

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
Petitioner,

v.

HEADWATER RESEARCH LLC,
Patent Owner.

IPR2023-01337
Patent 9,521,578

PATENT OWNER'S RESPONSE TO THE PETITION

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Background.....	2
	A. Overview of the '578 Patent.....	2
III.	Level of Ordinary Skill in the Art.....	4
IV.	Claim Construction	5
V.	The Petition does not demonstrate that its proposed combination discloses or renders obvious a “differential traffic control policy” meeting all of the claim 1 requirements.....	6
	A. Rao’s prioritization scheme relied on by the Petition does not disclose a “differential traffic control policy” such that any applications are only allowed to access the WWAN when they are classified as interacting in the foreground.	10
	B. Oestvall (alone or in combination with Rao) does not cure the deficiencies of Rao discussed above.....	15
	1. Oestvall does not disclose a “differential traffic control policy” applicable to WWAN but not WLAN.	16
	2. The Petition provides no explanation of how any differential traffic control policy of Rao or Montemurro would be modified in view of Oestvall to meet all claim requirements.	19
	3. The Petition provides no motivation to allow a user to select which applications should be classified as “untrusted.”	22
VI.	The Petition does not show that its combination discloses or renders obvious claim element [1e].	25
	A. The Petition’s reliance on Rao alone does not satisfy limitation [1e].	26
	1. The Petition’s Rao-based theory requires the remote access client being included within a particular application—one that is governed by the differential traffic control policy.	26

2.	The Petition’s Rao-based theory relies on Rao’s inclusion of a remote access client within a particular application, but Rao does not teach any particular configuration and the Petition does not motivate any particular configuration.....	28
3.	The Petition fails to motivate inclusion of Rao’s remote access client within an application subject to any differential traffic control policy, as the Petition’s theory for limitation [1e] would require.	33
B.	Oestvall/Dive-Reclus do not cure the deficiencies of Rao’s API-related disclosures.....	37
C.	Montemurro also does not cure the deficiencies of Rao and Oestvall/Dive-Reclus’s alleged API-related disclosures.	39
VII.	Conclusion	42

TABLE OF AUTHORITIES

Cases

<i>Nespresso USA, Inc. v. K-Fee Sys. GmbH,</i> IPR2022-01574, Paper No. 9 (PTAB Apr. 10, 2024).....	3
<i>OSI Pharms., LLC v. Apotex Inc.,</i> 939 F.3d 1375 (Fed. Cir. 2019).....	32, 33
<i>PAR Pharm., Inc. v. TWI Pharms., Inc.,</i> 773 F.3d 1186 (Fed. Cir. 2014).....	32
<i>Xerox Corp. v. ByteMark, Inc.,</i> IPR2022-00624, Paper No. 9 (PTAB Aug. 24, 2022)	33

PATENT OWNER'S EXHIBIT LIST

No.	Description
Ex. 2001	International Publication No. WO 2006/012610 to Rao et al. ("Rao-2")
Ex. 2002	Redline of the text of Rao (Ex. 1007) and Rao-2 (Ex. 2001)
Ex. 2003	U.S. Patent No. 8,825,109 to Montemurro et al. ("Montemurro Patent")
Ex. 2004	Redline of the text of Montemurro (Ex. 1009) and the Montemurro Patent (Ex. 2003)
Ex. 2005	U.S. Patent Application Publication No. 2006/0291419 to McConnell et al. ("McConnell")
Ex. 2006	Declaration of Dr. Zygmunt J. Haas in Support of Patent Owner's Response
Ex. 2007	<i>Curriculum vitae</i> of Dr. Zygmunt J. Haas
Ex. 2008	June 5, 2024 deposition transcript of Patrick McDaniel, Ph.D.

I. Introduction

The Petition fails to establish invalidity of any challenged claim for at least two reasons.

First, the Petition fails to explain how its proposed system involving a combination of several different references would include a “differential traffic control policy” that is applicable to WWAN but not WLAN traffic, and such that applications are “*only* allowed to utilize the at least one WWAN for Internet service activities when those applications are classified as interacting with a user in the device user interface foreground” as all challenged claims require. *See* Ex. 1001 at claim 1. Instead, the Petition’s proposed combination would have “prevent[ed] an untrusted application in the background from running or being given access to a service that consumes resources” (Pet. at 13-14), with no allegation that preventing an untrusted background application from running or being given access to services that consume resources would have allowed those applications to access the WLAN but not the WWAN.

Second, the Petition fails to show that its combination of references discloses or renders obvious an “[API] that allows a particular application to access one or more aspects of the differential traffic control policy applicable to that application” as required by all challenged claims. *See* Ex. 1001 at claim 1. The Petition sets forth a theory under which an application would have been able to access aspects of a

policy applicable to that application by virtue of the application including Rao's "remote access client" within it. But Petitioner's expert acknowledged that Rao does not teach *which* applications would include a "remote access client" (*see* Ex. 2008 at 6:22-7:6 ("Rao is sort of non specific about which application.")), and the Petition provides no motivation to include a remote access client within any application that is subject to any alleged differential traffic control policy as the Petition's theory would require.

Accordingly, all challenged claims should be found not unpatentable.

II. Background

A. Overview of the '578 Patent

At a high level, the '578 Patent is generally directed to, a device that "store[s] a differential traffic control policy applicable to data communicated ... using [a] WWAN modem ..., but not applicable to data communicated for Internet service activities using [a] WLAN modem," has "a user interface to allow a user to ... select ... applications that are only allowed to utilize the at least one WWAN ... when those applications are classified as interacting with a user in the device user interface foreground," and has "one or more processors configured to implement an [API] that allows a particular application to access one or more aspects of the differential traffic control policy applicable to that application." *See* Ex. 1001 at claim 1. More specifically, the only independent claim (claim 1) recites in full:

[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 at least one 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 at least one WLAN;

[1c] a non-transitory memory to store a differential traffic control policy applicable to data communicated for Internet service activities using the WWAN modem and the at least one WWAN, but not applicable to data communicated for Internet service activities using the WLAN modem and the at least one WLAN;

[1d] a user interface to allow a user to set one or more of a plurality of aspects of the differential traffic control policy to select one or more applications that are *only allowed to utilize the at least one WWAN* for Internet service activities *when those applications are classified as interacting with a user in the device user interface foreground*; and

[1e] one or more processors configured to implement *an application program interface (API) that allows a particular application to access one or more aspects of the differential traffic control policy applicable to that application*, including whether the user-settable

aspects of the policy only allow the particular application to utilize the at least one WWAN for Internet service activities when the particular application is classified as interacting with a user in the device user interface foreground.

Id. at claim 1.¹ As shown by claim element [1d], the differential traffic control policy of the claims, for at least one given application, must be such that the given application can only access the WWAN when the application is interacting with the user in the foreground. And as shown by claim element [1e], the claimed API must allow a given application to access information about the differential traffic control policy that is applicable to that application. Ex. 2006 ¶31.

III. Level of Ordinary Skill in the Art

The Petition proposes that a POSITA in the field of the '578 Patent “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. Additional graduate education could substitute for professional experience, and *vice versa*.” Ex. 1003 ¶18; *see* Pet. at 12 n.2 (citing Ex. 1003 ¶¶17-18).

¹ All emphases herein are added unless otherwise noted.

Patent Owner believes that Petition's stated level of skill is too vague. For example, it is unclear why the Petition proposes "three to five years of experience," when three years of experience already qualifies a person as a POSITA under the Petition's definition. And the Petition's proposal that "[a]dditional graduate education could substitute for professional experience, and *vice versa*" also lacks clarity. *See Nespresso USA, Inc. v. K-Fee Sys. GmbH*, IPR2022-01574, Paper No. 9 (PTAB Apr. 10, 2024). ("As for [the contention] that '[a]dditional education might substitute for some of the experience, and substantial experience might substitute for some of the educational background,' we find that this characterization is too vague."").

For purposes of this response, Patent Owner agrees that a person having a bachelor's degree in computer science, electrical engineering, or a related field, plus at least three years of experience with networking, power consumption of networked computing devices, and/or wireless digital communication systems qualifies as a POSITA. The three years of additional experience can be in either a professional setting or a research setting. *See* Ex. 2006 ¶27.

IV. Claim Construction

The Petition states that "no formal claim constructions are necessary." Pet. at 2. For purposes of this response, Patent Owner agrees that no formal claim construction is necessary.

V. The Petition does not demonstrate that its proposed combination discloses or renders obvious a “differential traffic control policy” meeting all of the claim 1 requirements.

The sole independent claim 1 of the '578 Patent recites a “differential traffic control policy” having several requirements. The Petition, however, fails to identify a single “differential traffic control policy” in its proposed combination of references that would even allegedly satisfy the requirements of the claimed “differential traffic control policy.”

Specifically, claim 1 recites, in part:

[1c] a non-transitory memory to store a differential traffic control policy applicable to data communicated for Internet service activities using the WWAN modem and the at least one WWAN, but not applicable to data communicated for Internet service activities using the WLAN modem and the at least one WLAN;

[1d] a user interface to allow a user to set one or more of a plurality of aspects of the differential traffic control policy to select one or more applications that are only allowed to utilize the at least one WWAN for Internet service activities when those applications are classified as interacting with a user in the device user interface foreground; and

[1e] one or more processors configured to implement an application program interface (API) that allows a particular application to access one or more aspects of the differential traffic control policy applicable to that application, including whether the user-settable aspects of the policy only allow the particular application to utilize the at least one

WWAN for Internet service activities when the particular application is classified as interacting with a user in the device user interface foreground.

Ex. 1001 at claim 1.

Claim 1 thus requires that aspects of the differential traffic control policy be modifiable (user-settable) through a user interface such that particular applications can be selected such that “they are only allowed to utilize the... WWAN... when those applications are... in the device user interface foreground” (limitation [1d]), such that there are “user-settable aspects of the policy” that would only allow particular applications “to utilize the at least one WWAN... when the particular application is classified as interacting... in the device user interface foreground” (limitation [1e]). Claim 1 *also* requires that the “differential traffic control policy” must be “applicable to... Internet service activities using the WWAN modem,” *and* that the “differential traffic control policy” must “*not* [be] applicable to... Internet service activities using the WLAN modem and the at least one WLAN” as recited by limitation [1c]. Ex. 2006 ¶35.

The claim thus requires the system to be configurable to define applications that are *only* permitted to access the WWAN when that application is interacting with a user in the foreground; if the application is running in the background (for example), its access to the WWAN is disallowed or blocked. Ex. 2006 ¶36. The

Petition confirms that it has the same understanding of the claim. *See* Pet. at 32-33 (in relation to this claim element, discussing “applying a policy to prioritize network transmissions of [an] application[to] result in ‘Internet service activities’ being ‘*allowed*’ or ‘*disallowed*’”) (first emphasis in original, other emphasis removed).

This understanding, in which the application (selectable through a user interface) must be ***blocked*** from accessing the WWAN modem, is also consistent with the specification of the ’578 Patent, which teaches “block[ing]” access as distinct from less drastic remedies that apply to individual network packets, such as delaying or re-ordering network packets by putting that traffic into lower-priority queues. Ex. 2006 ¶37; Ex. 1001 at 13:37-42 (discussing “block/allow” as different from “traffic control techniques,” such as “delay” or “priority queue”); *id.* at 57:6-7 (determines whether to allow or block a session, or alternatively, to implement traffic control techniques such as “queue priority”); *id.* at 11:38-49 (distinguishing “network access requests (e.g., IP address requests)” from “other network service usage activities”); *id.* at 77:54 (“priority level 0 can provide a blocked network access”); *id.* at 88:21-22 (“blocking [] access”); *id.* at 88:49-54 (“blocking [] access”); *id.* at 93:54-62 (“before a connection is allowed to be opened (e.g., before a socket is opened), transmission, or a flow/stream is initiated, it is blocked”); *id.* at 94:20-39 (“allow/block” is a “network access setting” applicable to a “network access request”). For example, the ’578 Patent describes “allow/block” as a separate

operation from “queue[ing]” or “defer[ring]” (*id.* at 94:22-32) and clarifies that “blocking” access applies to an entire network connection or socket rather than at the level of individual packets (*id.* at 93:54-62); *see also id.* at 104:51-105:8 (teaching that an advantage of “**block[ing]**” the application is “that the network service consuming application is prevented from consuming any [network] resources” so that costly network resources are not used when the user does not want them to be).

In sum, in order for the Petition to succeed, it must identify a “differential traffic control policy” that can be modified through a user interface to allow certain applications to **only** access the WWAN when those applications are classified as interacting in the device display foreground (as required by limitations [1d] and [1e]), and must **further** show that that same differential traffic control policy is applicable to data for activities using the WWAN and is **not** applicable to data for activities using the WLAN. Ex. 2006 ¶38. The Petition at pages 32-36 addresses this requirement that the policy provide “one or more applications that are only allowed to utilize the at least WWAN... when those applications are classified as interacting... in the device user interface foreground” with reference to **only** the Rao and Oestvall references. *See* Pet. 32-36 (citing **only** Rao, Ex. 1005, and Oestvall, Ex. 1006, as prior art references in support of this requirement).

As explained below, the Petition’s reliance on Rao and Oestvall (taken either alone or in combination with each other) for a “differential traffic control policy” that can be set such that particular applications are *only* allowed to utilize the WWAN when those applications are classified as interacting in the device interface foreground does not disclose or render obvious the claim requirements. *See* Ex. 2006 ¶¶38-45, 58-76.

A. Rao’s prioritization scheme relied on by the Petition does not disclose a “differential traffic control policy” such that any applications are only allowed to access the WWAN when they are classified as interacting in the foreground.

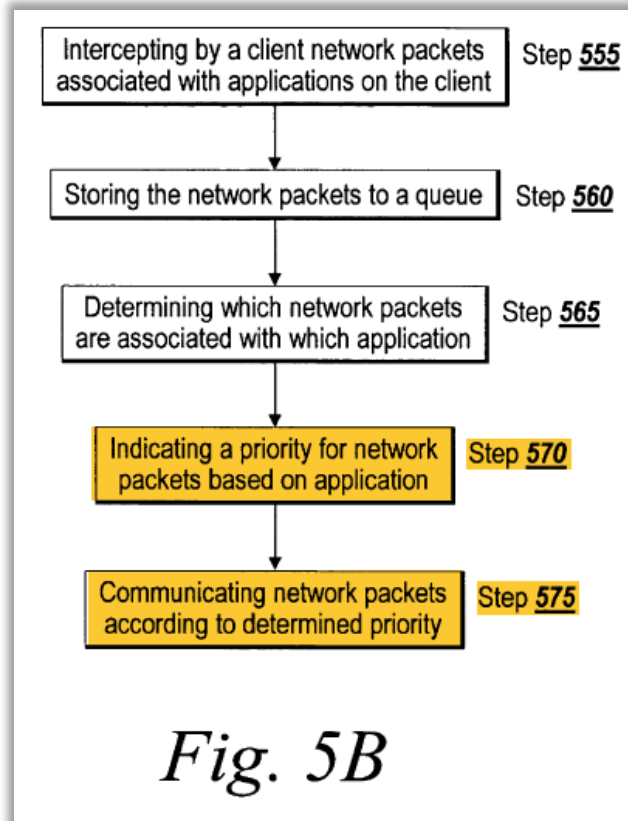
In alleging the obviousness of the requirement that particular applications would *only* be allowed to access the WWAN when they are classified as interacting with a user in the device user interface foreground, the Petition alleges that “a POSITA would have understood and found obvious that the Rao-Oestvall-Montemurro device would have been configured to implement Rao’s technique of intercepting network packets of an application based on the application’s prioritization, and (1) where the application is classified as running in the *foreground*, network packets of that application would be *stored in a queue ahead of other application(s) running in the background*, and (ii) where the application is classified as running in the *background*, network packets of that application would be *stored in a queue behind other application(s) running in the foreground*.” *Id.* at 33.

However as noted above, this is not what the claim requires. *See* Ex. 2006 ¶¶40-41. Rather, if the recited application is interacting with a user in the foreground, access to the WWAN modem is allowed. If that condition is not met (e.g., if the application is running in the background), the application is not permitted to access the WWAN modem at all—not simply assigned a lower priority within a queue.

Contrary to this requirement, the Petition acknowledges that even in its exemplary scenario, packets of a given application that are deprioritized as a result of Rao’s prioritization scheme are “presently disallowed” only until the device turns to handling the queued packets of the application—regardless of whether that application is interacting with a user in the foreground at that later time or not. *See id.* The Petition does not ever allege that Rao’s prioritization scheme results in only allowing *an application to access* to the WWAN modem when the application is classified as interacting with a user in the foreground, and otherwise disallowing or blocking access to the WWAN modem, and indeed it does not. Ex. 2006 ¶42.

Instead, Rao makes clear that its prioritization scheme, at most, simply *delays* the transmission of lower-priority packets (such as packets from applications running in the background) in favor of higher-priority packets—packets given a lower priority as a result of Rao’s prioritization scheme are nevertheless transmitted. *See* Ex. 2006 ¶43. Indeed, if there are no higher-priority packets ahead of them in the queue awaiting transmission, then Rao transmits the lower-priority packets

without any delay, even if the packets are associated with an application running in the background. Rao explains that “the network ***packets are organized into priority queues*** 540a-540[n] so that the network packets of the highest priority queue 540a-540n are communicated first, and then the next highest priority queue 540a-540n second, and so on Regardless of the queue 540a-540n organization and management, one ordinarily skilled in the art will recognize and appreciate that the ***remote access client of the present invention will communicate the network packets from the queues***” Ex. 1005 ¶[0194]; *see also id.* ¶[0184] (“[T]he outbound network packets generated by an application 338a-338n on the client 105 are ***prioritized by the client 105 prior to transmission*** based on the type and/or priority of the application 338a-338n.”). This is illustrated in Rao’s Figure 5B; after packets are assigned a priority “based on application” in step 570, those network packets are then communicated over the network in step 575:



Id. at Fig. 5B (annotation added). And because network packets are communicated “according to determined priority,” if there are no “higher priority” packets in Rao’s queue (such as those issued by applications running in the foreground) as compared with what would be “lower priority” packets (such as those issued by applications running in the background), the “low priority” packets in this scenario would still be communicated without any delay at all.

Rao’s claims also make it clear that even when a packet may have lower priority than other packets, the lower-priority packet is nevertheless eventually communicated, regardless of the foreground/background status of its corresponding application. *See id.* at claim 4 (only preventing a lower-priority packet from being

communicated “*ahead of*” higher priority packets); *id.* at claim 5 (discussing “holding” a deprioritized network packet, and then “releasing” that hold “upon communication” of certain higher priority packets). This is further confirmed because Rao teaches that assignment of priority involves at least *some* (non-zero) level of priority, contrary to the teachings of the ’578 Patent, which discloses that a “priority level 0” can be assigned to “block[]” modem access as opposed to non-zero priority levels that “provide” modem access. *Compare id.* ¶[0180] (referring to “levels of priority, such as high, medium, low, or numerically such as priority 1 ... 10”) (ellipses in original) *with* Ex. 1001 at 77:50-58 (disclosing that “a priority level 0 can provide a blocked network access, while priority levels between 1 through 9 can provide relatively increasing prioritized network access”); Ex. 2006 ¶44.

Indeed, as noted above, the Petition recognizes that packets of a given application that are deprioritized as a result of Rao’s prioritization scheme are “presently disallowed” only until the device turns to handling the queued packets of the application. Pet. at 33. In other words, the Petition itself recognizes that Rao (1) allows packets from background applications to be transmitted without any delay if there are no higher-priority packets in the queue, and (2) allows packets from background applications to be transmitted even when there are higher-priority packets from foreground applications, by only delaying the lower-priority packets to the extent that the higher-priority packets get transmitted first. Thus, the Petition

itself acknowledges that Rao lacks any policy that controls *whether* a packet is or is not transmitted based on the background or foreground status of the corresponding application. Ex. 2006 ¶45.

Accordingly, Rao’s prioritization scheme does not disclose any policy under which any application would be allowed to access the WWAN modem *only when* that application is classified as interacting with a user in the device user interface foreground. Indeed, the Board previously recognized as much, when it stated that in Rao, “the packets from the background application can eventually access the WWAN modem and be sent,” which “appears to be inconsistent with the plain meaning of the claim.” Paper No. 10 (Institution Decision) at 25.

Patent Owner recognizes that the Board further reasoned that the Petition had set forth a reasonable likelihood of prevailing on a theory where “a person having ordinary skill in the art would modify [Rao’s] differential traffic control policy based on teaching[s] of Oestvall.” *Id.* at 27. As explained in the following sections, however, the Petition does not explain *how* Rao’s policies would have been modified or provide any motivation to modify those policies.

B. Oestvall (alone or in combination with Rao) does not cure the deficiencies of Rao discussed above.

As noted above, the Petition does not establish that Rao’s alleged storing of “network packets of [a background] application” in “a queue behind other application(s) running in the foreground” (Pet. at 33) discloses that any application

would “**only** [be] allowed to utilize the at least one WWAN ... when [it is] classified as interacting with a user in the device user interface foreground,” as required by all challenged claims. *See supra* § V.A. Accordingly, the Petition relies on Oestvall’s “prevent[ing] the untrusted [background application] from running” (Ex. 1006 ¶¶0023); *see* Pet. at 34 (citing same)) as constituting “activity associated with [an untrusted background application] being **allowed only when** the application is running in the foreground.” Pet. at 34 (emphasis in original).

However, as the Board acknowledged, Oestvall alone does not supply a “differential traffic control policy” that is applicable only to WWAN and not to WLAN, as recited by the claims. *See* Paper No. 10 at 27 (“Petitioner relies on Rao and Montemurro, **but not Oestvall**, for a ‘differential traffic control policy.’”). And the Petition does not explain **how** any differential traffic control policies from Rao or Montemurro in the combined system would be modified to arrive at the claim language or provide any motivation to do so. *See* Ex. 2006 ¶¶60-76.

1. Oestvall does not disclose a “differential traffic control policy” applicable to WWAN but not WLAN.

For the requirement that particular applications are blocked from accessing the WWAN modem when they are not classified as interacting in the foreground, the Petition relies on “Oestvall’s techniques of preventing an untrusted application running in the background from ‘being given **any** services or consuming **any** resources’ while allowing the foreground application [whether trusted or untrusted]

to run and [be] ‘provided with resources and services.’” *Id.* at 34 (quoting Ex. 1006 ¶¶[0023], [0025]); *see also id.* at 31 (alleging that “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’”) (quoting Ex. 1006 ¶[0023]); *id.* at 34 (alleging the same).

The Petition does not allege that Oestvall’s prevention of untrusted background applications from running is somehow even related to any “aspects” of a “differential traffic control policy,” or is itself a “differential traffic control policy.” *See* Pet. at 25-26 (discussing only Rao in analyzing the “aspects of the differential traffic control policy” limitation); *see also* Paper No. 10 at 27 (“Petitioner relies on Rao and Montemurro, **but not Oestvall**, for a ‘differential traffic control policy.’”). Nor would Oestvall’s prevention of untrusted background applications from running meet the requirement that the “differential traffic control policy” be “*applicable to data communicated for Internet service activities using the WWAN modem..., but not applicable to data communicated for Internet service activities using the WLAN modem*” as required by claim 1 because Oestvall’s policy would be applicable to all network types (including WLAN).

As the Petition admits, in its Rao-Oestvall combination, where Rao’s application 338 is an untrusted application presently in the background, the Oestvall-like scheduler “would ‘**prevent[] the [application] from running**,’ e.g., ‘operates so

as to *never allocate any services or resources to the [application]*.” *Id.* at 34 (quoting Ex. 1006 ¶[0023]) (alterations in original). In other words, Oestvall stops untrusted background applications from running entirely, which prevents them from doing *anything*, including attempting to transmit network packets. Ex. 2006 ¶61; Ex. 1006 at Abstract (discussing “a control signal ... that in effect prevents the untrusted application from running, e.g., being given any services or consuming any resources”); *id.* ¶[0021] (“With the present invention, when an untrusted application is running on the battery operated device and another application should be in the foreground, the untrusted application is placed into the background *and is also actively prevented from running*.”); *id.* ¶[0014] (explaining that untrusted background applications “*need to be actively prevented from running*”); *see also id.* ¶¶[0023]-[0024]. Therefore, Oestvall’s disclosure of preventing untrusted applications from running *at all* if they are not running in the foreground, to the extent it meets other elements of claim 1, would not relate to any alleged “aspects of a differential traffic control policy,” or a “differential traffic control policy” itself, as required.

Furthermore, even if the Petition *had* alleged Oestvall’s preventing untrusted applications from running altogether constituted a “differential traffic control policy,” it would not be a “differential traffic control policy applicable to data communicated... using the WWAN modem... but not applicable to data

communicated... using the WLAN modem” as recited by limitation [1c]. Specifically, as the Petition acknowledges, preventing applications from running in the background would have operated “so as to never allocate *any services or resources* to the [application].” *Id.* at 34 (quoting Ex. 1006 ¶[0023]) (alterations in original). Of course, this would also prevent the application from receiving WLAN services or resources, and thus would prevent the application from accessing *both* the WLAN *and* WWAN modems (Ex. 2006 ¶62), and the Petition provides no explanation as to how any such policy would be “not applicable to data communicated... using the WLAN modem.”

2. The Petition provides no explanation of how any differential traffic control policy of Rao or Montemurro would be modified in view of Oestvall to meet all claim requirements.

After discussing the teachings of Rao and Oestvall separately, the Petition provides a conclusory allegation that in its proposed combination, a differential traffic control “policy is configurable to select an application only allowed to utilize WWAN (e.g., where WLAN is not available) based on the classification that the application is running in the foreground where the user interacts with the application via the device user interface (e.g., interacting with the device user interface for SMS or cellular calls).” Pet. 36. However, the Petition does not explain *how* a POSITA would supposedly have arrived at such a combination—for example, the Petition does not even explain what this policy would actually entail, much less explain why

this unspecified policy would have been motivated or have a reasonable expectation of success. Ex. 2006 ¶63.

In Patent Owner’s view, the only plausible reading of the Petition is that the “policy” that would prevent background applications from accessing the WWAN modem is simply Oestvall’s technique of preventing untrusted applications from running in the background. Ex. 2006 ¶64. For instance, the Petition is explicit that its proposed combination would have operated “to prevent an untrusted application in the background from running or being given access to a service that consumes resources.” Pet. 14 (discussing the “Rao-Oestvall” combination in the Petition’s Section III.A.3).

Notably, even if Oestvall’s technique of preventing background untrusted applications from running were *combined* with policies from Rao or Oestvall, the Petition does not identify any “differential traffic control policy applicable to data communicated... using the WWAN modem... but not applicable to data communicated... using the WLAN modem” as recited by limitation [1c]. Specifically, Oestvall’s technique (whether considered alone or in any disclosed combination with Rao or Oestvall) is clearly applicable to prevent background untrusted applications from receiving *any* services that consume resources, including WLAN services. Ex. 2006 ¶65.

Other than simply preventing background untrusted applications from running, the Petition provides no theory as to how the combined system would operate such that aspects of the differential traffic control policy would specify that certain “applications... are only allowed to utilize the at least one WWAN... when those applications are classified as interacting... in the device user interface foreground” as recited by limitation [1d]. For example, the Petition provides no theory as to how Rao’s packet prioritization and queuing policies would have been modified in view of Oestvall to meet this limitation.

Nor could the Petition have done so—in the proposed combination, there would be no need (for example) for Rao’s packet management policies to identify and discard packets from untrusted background applications, because in the proposed combination the Petition acknowledges that the system would “prevent an untrusted application in the background from running.” Pet. 14; Ex. 2006 ¶¶66-67.

The Petition’s theory is also consistent with Oestvall’s teachings that untrusted background applications need to be *prevented from running* altogether, such that untrusted background applications would never be able to establish a network connection or to generate any communications resulting in network packets. Ex. 1006 at Abstract, ¶¶[0014], [0021], [0023]. The Petition is explicit that its combination of Rao with Oestvall maintains this teaching of Oestvall, and the Petition does not provide any motivation to deviate from that teaching. *See* Pet. at

14 (“The [combination] would have also enabled the improved agent to prevent an untrusted application in the background from running ...”). Thus, the combined system would not need to modify any packet prioritization policies to account for packets generated from untrusted background applications, because untrusted background applications would be completely *incapable* of generating network packets in the first place under the Petition’s proposed combination. Ex. 2006 ¶68

Thus, because background untrusted applications are prevented from running, they would not generate any packets in the first place that would need to be discarded (e.g., using Rao’s alleged differential traffic control policy). Ex. 2006 ¶69.

3. The Petition provides no motivation to allow a user to select which applications should be classified as “untrusted.”

Limitation [1d] recites “a user interface to allow a user to set one or more of a plurality of aspects of the differential traffic control policy to select one or more applications that are only allowed to utilize the at least one WWAN for Internet service activities when those applications are classified as interacting with a user in the device user interface foreground.” However, the Petition makes clear that in combination with Oestvall, the applications that are “only allowed to utilize the at least one WWAN for Internet service activities when those applications are classified as interacting... in the device user interface foreground” are “untrusted

application[s].” *See* Pet. 34 (explaining that the “Oestvall-like scheduler” would apply to “an untrusted application presently in the background”); Ex. 2006 ¶70.

Thus, for a combination based in part on Oestvall to be consistent with this claim language and cure Rao’s deficiencies, the user interface would need to allow a *user* to select which applications were “trusted” or “untrusted.” Ex. 2006 ¶71. However, the Petition sets forth no motivation to place this important classification into the hands of the user, and indeed, Oestvall counsels against such a modification. *See id.*

Specifically, Oestvall teaches that whether an application is trusted or not should *not* be decided by a user. *Id.* ¶72. For instance, Oestvall discloses that “[t]rust will conventionally be established for a given application using a signature in the application installation file, although there are other techniques that may be deployed as part of the secure computing base of the device.” Ex. 1006 ¶[0015]; *see also id.* ¶[0020]. Oestvall further discloses other “criteria that may be relevant in assessing whether a give[n] application is ‘untrusted’ or not” and provides examples of those criteria. *Id.* ¶[0010]. A first example is “which protected resources on the device can be accessed by the application,” because “an ‘untrusted’ application might be defined as one that is not able to access certain predefined resources.” *Id.* ¶[0011]. A second example is “whether the application was loaded from ROM or RAM” because “applications loaded from RAM are likely to be from third party sources

and hence less trustworthy than applications loaded from ROM, which would typically be provided by the device manufacturer.” *Id.* ¶[0012]. And a third example is “whether the application has been validated using some predefined validation or certification process.” *Id.* ¶[0013].

The Petition cites to no evidence that a POSITA would have been motivated to allow a user to select which applications are “untrusted” or “trusted” in the combined system. Rather, Oestvall suggests that a user should *not* be permitted to do so. Ex. 2006 ¶73. Oestvall explains that preventing any activity from “untrusted” background applications is important because, as compared with “trusted” applications, they are “more likely to contain a wrong implementation of normal background behaviour” that can result in, for example, unnecessary battery drain. Ex. 1006 ¶¶[0014], [0021]. This is because “[a]pplications might, in theory, be written so that they take notice of an event sent to them when they are sent to background, causing them to automatically cease running. But even this is likely to be missed in application which are from certain kinds of third party programmers or are not validated as proper implementations.” *Id.* ¶[0014].

A POSITA would understand that permitting a user to select which applications are “untrusted” and “trusted,” as opposed to using “a signature in the application installation file,” or the other criteria that Oestvall discloses to do so (*id.* ¶¶[0010]-[0013], [0015]), would frustrate Oestvall’s goal of “preserving power ...

and system resources” by preventing applications that fail to meet those “trusted” criteria from running in the background at all (*id.* ¶[0021]). Ex. 2006 ¶74. For example, a user is unlikely to have any insight into the implementation details of “third party applications” such as “games or similar types of applications.” *See* Ex. 1006 ¶[0019]. Thus, a user would not have insight into whether these types of applications “contain a wrong implementation of normal background behavior” and should thus be deemed “untrusted.” *Id.* ¶[0014].

Indeed, if given the option, it would be commonplace for users to believe a downloaded game to be safe, flag it as a “trusted” application, and thus expose the system to unnecessary resource drain and network communications. It would thus not make sense to allow a *user* to determine which applications are “trusted” or not, as opposed to determining trust “conventionally” as Oestvall teaches, such as through “a signature in the application installation file.” *Id.* ¶[0015]; Ex. 2006 ¶75.

Accordingly, the Petition fails to show that its proposed combination discloses or renders obvious “a user interface to allow a user ... to select one or more applications that are only allowed to utilize the at least one WWAN ... when those applications are classified as interacting with a user in the foreground,” as required by all challenged claims. Ex. 2006 ¶76

VI. The Petition does not show that its combination discloses or renders obvious claim element [1e].

Claim element [1e] requires, in part, “an application programming interface (API) that *allows* a particular *application to access* one or more *aspects of the differential traffic control policy applicable to that application*, including whether the user-settable aspects of the policy only allow the particular application to utilize the at least one WWAN for Internet service activities when the particular application is classified as interacting with a user in the device interface foreground.” Ex. 1001 at 108:38-47. Put simply, this claim limitation requires an API that allows an application to access information concerning the “differential traffic control policy” that applies to the application’s Internet service activities. Ex. 2006 ¶77. As explained in further detail below, the Petition does not point to anything in Rao, Oestvall, or Montemurro that teaches this limitation, nor does the Petition show that the combination of these references renders this limitation obvious. *Id.* ¶¶77-100.

A. The Petition’s reliance on Rao alone does not satisfy limitation [1e].

1. The Petition’s Rao-based theory requires the remote access client being included within a particular application—one that is governed by the differential traffic control policy.

The Petition’s Rao-based theory for limitation [1e] relies on Rao’s teachings that the “agent 326 may communicate the priority of network packets to the filter 322 by any suitable means... such as via an application programming interface (API).” Pet. 36-37 (quoting Ex. 1005 ¶[0190]). The Petition also relies on Rao’s

teachings that remote access client (including agent 326 and/or the filter, ‘may be included within an application.’” *Id.* (quoting Ex. 1005, ¶[0115]). The Petition thus concludes that because there can be an “API that enables communication between agent 326 and filter 322,” and because “an application... includes the remote access client 120 (including agent 325 and/or filter 322),” that “an application... would access the policies accessible by agent 326 that enables communication between agent 326 and filter 322.” Pet. 37-38.

Put more simply, the Petition’s logic is that, based on Rao’s teachings, some application could include remote access client, which could further include filter 322. And filter 322 can receive information about policies from agent 326 via an API. Thus, because under the Petition’s logic filter 322 would be within some application, that application would receive information about policies from agent 326 via an API. *See* Ex. 2006 at ¶¶79-80.

Notably, limitation [1e] does not simply state that just *any* application receives information about policies via an API; it instead requires an API “that allows a *particular application to access one or more aspects of the differential traffic control policy applicable to that application.*” Ex. 1001 at 108:38-42. In other words, the application that receives information about the policy must be governed by the policy, such that it can access via the API “one or more aspects of the differential traffic control policy *applicable to that application.*” Ex. 2006 ¶81.

Accordingly, for the Petition's Rao-based theory to succeed, the Petition must show that Rao either discloses or renders obvious placing a remote access client within an application that is governed by any alleged differential traffic control policy. However, as explained in the two following subsections, Rao does not disclose placing the remote access client within an application that is governed by the differential traffic control policy, and the Petition fails to establish that such a solution would have been obvious because the Petition does not provide any motivation for doing so. Ex. 2006 ¶¶82-91.

2. The Petition's Rao-based theory relies on Rao's inclusion of a remote access client within a particular application, but Rao does not teach any particular configuration and the Petition does not motivate any particular configuration.

Despite the Petition's reliance on Rao teaching that "remote access client 120" "may be included within an application," Petitioner's expert conceded that Rao does not expressly teach *which* application the "remote access client" would be included within:

Q Okay. So you see the first sentence of paragraph 104 [of Exhibit 1003] says that: Additionally, Rao describes that its remote access client 120 which includes the agent 326 and/or the filter 322 may be included within an application 338, right?

A Yes.

Q Okay. *So what's your understanding of this teaching of Rao? And specifically, what application are you proposing that Rao teaches that the remote access client 120 would be included within?*

A *Rao is sort of non specific about which application.* This is a general concept.

Ex. 2008 at 6:16-7:6; *see also* Ex. 2006 ¶¶83-84 (Dr. Haas agreeing that “Rao does not specify *which* application a remote access client would be included within”). In fact, although Petitioner’s expert asserted at his deposition that Rao “is sort of teaching” a solution involving “incorporating something like [Rao’s] remote access client into multiple applications” (Ex. 2008 at 8:16-10:7), when asked what the benefits would be to pursuing such an implementation, Petitioner’s expert conceded that he was “inventing on the fly” because incorporating Rao’s remote access client into multiple applications was a “hypothetical system.” *Id.* at 10:8-14. Indeed, even counsel for Petitioner objected to Patent Owner’s questioning as to whether any given implementations of a remote access client into an application would be logical.

Q And I'm -- I'm looking at the realtime transcript so I may be getting this wrong.

But previously, I believe you testified that Rao is sort of nonspecific about which application the remote access client is incorporated into.

So with that context, my question is: In your opinion, if a POSITA were to incorporate remote access client 120 into one or more applications 338 within Rao's system, what would be the most logical way to do that?

MS. HUANG: Objection, calls for speculation; form.

Ex. 2008 at 8:16-9:6 (annotated).

We've been talking a little bit about what you said, a hypothetical system, where Rao -- you know, Rao's remote access client could be incorporated into multiple applications.

Do you understand Rao to teach that the remote access client could be incorporated into only a single application?

MS. HUANG: Objection, calls for speculation.

Id. at 11:2-10 (annotated).

Q So if a POSITA, understanding that the remote access client could be incorporated into just a single application, were to implement a system like that what would be an example of a logical way that that system would operate?

MS. HUANG: Objection, calls for speculation.

A Yeah. Again, I'm inventing -- you know, you're asking me to -- to interpret Rao. Rao

gives the -- describes that you want to -- that you would put one of these -- put the agent in the application. One way to do that, as I mentioned, would be to do it as a library. That would be a logical way to do it.

Id. at 11:14-12:5 (annotated).

The fact that both Petitioner's expert and Petitioner's counsel recognized that application of Rao's sparse and generalized teachings of incorporating a remote access client into an unspecified application "calls for speculation" and involves "inventing on the fly" shows that Rao does not provide *any* specific teachings regarding *which* application Rao's remote access client would be incorporated. *See also* Ex. 2008 at 12:13-13:4 (admitting that "there isn't one, you know, solution that [Rao is] promoting"); *id.* at 13:21-14:4 (acknowledging that at most, Rao teaches that you could put a remote access client in an application "where it's desirable," and that Rao "doesn't—and a POSITA wouldn't say, oh, well, [put it in] all of [the applications] or some of them or one of them. . . . That's how a POSITA would interpret that.").

Accordingly, because Rao is "non specific" about which applications would include a remote access client within them (*see, e.g.*, Ex. 2008 at 6:22-7:6), the Petition must show that a POSITA would have been motivated to pursue any

particular proposed configuration of remote access client(s) being included within any particular application(s) in order to show that such a configuration would have been obvious in view of Rao.² Ex. 2006 ¶¶85.

As explained in the following subsection, the Petition fails to set forth any motivation that would even allegedly render obvious placing the remote access client in an application that is subject to any alleged differential traffic control policy. *See* Ex. 2006 ¶¶86-91

3. The Petition fails to motivate inclusion of Rao’s remote access client within an application subject to any differential traffic control policy, as the Petition’s theory for limitation [1e] would require.

² Patent Owner acknowledges the Board’s reasoning that even if “Rao teaches something that is allegedly not logical,” that “Rao must be considered for all that it teaches, even if it is illogical.” Paper No. 10 at 31-32. However, as shown by the positions taken by Petitioner’s counsel and Petitioner’s expert, Rao does *not* teach that any specific application (such as an application actually subject to any alleged “differential traffic control policy”) would have included a remote access client. Thus, the Petition must show that such a POSITA would have been motivated to arrive at such an implementation of Rao’s teachings in order to establish a *prima facie* case of obviousness.

As explained in the preceding subsections (Sections VI.A.1-VI.A.2), the Petition's theory requires that Rao's remote access client would be included within an application subject to a differential traffic control policy, but Rao does not actually disclose that Rao's remote access client would necessarily be included within such an application. Accordingly, the Petition must establish the obviousness of pursuing such an implementation based on Rao, including identifying a motivation that would have led a POSITA to pursue such an implementation. *See PAR Pharm., Inc. v. TWI Pharms., Inc.*, 773 F.3d 1186, 1195 (Fed. Cir. 2014) ("The mere fact that a certain thing *may* result from a given set of circumstances is not sufficient [to establish inherency]."); *OSI Pharms., LLC v. Apotex Inc.*, 939 F.3d 1375, 1382 (Fed. Cir. 2019) ("An obviousness determination requires finding that a person of ordinary skill in the art would have been motivated to combine or modify the teachings in the prior art and would have had a reasonable expectation of success in doing so.").

However, the Petition does not even *allege* any motivation to create a system that would place a remote access client (i.e., the component that is responsible for actually enforcing the differential traffic control policy in Rao—*see* Ex. 2006 ¶88) within an application that is subject to the differential traffic control policy. *See* Pet. 36-38 (no discussion of any motivation to pursue such an implementation, nor any reasonable expectation of success). Rather, the Petition merely provides a

conclusory assertion, supported only by a conclusory statement in an expert declaration that parrots the Petition's conclusory allegation, that "the API allows application 338 to access one or more policies 520 that are configured for that application." Pet. 37-38 (quoting Ex. 1003 ¶104). This is insufficient to set forth a *prima facie* case of obviousness. See *OSI Pharms.*, 939 F.3d at 1382; *Xerox Corp. v. ByteMark, Inc.*, IPR2022-00624, Paper No. 9 at 15 (PTAB Aug. 24, 2022) (precedential) (rejecting conclusory assertions of a Petition when "the cited declaration testimony is conclusory and unsupported, [and] adds little to the conclusory assertion for which it is offered to support").

Furthermore, as Patent Owner's expert Dr. Haas explains, placing a remote access client within an application subject to Rao's prioritization policies would have made no sense, because it would place enforcement of the policy in the control of the application itself. Ex. 2006 at ¶¶89-90. This would be problematic because it would allow the application to circumvent or disregard the policies that are supposed to be applicable to that application. For example, consider the case of an application that would like to initiate a large download, which Rao's prioritization policies specify should receive a relatively low communication priority. If the remote access client were included within such an application, it would give that application control over enforcement of Rao's prioritization policies, and would allow that application to simply ignore the policies applicable to it. Ex. 2006 at ¶89. A POSITA

would readily recognize that such an implementation—providing a remote access client within an application that is subject to the policy that needs enforcement—would be contrary to the whole purpose of having traffic control policies in the first place, because it would create perverse incentives for the developers of those applications to simply ignore the applicable policies to the benefit of the application. *See id.*

In short, nothing in any cited prior art reference suggests that the remote access client (i.e., Rao’s mechanism for enforcing its policies) should be placed within an application that is itself subject to Rao’s policies, as the Petition’s Rao-based theory for limitation [1e] would require. And such an implementation would not have been obvious, because it would require the application to self-police itself, which would create perverse incentives and encourage the application developer to simply disregard any policy restrictions applicable to the application. Ex. 2006 ¶90.

Finally, the Petition also alleges that because “Rao describes that its device can run the Java operating system,” “a POSITA would have understood and found obvious that the application would have received an indication, via the Java sockets API, of the network access condition.” *Id.* at 39-40. Of course, the Petition does not allege that Rao discloses any “Java sockets API” and indeed it does not. The Petition likewise does not allege why a POSITA would have been motivated to use a Java sockets API rather than the APIs described in Rao, let alone use them for a

functionality that Rao does not contemplate for the APIs that Rao does disclose. *See* Ex. 2006 ¶91.

B. Oestvall/Dive-Reclus do not cure the deficiencies of Rao’s API-related disclosures.

The Petition claims that “Oestvall incorporates by reference Dive-Reclus, which teaches using APIs in accessing a network” and that “Dive-Reclus teaches permissions regulating network access by a third-party application that uses an API call.” Pet. at 38-39 (citing Ex. 1006 ¶[0020]; Ex. 1026 at 16:23-17:28, 20:1-12) (footnote omitted). Setting aside whether Oestvall effectively incorporates Dive-Reclus by reference, even assuming that it does, the Petition never alleges that Dive-Reclus discloses “an application programming interface (API) that allows a particular application to access one or more aspects of the differential traffic control policy applicable to that application.” And it does not. Dive-Reclus simply states that “on each access to the sensitive API call, a dialog box created by the server asks the user if they wish to grant the capability.” Ex. 1026 at 16:19-20; Ex. 2006 ¶92.

Based on this facially irrelevant disclosure, the Petition states in conclusory fashion that a “POSITA would have found it obvious that a permission decision (grant/deny) is communicated to the third-party application through a corresponding API” (Pet. at 36), with no explanation of what API it is referring to, and likewise with no explanation of why a POSITA would have been motivated to communicate any of Dive-Reclus’ (or Oestvall’s) permission decisions to any “third-party

application” such that it could access them. Again, the Petition simply provides no *motivation* to arrive at the claim’s API limitation in view of Dive-Reclus. *See* Ex. 2006 ¶93.

Moreover, to be consistent with any Oestvall-based theory for claim element [1d], in which it would be necessary to (incorrectly) assume that Oestvall’s prevention of untrusted background applications from running is a “differential traffic control policy” that is applicable to WWAN data but not applicable to WLAN data, the API would need to allow a given application to access “aspects” of that policy indicating whether it is “untrusted” or “trusted” (because whether the application is “untrusted” or “trusted” would determine whether the “policy only allow[s] the particular application to utilize the at least one WWAN... when the particular application is classified as interacting... in the device user interface foreground”). But the Petition does not allege that Dive-Reclus’ API (or any other API) would provide information to applications indicating whether they are trusted or not (or otherwise whether any aspects of the policy only allow the application to utilize WWAN when those applications are classified as interacting in the foreground), and the Petition likewise does not allege that Oestvall (or Dive-Reclus) renders doing so obvious. *See* Ex. 2006 ¶94. For example, the Petition provides no motivation to pursue such an implementation of Dive-Reclus’ API or any other API. Accordingly, the Petition sets forth no *prima facie* case that Oestvall (or Dive-

Reclus) discloses or renders obvious “an application programming interface (API) that allows a particular application to access one or more aspects of the differential traffic control policy.”

The Petition also alleges that (a) “based on Rao and Oestvall’s disclosure of API usage, Rao-Oestvall’s improved agent would have leveraged several types of APIs in *regulating applications*,” (b) “a POSITA would have found obvious that [this] improved agent leverages APIs including those Rao and Oestvall describes, and conventional APIs known by the Critical Date, *to support application operations* in mobile devices,” and (c) a “POSITA would have found it obvious to use well-known APIs *to provide communications to applications* in Rao-Oestvall.” Pet. at 38-40. Not only are these allegations conclusory, but they are also not relevant to the claim limitation at hand. The Petition does not (and could not) explain how generalized concepts such as using (unidentified) APIs to “regulat[e] applications,” “support application operations,” or “provide communications to applications” disclose or render obvious “an application programming interface (API) that allows a particular application to access one or more aspects of the differential traffic control policy applicable to that application.” See Ex. 2006 ¶95.

C. Montemurro also does not cure the deficiencies of Rao and Oestvall/Dive-Reclus’s alleged API-related disclosures.

The Petition further asserts that “a POSITA would have understood and found obvious that Montemurro’s API (e.g., socket-based API 206) ... operates to allow a

particular application 204 to access ‘various factors’ of one of ‘a set of rules/policies’ ... in rules engine 206A, which is applicable to that particular application.” Pet. at 41.

But Montemurro contains no such disclosure or suggestion. *See* Ex. 2006 ¶¶96-97. Rather, Montemurro discloses that one of the ways that “applications 204” can communicate “is socket-based using a socket-based application programming interface (API) 206 for communications.” Ex. 1007 ¶[0033]. “A socket-based connection uses the connection table and routing table to determine how an IP packet will be transmitted on the network 104 and 106.” *Id.* Even assuming that Montemurro’s “set of rules/policies” (*see id.* ¶[0029]) is the claimed “differential traffic control policy,” Montemurro does not contemplate that its socket-based API is used to “allow[] a particular application to access one or more aspects of” the “set of rules/policies” that apply to that application. Rather, Montemurro discloses that the socket-based connection is used to determine *how packets are transmitted*, and does not disclose or suggest that the connection is used to communicate anything about a “set of rules/policies” to the application to which those rules/policies apply (as limitation [1e] requires).

The Petition also alleges that “Montemurro describes that ‘[r]ules engine 206A also interacts with the connection API’s to determine which interface would be best used to serve a particular application,” and that “the instructions define a

communication API for handling communications on behalf of applications, said communication API routing said communications in accordance with the routing table and connection table.” Pet. at 40 (quoting Ex. 1007 ¶[0035], claim 7) (alteration in original). The Petition does not allege that Montemurro’s communication APIs are used to communicate anything about a “set of rules/policies” to the application to which those rules/policies apply. And they are not. Instead, Montemurro contemplates that its communication APIs (similar to its socket-based APIs) interact with the rules engine, or connection table and routing table, to determine what network interface will be used for a given application. *See* Ex. 2006 ¶98 (citing Ex. 1007 ¶[0035]).

Finally, the Petition does not provide any reasoning for why a POSITA would have been *motivated* to modify Montemurro such that its socket-based connection or its communication APIs would communicate to the application itself information concerning a “set of rules/policies” that apply to that application, in addition to (or instead of) performing their disclosed functions of interacting with the connection table, routing table, and/or the rules engine to determine how packets should be transmitted or what network interface should be used for a given application. *See* Ex. 2006 ¶99.

Accordingly, because the Petition does not establish that Montemurro discloses limitation [1e] or that a POSITA would have been motivated to modify any

APIs disclosed in Montemurro to arrive at limitation [1e], the Petition does not show that Montemurro (alone or in combination with Rao, Oestvall, or Dive-Reclus) discloses or render limitation [1e] obvious. *Id.* ¶100.

VII. Conclusion

For at least the foregoing reasons, Patent Owner respectfully requests that all challenged claims be found not unpatentable.

Date: July 2, 2024

Respectfully submitted,

/James A. Milkey/

James A. Milkey, Reg. No. 79,503

Reza Mirzaie, Reg. No. 69,138

Marc A. Fenster, *pro hac vice* forthcoming

Dale Chang, Reg. No. 61,476

Amy E. Hayden, Reg. No. 64,817

Neil A. Rubin, Reg. No. 67,030

Philip X. Wang, Reg. No. 74,621

RUSS, AUGUST & KABAT

12424 Wilshire Blvd., 12th Floor

Los Angeles, CA 90025

Counsel for Patent Owner

CERTIFICATION REGARDING WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Patent Owner certifies that there are 8,825 words in the paper excluding the portions exempted under 37 C.F.R. §42.24(a)(1).

Date: July 2, 2024

/James A. Milkey/

James A. Milkey, Reg. No. 79,503

Reza Mirzaie, Reg. No. 69,138

Marc A. Fenster, *pro hac vice* forthcoming

Dale Chang, Reg. No. 61,476

Amy E. Hayden, Reg. No. 64,817

Neil A. Rubin, Reg. No. 67,030

Philip X. Wang, Reg. No. 74,621

RUSS, AUGUST & KABAT

12424 Wilshire Blvd., 12th Floor

Los Angeles, CA 90025

Counsel for Patent Owner

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e)(1))

The undersigned hereby certifies that the above document was served on July 2, 2024, by filing this document through the Patent Trial and Appeal Case Tracking System as well as delivering a copy via electronic mail upon the following attorneys of record for the Petitioner:

W. Karl Renner (Reg. No. 41,265)
Jeremy J. Monaldo (Reg. No. 58,680)
Jennifer J. Huang (Reg. No. 64,297)
Sangki Park (Reg. No. 77,261)
FISH & RICHARDSON P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
IPR39843-0157IP1@fr.com
PTABInbound@fr.com
axf-ptab@fr.com
jjm@fr.com
jjh@fr.com
spark@fr.com

Date: July 2, 2024

/James A. Milkey/
James A. Milkey, Reg. No. 79,503
Reza Mirzaie, Reg. No. 69,138
Marc A. Fenster, *pro hac vice* forthcoming
Dale Chang, Reg. No. 61,476
Amy E. Hayden, Reg. No. 64,817
Neil A. Rubin, Reg. No. 67,030
Philip X. Wang, Reg. No. 74,621
RUSS, AUGUST & KABAT
12424 Wilshire Blvd., 12th Floor
Los Angeles, CA 90025

Counsel for Patent Owner