “untrusted” applications (...*distinguishing between a first one or more applications resident on the device*) and (ii) “trusted” applications (... *and a second one or more applications resident on the device*). SAMSUNG-1006, [0010], [0015], FIG. 1; SAMSUNG-1003, ¶145.

To the extent that Oestvall does not expressly describe representing these applications in the form of a list, a POSITA nevertheless would have found it obvious to implement such a list, as they would have recognized that a list is a commonplace format of syntax and/or language for enumerating data. *Id.*, ¶146.

Further, like Rao, Oestvall describes that applications can be classified as “in the background or foreground on [a] display” (*performing the second classification*). SAMSUNG-1006, [0023]; SAMSUNG-1003, ¶147. *See also* [1e].

In addition, Oestvall describes applying a traffic control policy to an application differently, depending on these classifications (*apply a differential traffic control policy to the Internet service access request*). SAMSUNG-1003, ¶148. For example, Oestvall’s system denies resources to applications that are not sufficiently important to consume resources, and provides resources to applications that are sufficiently important to consume resources (e.g., to selectively allow certain applications to “poll[]’ for data over a wireless network”). SAMSUNG-1006, [0008], [0010], [0015]-[0017], [0022]-[0025].

[1g]

A POSITA would have found it obvious to (i) select a particular network to transmit an application’s network traffic in accordance with the Internet service access request and (ii) apply a particular differential traffic control policy to the Internet service access request based on the selected network and the characteristics of

the application. III.A.4; [1f]; SAMSUNG-1003, ¶¶149-150.

For example, in view of Montemurro, if a WWAN is selected to transmit an application's network traffic (*a first state of the first ... classifications, wherein data for Internet service activities is classified as to be provided through the WWAN modem*), a POSITA would have found it obvious to apply a WWAN-specific policy to the network traffic. SAMSUNG-1003, ¶151.

Further, upon selecting the WWAN, the ROMC system would, in at least some implementations, prioritize the application's network packets based on the specific application classification criteria taught by Rao and Oestvall. SAMSUNG-1003, ¶152.

Specifically, the “filter 322” would selectively “discard” network packets (*block the Internet service access request*) from applications that are “untrusted” (*...when the particular application is one of the first one or more applications*) and running in the background (*in a first state of the ... second classifications, wherein ... the particular application is not classified as interacting with a user in the device user interface foreground*) (e.g., a classification of applications that should be assigned a low priority, as taught by Oestvall). See §III.A.4; SAMSUNG-1003, ¶¶153-154. Accordingly, these applications can no longer poll for data over a wireless network (i.e., an activity that Oestvall teaches as being particu-

larly burdensome on a battery). *See* §III.A.4; SAMSUNG-1006, [0024]; SAMSUNG-1003, ¶¶153-154.

[1h]

Upon selecting the WWAN, the ROMC system would, in at least some implementations, prioritize the application's network packets based on the specific application classification criteria taught by Rao and Oestvall. [1g]; SAMSUNG-1003, ¶¶155-156.

Specifically, the “filter 322” would selectively “allow” network packets (*allow the Internet service access request*) when the application is “untrusted” (*one of the first one or more applications*) and selected for WWAN communications and in the foreground (*...under at least one different state of the first and second classifications*). The allowance of the network packets over the WWAN would occur, for example, as a result of the “untrusted” application changing from being in the background to being in the foreground and thereby enjoying a higher priority per Rao's and Oestvall's teachings. *See* §III.A.4; SAMSUNG-1003, ¶157.

Specifically, by virtue of the application now being in the foreground, these network packets would be placed into a “highest priority queue,” thereby having their communication be unfettered as taught by Oestvall such that the network packets are immediately transmitted to the network (e.g., prior to the transmission of network packets placed into lower priority queues). SAMSUNG-1005, [0194];

SAMSUNG-1003, ¶158; §III.A.4. Accordingly, applications that are sufficiently important can continue to exchange data in accordance with one or more Internet services. *See* §III.A.4; [1f]; SAMSUNG-1003, ¶158.

[2]

In ROMC, a device classifies “whether an application is running in the foreground or the background of the client 105,” as taught by Rao. SAMSUNG-1005, [0182], [0188]-[0189]; [1e]; SAMSUNG-1003, ¶¶159-160. Further, Rao describes that, in at least some cases, “an application [that] is running in the foreground [is] currently in active use by the user.” SAMSUNG-1005, [0003].

As also discussed in [1e], in ROMC, Oestvall describes that the device uses a “window server component 2 ... to determine if an application is in the background or foreground on display.” SAMSUNG-1005, [0008], [0016]-[0017], [0022]-[0023]; [1e]; SAMSUNG-1003, ¶163. Oestvall additionally describes that “[a] foreground application ... present[s] a user interface with which a user can interact.” SAMSUNG-1006, [0006].

Further, in ROMC, the device performs this classification upon generating and intercepting a network packet by the application to determine the priority of that network packet. [1f]-[1g]; SAMSUNG-1003, ¶161, ¶163.

Accordingly, a POSITA would have understood or found it obvious that, when the ROMC device classifies that “an application is running in the foreground

... of the client 105” (as taught by Rao) or “an application is in the ... foreground on display” (as taught by Oestvall), this classification would be performed based on the *current state* of the application (e.g., at the time that the packet was generated and intercepted by the ROMC system, such that the network packet can be accurately prioritized). SAMSUNG-1003, ¶162, ¶164. Specifically, this classification would be performed *when a user of the device is directly interacting with that application* (e.g., by engaging in “active use” of the application, as taught by Rao, or by interacting with a user interface of the application, as taught by Oestvall) and/or is *perceiving any benefit from that application* (e.g., by viewing the application as it is running in the foreground and/or perceiving that the application is ready for input by the user, as taught by Rao and Oestvall). SAMSUNG-1005, [0003]; SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶162, ¶164.

Further, techniques for adapting the prioritization for an application or otherwise impacts its operation based on the application’s direct user interaction were well-known by the Critical Date. SAMSUNG-1003 ¶¶165-166; SAMSUNG-1012, 9:33-35; SAMSUNG-1009, 10:16-44.

[4]

In ROMC, a device would apply *a differential traffic control policy* to the Internet service access request. [1f]; SAMSUNG, 1005, [0182]; SAMSUNG-1003, ¶167-168.

Further, Rao describes that a system can “provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies” (*a user interface ... to inform a user of the wireless end-user device when there are options to set, control, override, or modify service usage controls that affect the differential traffic control policy and/or the differential traffic control policy list*). SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶169.

A POSITA would have understood or found it obvious to implement Rao’s user interface to provide a user with a greater degree of control over the prioritization of network packets by the ROMC system. SAMSUNG-1003, ¶170.

[5], [6]

In view of Montemurro a POSITA would have found it obvious to configure the ROMC system such that it applies different “rules/policies” for controlling network traffic for different networks (*wherein the differential traffic control policy is part of a multimode profile having different policies for different networks [5]*). §III.A.4; [1f]; SAMSUNG-1003, ¶¶171-175.

As an example, in view of Montemurro, if a particular network (e.g., WWAN or WLAN) is selected from among multiple networks to transmit an application’s network traffic, a POSITA would have found it obvious to apply a policy specific to the first network to the network traffic during use of the first network by

the application (*select a traffic control policy from the multimode profile based at least in part on a network type of a network connection currently in use by the wireless end-user device [6]*) such that the network traffic is continuously or periodically provided to the appropriate set of queues and transmitted to the first network without delay. §III.A.4; SAMSUNG-1003, ¶¶176-179. This configuration would allow the system “to optimize communications for multi-mode capable devices” by accounting for “different radio access technologies,” as taught by Montemurro. SAMSUNG-1007, [0030]; SAMSUNG-1003, ¶175, ¶179.

[7]

In view of Montemurro a POSITA would have found it obvious to configure the ROMC system such that it applies different “rules/policies” for controlling network traffic for different networks (*multimode profile*). §III.A.4; [1f], [5], [6]; SAMSUNG-1003, ¶¶180-181.

Further, Montemurro teaches that when a device is connected to a WLAN (*when the network type of a network connection is at least one type of WLAN connection*), the device can select from among different policies or rules to control network traffic (*select a traffic control policy from the multimode profile based on a type of network connection from the WLAN to the Internet*). SAMSUNG-1003, ¶182.

For instance, Montemurro describes that when a device is connected to a

“WLAN,” the device can route network traffic differently across the WLAN and to the Internet depending on the time of day. SAMSUNG-1007, [0040]-[0040]; FIG.

3. Specifically, during work hours, “a virtual private network (VPN) connection is established via Internet 112 between the device 102 and an enterprise server” (a first *type of network connection from the WLAN to the Internet*). *Id.*, [0040]. In contrast, during non-work hours, “a SIP connection to the user's appropriate “home” server (e.g. a backend server 120 providing SIP services) is established for SIP services when the user is not working” (a second *type of network connection from the WLAN to the Internet*). *Id.*, [0041]. In doing so, the device would route network traffic differently (*select a traffic control policy from the multimode profile*) based at least in part on whether network traffic from the WLAN to the Internet is to be provided via a “VPN connection” or a “SIP connection” (...*based at least in part on a type of network connection from the WLAN to the Internet*). SAMSUNG-1003, ¶183.

This configuration would allow the system to intelligently route network traffic to an appropriate network (e.g., a work network or a home network) depending on the type of work that the user is likely to be performing at a given time. *Id.*, ¶184.

[8]

Upon selecting the WWAN (*when data for Internet service activities is*

classified as to be provided through the WWAN modem), the ROMC system

would, in at least some implementations, prioritize the application's network packets based on the specific application classification criteria taught by Rao and Oestvall. [1g]; SAMSUNG-1003, ¶¶185-186.

For example, the “filter 322” would selectively “allow” network packets (*apply the differential traffic control policy by allowing the Internet service access request*) from applications that are “trusted” (*...when the particular application is one of the second one or more applications*), even if those applications are running in the background (*...and the particular application is not classified as interacting with a user in the device user interface foreground*) (e.g., a classification of applications that should be assigned a higher priority, as taught by Oestvall). *See* §III.A.4; SAMSUNG-1003, ¶¶187-188. Accordingly, applications that are sufficiently important can continue to exchange data in accordance with one or more Internet services. *See* §III.A.4; [1f]; SAMSUNG-1003, ¶¶187-188.

[9]

Rao discloses a WWAN. [1a]; SAMSUNG-1003, ¶¶189-190.

Similarly, Montemurro also discloses a WWAN. SAMSUNG-1007, [0011], [0013], [0028]. Further, Montemurro discloses that, depending on the location, a network can be a “roaming” network. SAMSUNG-1007, [0029]; SAMSUNG-1003, ¶191.

In view of Montemurro, a POSITA would have understood that a WWAN network can include a portion that is a *home WWAN* (e.g., not “roaming”) and a portion that is a *roaming WWAN*, depending on the location. SAMSUNG-1003, ¶192.

The ROMC system includes *one or more processors configured to apply the differential traffic control policy* to an Internet service access request. [1c]; [1d]; [1f]; §III.A.3; SAMSUNG-1003, ¶193. Further, as modified by Montemurro, the ROMC system would selectively apply *the* differential traffic control policy depending on whether data communication for Internet service activities is provided by a roaming WWAN or a home WWAN. SAMSUNG-1003, ¶194.

Specifically, a POSITA would have found it obvious to modify Rao-Oestvall system to further consider the type of network(s) to which a device is connected and available for use by the device, as taught by Montemurro, to improve the prioritization of network traffic by the device, while also accounting for the characteristics of a network (e.g. the “bandwidth” of a network and/or the “cost” that is associated with using a network). §III.A.4; SAMSUNG-1008, [0030]; SAMSUNG-1003, ¶195.

In view of Montemurro, a POSITA would have applied different differential traffic control policies, depending on which network is selected to transmit an application’s network traffic. SAMSUNG-1003, ¶196. For instance, if a roaming

WWAN were selected from among multiple networks to transmit an application's network traffic, a POSITA would have found it obvious to apply a first policy specific to the roaming WWAN (e.g., ***the differential traffic control policy***, as introduced in [1f]), such as by selectively placing network packets in a set of queues that are specific to the roaming WWAN. *Id.*, ¶196.

Further, if a home WWAN is selected from among multiple networks to transmit an application's network traffic instead, a POSITA would have found it obvious to apply a second, ***different*** policy specific to the home WAN network (i.e., ***not apply the differential traffic control policy, and instead apply a different differential traffic control policy***), such as by selectively placing network packets in a set of queues that are specific to the home WWAN. *Id.*, ¶197. That is, a second and ***different*** policy would be applied at least because the second policy selectively places network packets in a different set of queues compared to the first policy. *Id.* Accordingly, a particular differential traffic control policy would be ***applied to one of but not both of a WWAN modem connection to a roaming WWAN network and a WWAN modem connection to a home WWAN network***. *Id.*

[14]

In ROMC, a device would apply ***the differential traffic control policy*** to the Internet service access request. [1f]; SAMSUNG-1003, ¶¶198-199.

Further, Rao describes that policies “may be provided by or downloaded via

a gateway.” SAMSUNG-1005, [0183]. In view of Rao, POSITA would have understood or found it obvious that a device can specify at least some of its policies, such as adding new policies (*update the differential traffic control policy and/or the differential traffic control policy list*), by downloading and implementing policies from a gateway (*...based on information received from a network element*) to allow for centralized control and/or remote administration of multiple devices in prioritizing network packets, and/or to allow devices to maintain up-to-date policies with which to prioritize network packets. SAMSUNG-1003, ¶¶200-201.

[16]

The ROMC device will *selectively block the Internet service access request* in a first state of the first and second classifications. [1f]-[1g]; SAMSUNG-1003, ¶¶202-203.

Further, Rao describes that the device includes a “network stack 310” that “include[s] one or more network drivers.” SAMSUNG-1005, [0100], FIG. 1C. Further, Rao describes that network packets can be communicated “via a secure socket layer.” SAMSUNG-1005, [0035].

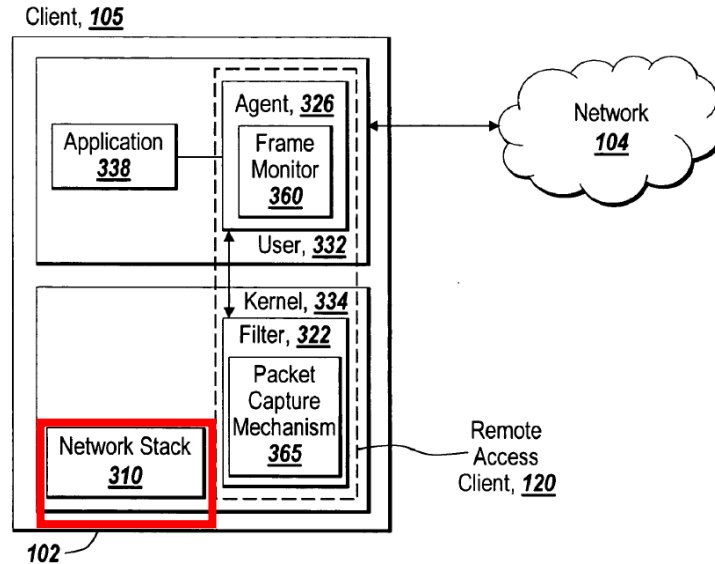


Fig. 1C

SAMSUNG-1005, FIG. 5A (annotated)

Rao teaches that the device “may intercept network packets of one or more applications 338 a-338 n transparently to the application 338 a-338 n ... and any of the network layers of a network stack,” which allows the prioritization technique to “support any type of application 338 a-338 n on the client 105.” SAMSUNG-1005, [0185].

In view of Rao, a POSITA would have understood or found it obvious that the ROMC device enables applications to transmit network packets to a remote server on the Internet by transmitting requests to a network stack, and that such requests could include requests to the network stack to open, connect to, and/or write data to a socket (e.g., using the “secure socket layer”) (*open, connect, and/or write*

requests by the particular application to a network stack). SAMSUNG-1003, ¶¶204-206. Further, in view of Rao, a POSITA would have understood or found it obvious to selectively block such requests to the network stack (*selectively block the Internet service access request by intercepting open, connect, and/or write requests by the particular application to a network stack*) to enable Rao's prioritization technique to "support any type of application" on a device, as taught by Rao. *Id.*, ¶¶204-206.

[19]

In ROMC, the device classifies "whether an application is running in the foreground or the background of the client 105," as taught by Rao. SAMSUNG-1005, [0182], [0188]-[0189]; [1e]; SAMSUNG-1003, ¶¶207-208.

Further, Oestvall describes that an application's user interface can have a different *state of user interface priority*, depending on whether it is in the foreground or the background. SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶¶209-212. For instance, when the application is in the background, the user interface has a low state of priority, such that the user interface is relegated to "an icon indicating [the application's] presence and the fact that it was still active." SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶209. Further, when the application is in the foreground, the user interface has a high state of priority, such that the user inter-

face is presented to the user for interaction. SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶210.

A POSITA would have understood or found it obvious that, when the ROMC device classifies “whether an application is running in the foreground or the background of the client 105,” this classification could be efficiently implemented *based on a state of a user interface priority of that application* (e.g., by assessing the state of the user interface priority for the application, such as whether the application’s user interface is visible, is available for interaction with a user, and/or is merely represented by an icon, as taught by Oestvall). SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶211. Moreover, the use of states of user interface priority in coordinating application operation was well known before the Critical Date and a POSITA would have found obvious the use of states of user interface priority for classification in Rao-Oestvall. SAMSUNG-1003, ¶212; SAMSUNG-1012, 9:19-35).

[20]

A POSITA would have found it obvious to modify Rao’s system of prioritizing network packets based on the specific application classification criteria taught by Oestvall and the network criteria taught by Montemurro. §III.A.4; [1g]; [8]; SAMSUNG-1003, ¶¶213-214. Specifically, a POSITA would have found it obvious to modify Rao’s system to prioritize network packets (provide a *differential*

network access control) for “untrusted” applications (*first one or more applications*) by blocking the applications’ attempt to access a WWAN when the applications are running the background. See [1g]; SAMSUNG-1003, ¶214. Further, a POSITA would have found it obvious to modify Rao’s system to prioritize network packets (provide a *differential network access control*) for “trusted” applications (*second one or more applications*) by allowing the applications to access a WWAN instead. See [8]; SAMSUNG-1003, ¶214. Accordingly, the “trusted” applications (*second one or more applications*) would *not be subject to a differential network access control* that is applicable to the “untrusted” applications (*first one or more applications*). SAMSUNG-1003, ¶214

[23]

The ROMC system can include “trusted” applications (*second one or more applications*). [1e]; SAMSUNG-1003, ¶¶215-216. Further, as described by both Rao and Oestvall, an application can provide services in the foreground. SAMSUNG-1003, ¶¶216-218.

For example, Rao describes that applications can request access to Internet services. SAMSUNG-1005, [0090]. Further, Rao describes that an application may be “running in the foreground” (*...comprising foreground services*). SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶217. See also SAMSUNG-1005, [0188]-[0189].

Similarly, Oestvall describes that application can interact with users in the foreground by “present[ing] a user interface with which a user can interact” to allow users to engage in Internet activities (...*comprising foreground services*). SAMSUNG-1006, [0006]; SAMSUNG-1003, ¶218.

[26]

The ROMC system would allow the Internet service access request under at least one different state of the first and second classifications. §III.A.4; [1h]; SAMSUNG-1003, ¶¶219-220.

Specifically the ROMC system would allow network packets when the application is “untrusted” and selected for WWAN communications (*the at least one different classification state comprises a state wherein data for Internet service activities is classified as to be provided through the WWAN modem*) and in the foreground (...*and the particular application is classified as interacting with a user in the device user interface foreground*). [1h]; SAMSUNG-1003, ¶221.

B. [GROUND 2] – Claims 10-12, 15, 17, 18, 22, and 25 are rendered obvious by Rao, Oestvall, Montemurro, and Araujo

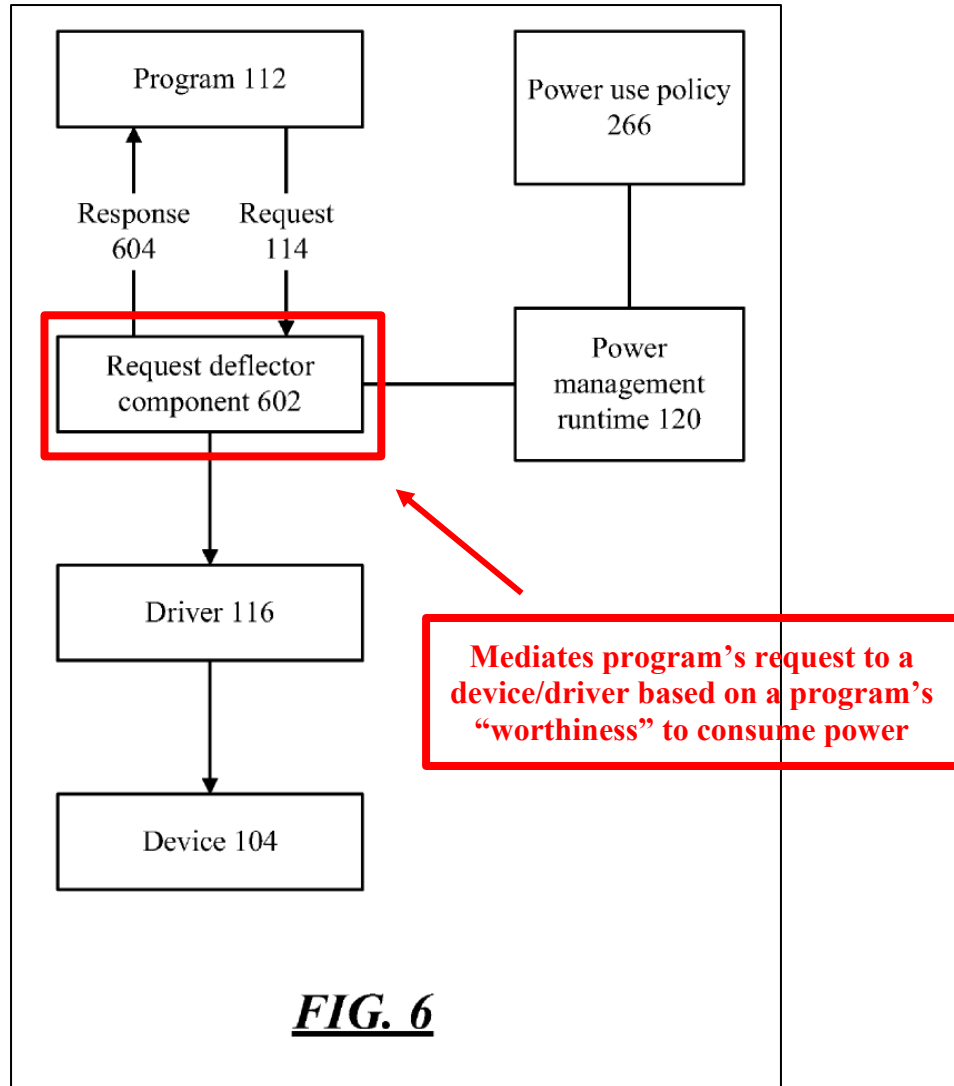
1. Overview of Araujo

Araujo describes “a power-management policy” for managing a “machine's power usage.” SAMSUNG-1008, Abstract; SAMSUNG-1003, ¶¶222-226.

Araujo’s device determines “[w]hether a program is permitted to consume power

... based on a finding as to whether the program's status justifies the consumption of power under the circumstances that are present.” SAMSUNG-1008, [0027].

For example, each program can generate “a request to perform an action using a particular device, such as “a request to send data over a wireless network” using a “wireless network card.” *Id.*, [0020], [0024]. Further, a “request deflector component” “intercepts requests and responds to the requests based on power management considerations before the request reach[es] a device driver.” *Id.*, [0024], [0050]. If “[a] request 114 may be carried out under [a] power policy, then request deflector component 602 passes the request along to driver 116. Otherwise, request deflector component deflects the request from reaching driver 116.” *Id.*



SAMSUNG-1008, FIG. 6 (annotated)

2. Combination of Rao-Oestvall-Montemurro and Araujo

A POSITA would have found it obvious to modify the ROMC system to include Araujo’s “request deflector component” to allow the ROMC system to better “use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.” SAMSUNG-1008, [0001]; SAMSUNG-1003, ¶¶227-231; §III.B.1. This modification would have involved (1) combining

prior art elements according to known methods to yield predictable results; and (2) use of a known technique to improve similar devices (methods, or products) in the same way. *See KSR Int'l Co.*, 550 U.S. and 415-421; MPEP 2143; SAMSUNG-1003, ¶¶227-231.

The ROMC system controls each of the applications' access to the network by intercepting packets of network traffic by the applications, determining the priority of the packets based on the application that is associated with each packet, and selectively communicating the packets to the network based on the determined priority. §III.A.3-4. As taught by Rao, these operations can be performed, at least in part, by one or more “network drivers of a network stack 310.” SAMSUNG-1005, [0100]. As an example, the ROMC system can include “[a] filter 322 [to] place, arrange, or coordinate network packets into queues 540 a-540 n in support of the priorities,” and these “queues 540 a-540 n may be included in a network driver, such as an NDIS driver for the filter 322.” *Id.*, [0143], [0180], [0191].

In view of Araujo, a POSITA would have understood that an application's request to the network driver (e.g., including network packets for transmission to a network) can be intercepted and mediated by a “request deflector component” that is “interposed” between each application and the network driver to selectively allow or block an application from transmitting data to the network based on whether

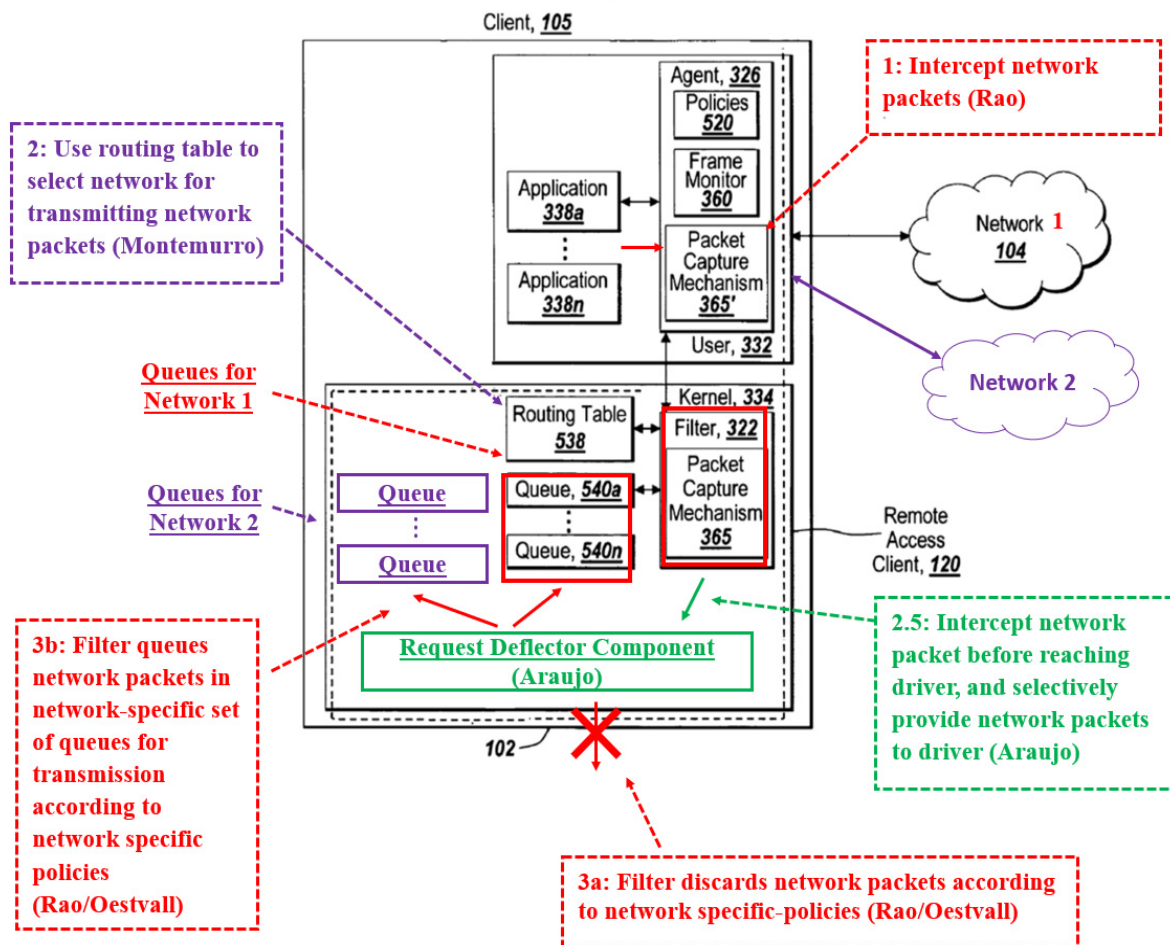
the application has a “status [that] justifies the consumption of power under the circumstances that are present.” SAMSUNG-1008, [0024], [0027], [0050]; SAMSUNG-1003, ¶¶228-229.

For instance, a POSITA would have “interposed” Araujo’s “request deflector component” between the ROMC’s applications and the network driver(s) (i.e., including the queues 540a-540n) to process network packets subsequent to the selection of a network by the routing table 538 (e.g., based on Montemurro’s criteria). SAMSUNG-1003, ¶¶230-231.

Further, a POSITA would have configured the “request deflector component” to determine whether each of the applications has a “status [that] justifies the consumption of power under the circumstances that are present,” and selectively allow or block the request and, hence, the network packets from proceeding to the network driver for communicating with the selected network based on the determination (see step 2.5 below). *Id.*, Upon determining that the application’s status justifies the consumption of power, the “request deflector component” can allow the request, and hence, the network packets to proceed to the appropriate network driver and be prioritized according to the Rao-Oestvall combination (see steps 3a and 3b below). *Id.* Alternatively, upon determining that the application’s status does not justify the consumption of power, the “request deflector component” can block the request and, hence, the network packets from reaching the network

driver. *Id.* Accordingly, the “request deflector component” would provide an additional layer of control for regulating each of the applications’ access to the network (e.g., to supplement the functionality taught by Rao, Oestvall, and Montemurro). *Id.*

An example modification to the Rao-Oestvall-Montemurro system in view of Araujo’s teachings (“Rao-Oestvall- Montemurro-Araujo,” ROMAC) is shown below.



Rao’s FIG. 5A (revised and annotated)

3. Analysis

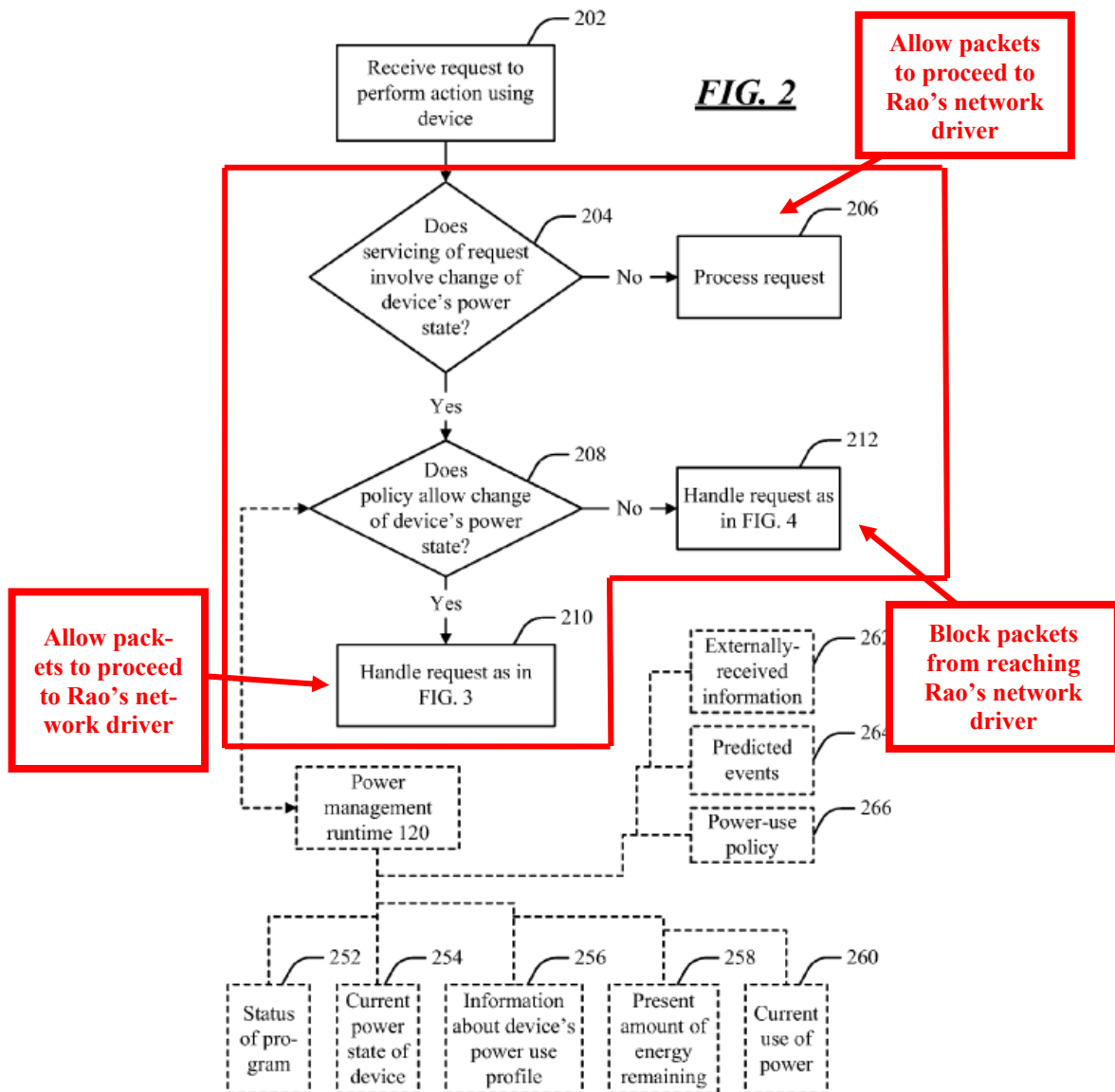
[10], [12]

The ROMAC system would use a network driver to apply *a differential traffic control policy* to the Internet service access request. [1f]; §III.B.2; SAMSUNG-1003, ¶¶232-233.

Further, as modified by Araujo, the ROMAC system would selectively allow network packets to proceed to the network driver for prioritization (*dynamically change the application of the differential traffic control policy*) depending on whether an application has a “status [that] justifies the consumption of power under the circumstances that are present.” SAMSUNG-1008, [0027]; §III.B.2; SAMSUNG-1003, ¶¶234-235. In the example configuration of the ROMAC shown in §III.B.2, the ROMAC system would determine whether to allow an application’s request to proceed to the network driver based on a device’s power state, such as the power state of the device’s network card or modem (*...based on a power state of the device [10]*). SAMSUNG-1008, FIG. 2 (204), [0025]; SAMSUNG-1003, ¶236. Specifically, the ROMAC system would determine whether a device’s components “may already be powered on and/or in an appropriate power state” to better regulate power consumption by the device. SAMSUNG-1008, [0037]. For example, if a device’s network card or modem are already powered on and/or is “in an appropriate power state,” the ROMAC system determines that an application’s

use of those components “does not affect power management,” and selectively allows the application’s network packets to proceed to the network driver to service the application’s request. *Id.*; SAMSUNG-1003, ¶236.

Specifically, the ROMAC system would determine whether to allow an application’s request to proceed to the network driver based on power control state changes for a device, such as a network card or modem (*...based on power control state changes for one or more of the modems [12]*). SAMSUNG-1003, ¶237. For example, as shown in FIG. 2, if servicing the application’s request would not involve a change in the power state of the device’s components, the ROMAC system would process the request and “proceed[s] as normal.” SAMSUNG-1008, FIG. 2 (206), [0025]. Accordingly, the network packets representing the request would be forwarded to the network driver for prioritization. SAMSUNG-1003, ¶237. Otherwise, the ROMAC system determines whether a policy would allow a change of the device’s power state, and selectively (i) allows the request and transmits the network packets to the network driver (e.g., as shown in FIG. 3) (SAMSUNG-1008, FIG. 2 (210), FIG. 3, [0035]), or (ii) blocks the network packets from reaching the network driver, either permanently or temporarily (e.g., as shown in FIG. 4) (*id.*, FIG. 2 (212), FIG. 4, [0035]). SAMSUNG-1003, ¶237.



SAMSUNG-1008, FIG. 2 (annotated)

[11]

The ROMAC system would selectively allow network packets to proceed to a network driver for prioritization (*dynamically change the application of the differential traffic control policy*). §III.B.2; [1f]; [10], [12]; SAMSUNG-1003, ¶¶238-239.

Specifically, as modified by Araujo, the ROMAC system would determine whether to allow an application's request to proceed to the network driver based on *a device usage state*, such as:

- (i) the “[s]tatus of program” that is being used by a user,,
- (ii) the “[c]urrent power state of the device,” and/or
- (iii) “[p]resent use of power” by the device. SAMSUNG-1008, [0027]-[0028], [0031], FIG. 2; SAMSUNG-1003, ¶240.

As Araujo explains, each of these factors reflects an application's “worthiness to consume power” in a given situation. SAMSUNG-1008, [0027]. Accordingly, based on these factors, the ROMAC system can better “use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.” *Id.*, [0001]; SAMSUNG-1003, ¶241.

[15]

Araujo describes that “if a power state change is not allowable under a policy,” the system can generate “a dialog box ... on a display that informs the person

in front of the display that the card is off.” SAMSUNG-1008, [0041]; SAMSUNG-1003, ¶¶242-243.

In view of Araujo, a POSITA would have understood or found it obvious that a system can present information to a user regarding a blocked Internet service access request, thereby modifying and/or replacing what was previously displayed and/or would have been displayed on the user interface (*block, modify, remove, or replace user interface messages generated by the particular application based on the applied differential traffic control policy*). SAMSUNG-1003, ¶¶244-245.

This would allow the system to alert the user to changes in the operation of the device, as taught by Araujo. *Id.*

Further, in view of Araujo, a POSITA would have understood that this functionality can be provided, at least in part, using “[s]oftware ... stored in [a] data remembrance component(s) 704)” and “execute[d] on ... one or more processor(s) 702) (*agent*). SAMSUNG-1008, [0055]; SAMSUNG-1003, ¶246.

[17]

The ROMAC system would include Araujo “request deflector component” to “intercept[] requests and respond[] to the requests based on power management considerations before the request reach[es] a device driver.” §III.B.2; SAMSUNG-1008, [0024], [0050]; SAMSUNG-1003, ¶¶247-248.

Specifically, Araujo explains that “if the power state change is not allowable

under the policy,” the device can “block the request” and “notif[y] [the program] that the request will not be processed.” SAMSUNG-1008, [0038], [0041]. Further, “[t]he program may also be notified that the reason for the request is that the device is off. For example, the program may receive an error code or result code indicating that the request calls for a device that is not turned on.” *Id.*, *See also id.*, [0017].

In view of Araujo, a POSITA would have understood or found it obvious that a system can respond to an intercepted request by a particular application by notifying the application that the request will not be processed and/or transmitting an error code or result code to the application (*respond to an intercepted request by the particular application*). SAMSUNG-1003, ¶¶249-250. In doing so, the system would provide an application with feedback regarding its attempt to access a network, as taught by Araujo. *Id.*,

Further, a POSITA would have found it obvious to notify the application by emulating conventional network messages, such as those generated by an Application Programming Interface (API) for facilitating network access for applications (*...by emulating network messaging*), as doing so would provide functionality in a manner that is transparent to the application, thereby providing support for any type of application (e.g., as taught by Rao). SAMSUNG-1003, ¶¶251-254. *See also* SAMSUNG-1013, 1-20.

Araujo's use of an "error code or result code" is also consistent with the specification of the '445 Patent, which describes that "an emulated network API" can block an application's connection attempt and send "a message ... back to the application" regarding the blocking, such as a "message that the application will understand and can interpret to indicate that the network access attempt was not allowed/blocked, that the network is not available, and/or to try again later for the requested network access." SAMSUNG-1001, 91:25-49; SAMSUNG-1003, ¶255.

[18]

The ROMAC system would notify an application that a request will not be processed and/or transmit an error code or result code to the application by emulating conventional network messages (*emulating network messaging*). [17]; SAMSUNG-1003, ¶¶256-257.

A POSITA would have understood or recognized that, in blocking the request from reaching the network driver, the ROMAC system would block the request from passing to Rao's "network stack" (which includes "one or more network drivers" supporting the network stack) (*responding to a network request from the particular application by blocking the request from passing to a network stack*). SAMSUNG-1005, [0100]; SAMSUNG-1003, ¶258.

Further, a POSITA would have understood or recognized that, in notifying an application that a request will not be processed and/or transmitting an error code

or result code to the application, the ROFAC would *return to the particular application a message indicating the network request was not successful*. SAMSUNG-1008, [0038], [0041]; SAMSUNG-1003, ¶259. *See also* SAMSUNG-1008, [0017].

[22]

As taught by Montemurro, a system includes various applications, functions, or processors, such as (i) “[o]perating system software” (*operating system application, utilities, functions, or processes*), (ii) “predetermined set of applications that control basic device operations, including at least data and voice communication applications, will normally be installed on handheld device 600 during its manufacture” (*system applications, utilities, functions, or processes*), and (ii) “[a]dditional applications ... installed by a user” (*user applications*), each of which provides different respective functionality. SAMSUNG-1007, [0055]-[0057].

In view of Montemurro, a POSITA would have understood or recognized that the ROMAC system would differentiate between these types of applications, functions, or processes (*classify between* these types of applications, functions, or processes) such that they are executed by the processor(s) in the correct mode (e.g., kernel mode vs. user mode), which was well known by the Critical Date. SAMSUNG-1014, 22-35; SAMSUNG-1003, ¶¶260-263.

[25]

If servicing a request would involve a change in the power state of a device (e.g., a network card or modem), the ROMAC system determines whether a policy would allow changing the power state. [10]; SAMSUNG-1008, FIG. 2 (210), FIG. 3, [0035]. If a change is not allowed, the ROMAC system would block the network packets from reaching the network driver (e.g., as shown in FIG. 4). *Id.*, FIG. 2 (212), FIG. 4, [0035]; SAMSUNG-1003, ¶¶264-265. Accordingly, the power state of the network card or modem would remain unchanged (*prevent ... applications from changing the power state of the modem*). *Id.*

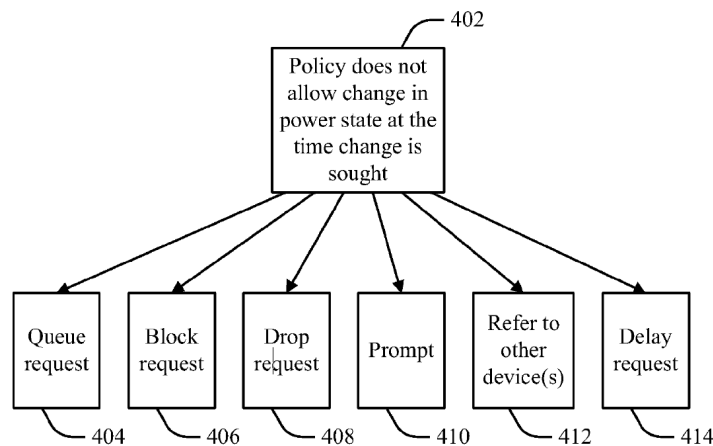


FIG. 4

SAMSUNG-1008, FIG. 4

Further, Araujo teaches that a device can selectively allow a program's request depending on whether the program is sufficiently important to consume resources. §III.B.1; SAMSUNG-1008, [0024], [0050]; SAMSUNG-1003, ¶266. Further, Oestvall teaches that certain applications (e.g., "trusted" applications)

(*second one or more applications*) are more important than other applications (e.g., “untrusted” applications) (*first one or more applications*) and should be given preferential treatment by a device. §III.A.2; §III.A.4; SAMSUNG-1006, [0010]-[0017], [0021]-[0025]; SAMSUNG-1003, ¶266.

In view of Araujo and Oestvall, a POSITA would have found it obvious to allow “trusted” applications to change the power state of the modem (*not prevent the second one or more applications from changing the power state of the modem*), while not allowing “untrusted” applications to change the power state of the modem (e.g., when they are running in the background) (*prevent the first one or more applications from changing the power state of the modem*). SAMSUNG-1003, ¶267. Accordingly, the ROMAC system can better “use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.” SAMSUNG-1008, [0001]; SAMSUNG-1003, ¶267.

C. [GROUND 3] – Claims 3, 13, 21, and 24 are rendered obvious by Rao, Oestvall, Montemurro, and Freund

1. Overview of Freund

Freund describes “[a] computing environment with methods for monitoring access to an open network, such as WAN or the Internet.” SAMSUNG-1009, Abstract; SAMSUNG-1003, ¶¶268-273. Freund’s system includes “a client-side monitoring component for monitoring Internet access” (“Client Monitor”) and a “supervisor 323 [that] directs runtime monitoring operations.” SAMSUNG-1009,

3:50-4:4, 14:62-67, 14:51-62, FIG. 3A (310a-310c). Freund's system "monitor[s] and regulate[s] Internet access on a per application basis," and "specif[ies] which applications can (and cannot) access the Internet." *Id.*, 10:44-50.

For instance, Freund's system "allows user (e.g., administrator) configuration of rules which govern use of the protocols monitored by the system." SAMSUNG-1009, 23:65-27:50. Rules can be specified based on various criteria, such as the "particular application" that is being used, and can be "time-based in nature." *Id.*, 23:65-24:15.

Further, Freund's system can "monitor[] access to the Internet by individual applications ... to not only track Internet traffic but also [to] determine in many cases data exchanged on a per application basis." *Id.*, 11:10-15. As Freund teaches, "this system can "avert ... [i]nadvertent disruptions of the network by individual users, such as bandwidth hording [sic] by a user using RealAudio for listening to a Web audio 'broadcast.'" *Id.*, 11:21-28.

2. Combination of Rao-Oestvall-Montemurro and Freund

In view of Freund, a POSITA would have found it obvious to modify the ROMC system to regulate an application's access to a network based on time-based criteria and/or the amount of network data that has been used by that application. SAMSUNG-1003, ¶¶274-279; §III.C.1. Combining ROMC with Freund

would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of a known technique to improve similar devices (methods, or products) in the same way. *See KSR Int'l Co.*, 550 U.S. and 415-421; MPEP 2143; SAMSUNG-1003, ¶¶274-279.

Specifically, a POSITA would have recognized that, like the ROMC system, Freund's system is configured to control an application's access to a network to preserve limited system resources. SAMSUNG-1009, 11:19-28; SAMSUNG-1003, ¶275. Further, a POSITA would have recognized that Freund describes specifying techniques for regulating an application's access to a network based on both (i) time-based criteria and (ii) a "bandwidth and interactive use monitoring" technique for selectively blocking an application's request to access a network to achieve a specific technical benefit (e.g., to "avert ... [i]nadvertent disruptions of the network by individual users, such as bandwidth hording [sic] by a user"). SAMSUNG-1009, 11:19-28; SAMSUNG-1003, ¶275.

In view of Freund, a POSITA would have found it obvious to modify the ROMC system to allow users to control an application's access to a network based on time-based criteria (e.g., to "monitor and regulate the amount of time employees spend on the Internet"), such as by "specify[ing] the start date and expiration date (if any)" for a rule and/or "particular time intervals (e.g., during weekdays and/or

during weekends) when the rule is enforced.” SAMSUNG-1009, 9:65-10:1; SAMSUNG-1003, ¶276.

Further, in view of Freund, a POSITA would have found it obvious to modify the ROMC system to additionally include Freund’s “bandwidth and interactive use monitoring” to prevent an application from hoarding the bandwidth of a network. SAMSUNG-1008, 11: 19-28; SAMSUNG-1003, ¶¶277-279.

3. Analysis

[3]

Rao describes that a system can “provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies.” [4]; SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶¶280-281.

Similarly, Freund describes a “rule wizard interface” that “allows user (e.g., administrator) configuration of rules which govern use of the protocols monitored by the system” through a graphical user interface, such as by selecting which applications are affected by each rule. SAMSUNG-1009, 24:16-27:50, 25:20-33, FIG. 7D.

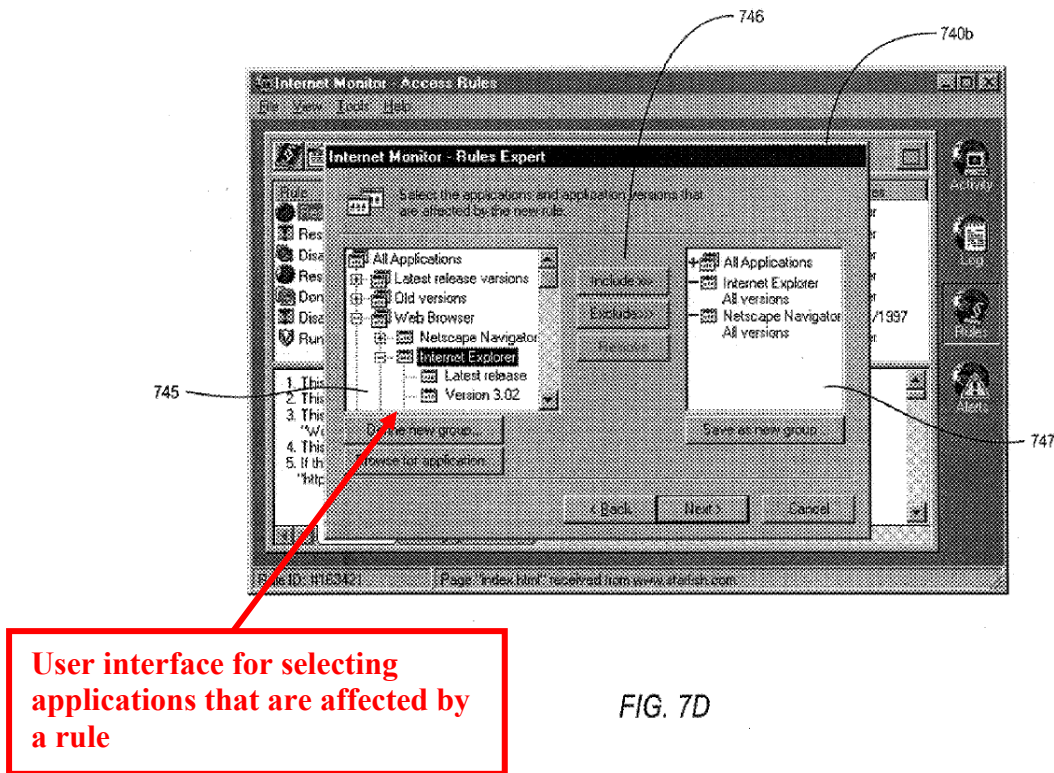


FIG. 7D

SAMSUNG-1009, FIG. 7D

In view of Rao and Freund, a POSITA would have understood or found it obvious to implement a user interface to *provide the user of the device with information regarding why the differential traffic control policy is applied to the particular end-user application* (e.g., by providing the user with detailed information regarding each of the policies). SAMSUNG-1003, ¶¶281-283.

[13], [24]

In view of Freund, a POSITA would have found it obvious to modify the ROMC system to regulate an application's access to a network based on time-based criteria, such as by blocking certain applications from accessing a network

during certain times of day. §III.B.1-2; SAMSUNG-1009, 27:-4-16 (“This allows an administrator, for instance, to specify that a rule blocking a RealAudio application remains in force during working hours on weekdays-that is, at times when network traffic is already congested.”); SAMSUNG-1003, ¶¶284-285.

Specifically, a POSITA would have found it obvious to configure a rule or policy (*the differential traffic control policy*) such that at least some of applications (*...defines that the first one or more applications*) can access a particular network only during certain times of the day (*...can only have WWAN network access events during particular time windows [10]*). SAMSUNG-1003, ¶286. Accordingly, Internet service access requests occurring outside of the specified times would be blocked (*wherein block comprises intermittently block when the Internet service access request occurs during selected time windows [24]*). *Id.*

A POSITA would have recognized that time-based limitations allow the device to reduce network usage during specific times in which “network traffic is already congested,” thereby improving the performance of the network. SAMSUNG-1003, ¶287.

[21]

In view of Freund, a POSITA would have found it obvious to modify the ROMC system to monitor the amount of network data that has been used by each application individually. §III.C.2; SAMSUNG-1003, ¶¶288-289.

For example, a POSITA would have configured a “Client Monitor” to:

- (i) Intercept an application’s requests to access the Internet (e.g., “Winsock ... calls” to a “communications driver”) (SAMSUNG-1009, 29:17-30:9, FIG. 13A (1301)),
- (ii) Track the amount of Internet data that is transmitted and/or received by that application (e.g., “[a]dd[ing] the data lengths to a DataIn or DataOut accumulator or counter of the Application's list entry and global activity record”) (determine that *Internet service activity usage by an third application*), (SAMSUNG-1007, 30:24-29, FIG. 13A (1302(D))), and
- (iii) “[D]isable[] future Internet access” by that application if the amount of data exceeds a particular application-specific limitation (e.g., “[i]f the DataIn or DataOut fields exceed rule-based quantity either for the specific Application”) (...*exceeds a data usage threshold.*) (SAMSUNG-1007, 30:24-29, FIG. 13A). SAMSUNG-1003, ¶290.

Further, Freund’s “Client Monitor” “maintain[s] a detailed log of access related activities,” and provides the log to a “Supervisor” implemented on a remote server. *Id.*, 4:29-32; 4:51-63; 28:24-28; 28:51-53. In view of Freund, a POSITA would have found it obvious to report an application exceeding the data usage

threshold (*report the activity usage*) to a remote “Supervisor” (*...to network element when Internet service activity usage by the third application exceeds a data usage threshold*) in order to “facilitat[e] administration needs.” *Id.*; SAMSUNG-1003, ¶291.

Further, a POSITA would have understood or recognized that Freund’s “bandwidth and interactive use monitoring” technique could be applied to any of the applications that are running on the device, and thus would have applied this technique to any of the applications that are running on the ROMFC system. *Id.*, ¶292.

As an example, a POSITA would have recognized that (i) “trusted” applications and “untrusted” applications (e.g., as described by Oestvall) could be further differentiated based on additional criteria, such as “the type of one or more protocols used by the application[s]” and “the size of the payload of the network packet,” and (ii) the applications could be prioritized differently based on these criteria (e.g., as taught by Rao). *Id.*, ¶293. For instance, a POSITA would have recognized that “trusted” applications may be instead categorized into at least two different categories of applications, including a higher priority category (*second one or more applications*) and a lower priority category (and *a third application that is neither one of the first one or more applications nor one of the second one or more applications*) in accordance with Rao’s criteria. *Id.* However, regardless of

each application's categorization, a POSITA would have been motivated to apply Freund's technique to track the network usage of each of the applications individually to obtain more granular data regarding each application's data usage. *Id.*

D. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

1. 35 U.S.C. §325(d) – Discretionary Denial under 325(d) is not warranted

Discretionary denial under the Board's §325(d) *Advanced Bionics* analysis is not warranted. *See Advanced Bionics, LLC v. Med-El Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, 8-9 (PTAB Feb. 13, 2020) (precedential) ("*Advanced Bionics*").

None of the prior art references advanced in this Petition was previously before the Office. While a relative of Rao (PCT application WO 2006/012610A2 ("Rao-2")) was cited on the face of the '445 Patent, there is no evidence that the Office substantively considered this reference among the references listed on the first 11 pages of the '445 Patent. *See, generally*, SAMSUNG-1002. Moreover, the same or substantially the same arguments were not previously presented to the Office. *Id.* Indeed, there could be no overlap between the arguments made before the Office because the Examiner issued no prior art rejections during prosecution.

To the extent it is argued that the same or substantially the same art or arguments were previously presented to the Office, the second prong is not met. *Advanced Bionics*, 8-10. The Examiner issued no prior art rejections and included no substantive discussion of any prior art reference. *See, generally*, SAMSUNG-1002. Therefore, although Rao-2 was cited on the face of the '445 Patent, neither Rao nor Rao-2 nor the obviousness of the Challenged Claims in view of those references was ever addressed during prosecution. As highlighted in Grounds 1 and 2, the Examiner clearly did not appreciate Rao's disclosures and how those references in combination and in combination with other prior art references not previously before the Office (Oestvall, Montemurro, Araujo, and Freund) render the Challenged Claims obvious. Moreover, Petitioner has shown a reasonable likelihood that it would prevail that at least one of the Challenged Claims is unpatentable over the applied art based on the current record. *Supra* §III A-E; *see Tokyo Ohka Kogyo Co., Ltd. v. Fujifilm Elec. Materials U.S.A., Inc.*, PGR2022-00010, Paper 9, 8-9 (PTAB June 6, 2022). As such, Petitioner has demonstrated material error by the Office, and discretionary denial is not warranted.

2. 35 U.S.C. §314(a) – Discretionary Denial is not Merited in view of Petitioner's *Sotera* Stipulation

In *Apple Inc. v. Fintiv, Inc.*, the Board enumerated six factors to determine whether a petition should be discretionarily denied institution under §314(a). IPR2020-00019, Paper 11 at 2-3 (PTAB "precedential" Mar. 20, 2020) ("*Fintiv*").

In June 2022, the USPTO issued updated discretionary denial guidance in view of the *Fintiv* factors and expressly noted that ***the PTAB will not discretionarily deny institution if Petitioner presents a Sotera stipulation.*** SAMSUNG-1015, 3, 7-8. Here, Petitioner has eliminated any risk of duplicated effort by voluntarily presenting a *Sotera* stipulation to Patent Owner. SAMSUNG-1016; *Sotera Wireless, Inc. v. Masimo Corp.*, Case IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020). For at least this reason, the Board should not discretionarily deny this petition.

Although the Board need not address additional *Fintiv* factor considerations in light of Samsung's *Sotera* stipulation, indeed, the *Fintiv* factors do not favor denial.

Factor 1 is neutral because neither party has requested a stay in co-pending litigation.

Factor 2 is neutral because the Court's trial date is speculative at this point and subject to change. The Board will likely issue its Final Written Decision around March 2025, approximately seven months after the currently scheduled trial date (August 5, 2024). SAMSUNG-1018, 1. However, as the Board and Director have previously recognized, "scheduled trial dates are unreliable and often change." SAMSUNG-1015, 8.

Factor 3 also favors institution because Petitioner has diligently filed this Petition months ahead of the one-year time bar, while the EDTX Litigation is still

in its early stages. Beyond exchanging preliminary infringement/invalidity contentions, the parties and the District Court have yet to expend significant resources on invalidity. SAMSUNG-1018, 5.

Factor 4 also favors institution because Petitioner has provided a *Sotera* stipulation. SAMSUNG-1016.

Factor 5: The parties in the parallel EDTX litigation are the same.

Factor 6 favors institution because the merits of this Petition are compelling.

IV. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Petitioner authorizes charge of fees to Deposit Account 06-1050.

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

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

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Samsung”) are the real parties-in-interest.

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

The ’445 Patent is the subject of a civil action, *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:22-cv-00422, E.D. Tex., filed October 26, 2022 (SAMSUNG-1004). Petitioner and Headwater are also involved in case nos. 2:22-cv-00467 and 2:23-cv-00103, also in E.D. Tex.

Petitioner is not aware of any other disclaimers, reexamination certificates, or IPR petitions addressing the ’445 Patent.

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

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR39843-0162IP1@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Roberto Devoto, Reg. No. 55,108 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above.

Petitioner consents to electronic service by email at IPR39843-0162IP1@fr.com

(referencing No. 39843-0162IP1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, jjm@fr.com, and devoto@fr.com).

Respectfully submitted,

Dated 9-28-23

/Roberto J. Devoto/
W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Roberto Devoto Reg. No. 55,108
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2023-01462)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,940 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated 9-28-23

/ Roberto J. Devoto /
W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Roberto Devoto Reg. No. 55,108
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on September 28, 2023, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

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

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667