UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
Petitioner,

v.

HEADWATER RESEARCH LLC,
Patent Owner.

IPR2023-01462
Patent 9,277,445

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I. INTRODUCTION 1

II. OVERVIEW OF THE '445 PATENT 2

III. LEVEL OF ORDINARY SKILL IN THE ART 4

IV. CLAIM CONSTRUCTION 4

V. THE PETITION FAILS TO SHOW A REASONABLE LIKELIHOOD OF UNPATENTABILITY FOR ANY CHALLENGED CLAIM 4

A. The Petition fails to show that a POSITA would have been motivated to modify Oestvall to allow untrusted applications to continue to run in the background (contrary to Oestvall's teachings and purpose), only to generate network packets that are ultimately discarded by Rao's filter. 7

B. The Petition's theory also fails because prioritizing and discarding network packets after an application's Internet service access request has been granted does not constitute blocking the application's Internet service access request. 24

VI. CONCLUSION 31

TABLE OF AUTHORITIES

Cases

Galderma Labs., L.P. v. Tolmar, Inc.,
737 F.3d 731 (Fed. Cir. 2013).....11

KSR Intern. Co. v. Teleflex Inc.,
550 U.S. 398 (2007).....23

Meiresonne v. Google, Inc.,
849 F.3d 1379 (Fed. Cir. 2017).....11

Santarus, Inc. v. Par Pharm., Inc.,
694 F.3d 1344 (Fed. Cir. 2012).....12

Xerox Corp. v. Bytemark, Inc.,
IPR2022-00624, Paper No. 9 (Aug 24, 2022) 16

Statutes

37 CFR § 42.65 15

MPEP § 2142 23

PATENT OWNER'S EXHIBIT LIST

No.	Description
Ex. 2001	IPR Petition, *Samsung Elecs. Co. v. Headwater Research LLC*, IPR2023-01253, Paper No. 2 (PTAB Aug. 11, 2023)
Ex. 2002	IPR Petition, *Samsung Elecs. Co. v. Headwater Research LLC*, IPR2023-01337, Paper No. 2 (PTAB Aug. 25, 2023)
Ex. 2003	IPR Petition, *Samsung Elecs. Co. v. Headwater Research LLC*, IPR2023-01336, Paper No. 2 (PTAB Aug. 25, 2023)
Ex. 2004	IPR Petition, *Samsung Elecs. Co. v. Headwater Research LLC*, IPR2023-01361, Paper No. 3 (PTAB Sept. 8, 2023)

I. INTRODUCTION

The Board should deny institution of *inter partes* review ("IPR") of U.S. Patent No. 9,277,445 ("the '445 Patent"). The Petition fails to show a reasonable likelihood of unpatentability for two independent reasons.

First, the Petition alleges a combination of Rao and Oestvall in which untrusted applications are allowed to run in the background and generate network packets, only for those packets to be discarded before transmission. This is illogical, and the Petition fails to show why a POSITA would be motivated to combine Rao and Oestvall in this manner. Indeed, in asserting the purported combination, the Petition *ignores* Oestvall's teachings that untrusted applications should be prevented from running while in the background, such that untrusted background applications would never generate any network packets in the first place. Pet. 15.

Second, all challenged claims require "block[ing] the Internet service access request." Under the Petition's theory, the action alleged to constitute "block[ing] the Internet service access request" is discarding network packets generated by untrusted background applications. *See id.* 42. But contrary to the Petition's argument, discarding a network packet in Rao does ***not*** constitute blocking an "Internet service access request" because Rao's network packets are only discarded after access to Internet service has already been granted.

These deficiencies apply to all challenged claims. Accordingly, the Petition fails to show unpatentability for any claim, and institution should be denied.

II. OVERVIEW OF THE '445 PATENT

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." Ex. 1001, Abstract. More specifically, the only independent claim (Claim 1) recites:

> [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; and
>
> [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] 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

As explained by the ’445 Patent, the claimed invention allows the system to prevent particular applications from accessing network connections (and thus prevent them from consuming network resources), such as when they are not classified as interacting with a user in the device user interface foreground. Indeed, the ’445 Patent provides an example of blocking a network access request (i.e., a request to connect to the network such as by opening a socket), such that the application needs to submit its network access request later: “As yet another

example, ***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*** and a message is sent back to the application… ***to try again later for the requested network access***." Ex. 1001, 91:41-49.[1]

III. LEVEL OF ORDINARY SKILL IN THE ART

The Petition proposes that a POSITA in the field of the '445 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*." *See* Pet. at 3 (citing Ex. 1003 ¶¶15-17). For purposes of this preliminary response, Patent Owner does not challenge that definition.

IV. CLAIM CONSTRUCTION

The Petition states that "no formal claim constructions are necessary." *Id.* 2-3. For purposes of this preliminary response only, Patent Owner agrees that no formal claim construction is necessary.

V. THE PETITION FAILS TO SHOW A REASONABLE LIKELIHOOD OF UNPATENTABILITY FOR ANY CHALLENGED CLAIM

[1] All emphasis added unless otherwise noted.

Claim 1 (from which all challenged claims depend) recites, in part, "apply a differential traffic control policy to the Internet service access request" that "block[s] the Internet service access request" when "the particular application is not classified as interacting with a user in the device user interface foreground" and "allow[s] the Internet service access request under at least one different state of the first and second classifications."

The Petition relies on Rao in view of Oestvall for these limitations, which the Petition labels [1g] and [1h]. Pet. at 32-36 (relying on the combination of Rao and Oestvall for the aspects of [1f] that relate to applying a differential traffic control policy to the Internet service access request), 36-37 (relying on the combination of Rao and Oestvall for the aspects of [1g] that require blocking the Internet service access request based on whether the application is classified as interacting with a user in the foreground), 38 (relying on the combination of Rao and Oestvall for the aspects of [1h] requiring allowing the Internet service access request). Although the Petition relies on Montemurro for other limitations, the Petition relies only on features allegedly taught in Rao or Oestvall, rather than Montemurro, to show "apply[ing] a differential traffic control policy to the Internet service access request" that "block[s]" or "allow[s]" the request. Pet. 32-38.

The Petition's proposed combination requires modifying Oestvall to allow untrusted applications in the background to continue to run, so that Rao's filter can

also be modified to selectively discard all network packets associated with those untrusted background applications. *See id.* 14-15 (acknowledging that, "while Oestvall teaches increasing battery life by preventing such applications from running," the Petition's proposed combination does ***not*** "prevent[] such applications from running" and, instead, it ***allows*** the untrusted applications to run in the background, where a filter "would selectively 'discard[]' network packets from applications that are 'untrusted' and ***running in the background***"); *id.* 37 (relying on discarding of packets generated by background untrusted applications that continue to run in meeting limitation [1g]). But the Petition fails to show that a POSITA would have been motivated to pursue its proposed combination, which is contrary to Oestvall's express teaching to prevent untrusted background applications from consuming system resources by stopping them from running, as well as its stated goal of avoiding all battery drain from untrusted background applications.

Moreover, even assuming counterfactually that a POSITA would have been motivated to pursue the Petition's proposed combination the Petition fails to show that the application's "Internet service access request" would be blocked, or even controlled, in the proposed Rao-Oestvall-Montemurro combination. On the contrary, the proposed Rao-Oestvall combination has no such feature for blocking Internet service access requests, and the Petition fails to even identify the "Internet service access request" that is purportedly being blocked.

A. The Petition fails to show that a POSITA would have been motivated to modify Oestvall to allow untrusted applications to continue to run in the background (contrary to Oestvall's teachings and purpose), only to generate network packets that are ultimately discarded by Rao's filter.

Neither Rao nor Oestvall, nor their combination, teaches or renders obvious that a processor would be operable to ***block*** a network packet (i.e., the alleged "Internet service access request") when an application is not classified as interacting with a user in the foreground, as required by limitation [1g] under the Petition's theory.

Specifically, for limitation [1g], the Petition alleges that the system's filter 322 "would selectively '<u>discard</u>' network packets (***block the Internet service access request***) from applications that are 'untrusted' [] and running in the background (***the particular application is not classified as interacting with a user in the device user interface foreground***)." Pet. at 37 (emphasis original). But neither Rao nor Oestvall discloses taking ***any*** action with regard to network packets on the basis of the application being "untrusted" and running in the background, much less configuring the device to consume power to generate packets for such applications only to use even more power to discard the same packets, as the Petition's theory requires. *See*

Pet. 37. Furthermore, the Petition fails to establish why a POSITA would be motivated to modify Rao's remote access client in such a manner.

By way of background, and as the Petition acknowledges, Oestvall discloses "preventing such [background untrusted] applications from running." Pet. 14; *see* Pet. 8, citing Ex. 1006 ¶[0023] (acknowledging that Oestvall "prevent[s] untrusted applications in the background from running (e.g., by preventing the application from 'being given any services or consuming any resources')"); Ex. 1006, ¶[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.* at Abstract (explaining that the invention "prevents the untrusted application from running, e.g. being given any services or consuming any resources"); *id.* at ¶¶[0008], [0016], [0017] (describing each of "a first aspect of the present invention," "a second aspect" of the invention, and "a third aspect" of the invention, each of which involves "prevent[ing] an untrusted application that is in the background from running in order to conserve system resources"). Thus, background untrusted applications are from prevented from using ***any*** system resources (CPU or memory) and cannot take ***any*** actions whatsoever (much less any actions that could generate network packets). Oestvall takes no action regarding network packets generated by background untrusted applications, because those

packets can never be generated and do not exist as such applications are prevented from running entirely.

Preventing background untrusted applications from running is not some optional way to implement Oestvall's system; rather it is a ***requirement*** of Oestvall's invention. *See id.* ¶[0014] ("[M]erely relying on an application to voluntarily cease running when notified that it is in the background is an inadequate strategy for untrusted applications. Instead, ***they <u>need</u> to be actively be prevented from running***."). Each of Oestvall's independent claims confirm that preventing background untrusted applications from running is the essence of Oestvall's invention. *See id.*, Claims 1 & 11 (both requiring "preventing an untrusted application that is in the background from running").

Oestvall further explains that there is good reason to prevent background untrusted applications from running in their entirety: such untrusted applications will "often run[] at full speed to update graphics, sounds, etc." and these operations "will still run in the background and drain the battery." *Id.* ¶[0019]. Furthermore, in battery-powered and multi-tasking systems (such as the mobile device the Petition alleges its combination would entail), preserving system resources such as power consumed by CPU activity is "especially valuable." *Id.* ¶[0021] (explaining that "actively prevent[ing]" a background untrusted application from running "denies it system resources and hence preserves power, as well as unnecessary CPU activity

associate with the untrusted application in [the] background," which "could be especially valuable not only in the context of portable, battery powered devices, but also a UPS (uninterruptible power supply) powered system"); *see also id.* ¶[0007] ("the problem of battery conservation is especially acute for multi-tasking devices, i.e. devices with an operating system that can run several applications at the same time."), ¶[0009] ("It is valuable to preserve system resources (CPU, power) in multitasking computing devices.").

But the Petition's proposed combination of Rao with Oestvall disregards Oestvall's stated requirement of preventing untrusted background applications from running. Instead, the Petition proposes that, contrary to Oestvall's teachings, such applications would be ***allowed*** to run and even generate network packets, but that such packets would be ultimately discarded by Rao's packet filter 322. *See* Pet. 14-15 (acknowledging that, "while Oestvall teaches increasing battery life by preventing such applications from running," the proposed combination does not do this and, instead, allows the untrusted applications to run in the background, where a filter "would selectively 'discard[]' network packets from applications that are 'untrusted' and running in the background"); *id.* at 37 (relying on discarding of packets generated by background untrusted applications that continue to run in meeting limitation [1g]).

The Petition's combination fails out at the outset because Oestvall teaches away from allowing background untrusted applications to continue to run and consume system resources (CPU, memory) and services, only to generate network packets that will all be discarded. Oestvall expressly teaches that for multi-tasking devices, "the problem of battery conservation is *especially acute.*" Ex. 1006 at ¶[0007]. Oestvall further teaches that it is "valuable to preserve system resources (CPU, power) in multitasking devices" and that for battery powered devices, "it is *especially valuable* to conserve system resources *wherever possible* since doing so can increase battery life." *Id.* at ¶[0009]. Accordingly, Oestvall teaches that untrusted applications in the background "***need to be actively prevented from running.***" *Id.* ¶[0014]. In view of these teachings, as well as Oestvall's stated purpose, a POSITA would understand that Oestvall teaches away from allowing background untrusted application to continue running, consuming resources, and draining battery—as the Petition proposes. *Meiresonne v. Google, Inc.*, 849 F.3d 1379, 1382 (Fed. Cir. 2017) ("A reference teaches away 'when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken' in the claim.") (quoting *Galderma Labs., L.P. v. Tolmar, Inc.*, 737 F.3d 731, 738 (Fed. Cir. 2013)); s*ee also Santarus, Inc. v. Par Pharm., Inc.*, 694 F.3d 1344,

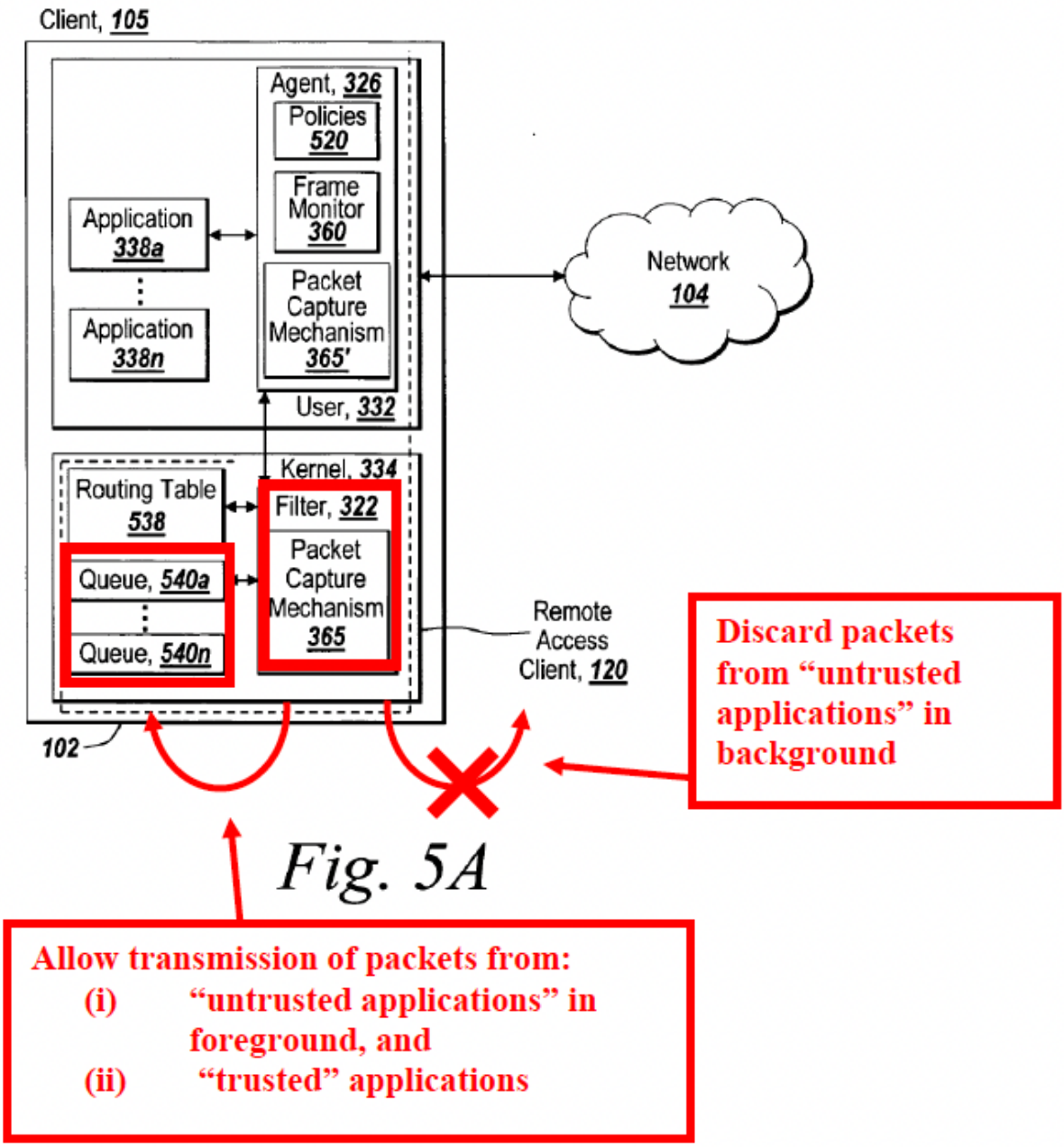
1355 (Fed. Cir. 2012) (holding that prior art reference taught away from an option when it "explicitly 'ruled out'" that option).

But even if Oestvall's disclosures do not rise to the level of teaching away, they clearly negate a finding of motivation to combine here.

The only rationale the Petition proposes for ignoring Oestvall's teachings that background untrusted applications must be prevented from running is that *allowing* them to run and discarding their packets "could be used to enable a similar increase in battery life by specifically preventing the battery draining activity identified by Oestvall." Pet. at 14, citing Ex. 1003 ¶80 (Petitioner's expert alleging that "[combined Rao-Oestvall] system can reduce battery drain while controlling the network activities of applications to a much greater degree of granularity than offered by Oestvall's relatively blunt approach of completely shutting down applications to achieve this benefit."). Notably, however, the Petition does not allege that a POSITA would have viewed Oestvall's "relatively blunt approach of completely shutting down applications" as detrimental in any way, such that they would ignore Oestvall's teachings that background untrusted applications "need to be prevented from running." Pet. 16-17; *see* Ex. 1006 (Oestvall), ¶[0014].

Indeed, the Petition does not allege that ***allowing*** untrusted background applications to run (directly contrary to Oestvall's teachings) would have ***any*** benefit at all. At most, the Petitioner's expert alleges that doing so would have "controll[ed]

the network activities of applications to much greater degree of granularity than offered by Oestvall's relatively blunt" solution. Pet. 14, citing Ex. 1003 ¶80. This is unfounded, however, because the Petition's own theory of invalidity for claim 1 involves ***discarding*** "network packets… from applications that are 'untrusted'… and running in the background." Pet. 37 (addressing the claim language of limitation [1g]). For instance, the Petition's annotation to Rao's FIG. 5A makes clear that the proposed combination would discard the network packets from untrusted background applications, while only allowing packets from trusted applications and untrusted applications in the foreground:



SAMSUNG-1005, FIG. 5A (annotated)

Pet. 16 (Petition's annotations of Rao's FIG. 5A); *id.* at 37 (relying on this same configuration that discards packets based on a determination that they originated from untrusted applications running in the background as allegedly satisfying limitation [1g]); Ex. 1003 ("Butler Decl.") at ¶81-83 (same) ; *see also* Pet. 37 (stating

that as a result of discarding packets from background untrusted applications, "these applications can no longer poll for data over a wireless network"); Ex. 1003 ¶84 (explaining that in the alleged combination, "an application's network packets… would be blocked on a permanent basis").

Thus, the Petition's proposed combination does not improve on Oestvall's low-granularity restriction on network activities of untrusted background applications (because the Petition's invalidity theory, like Oestvall, prevents such activities in their entirety), but the Petition's combination does so in a less effective manner from which Oestvall explicitly teaches away from. Furthermore, because Oestvall discloses that its allegedly "blunt" approach is beneficial and even mandatory, there is no competent evidence that a POSITA would have viewed ***avoiding*** that approach as beneficial. *See* Pet. 16.

The *only* evidence at all the Petition cites on this point is the *ipse dixit* opinion of its expert declaration. Pet. at 14 (citing Ex. 1003, ¶79-80). Because the expert declaration largely parrots the conclusory allegations of the Petition on this point, and cites provides no reasoned explanation or rationale for why discarding network packets would provide a "greater degree of granularity" than preventing those packets from being generated in the first place (*see* Ex. 1003 ¶80), it should be accorded little weight. *See* 37 CFR § 42.65 ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no

weight."); *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper No. 9 at 15 (Aug 24, 2022) (precedential) (denying institution and giving "little weight" to "cited declaration testimony [that] is conclusory and unsupported" and "adds little to the conclusory assertion for which it is offered to support").

The Petition further fails to acknowledge the significant ***disadvantages*** a POSITA would have recognized would result from disregarding Oestvall's mandatory teachings of preventing untrusted background applications from running. Specifically, Oestvall teaches benefits of denying untrusted background applications access to ***all*** system resources, not just network resources. *See* Ex. 1006, Abstract (explaining that the invention "prevents the untrusted application from running, e.g., being given ***any*** services or consuming ***any*** resources"). While prevention of network activity is "[o]ne example" of a benefit to Oestvall's disclosed technique (*id.* at ¶[0024]), Oestvall is clear that the prevention of preventing background untrusted applications provides the benefit of preventing consumption of ***any*** system resources, not simply resources associated with network activity. *See, e.g.*, *id.*, Abstract; *id.* ¶[0006] (explaining that "applications will continue to run even when in not actually in active use," and "will therefore continue to use ***some*** system resources, even when residing in the 'background'"); *id.* ¶[0008]-[0009] ("[T]he fact that [untrusted] applications can run in the background and consume some system resource is a waste of CPU and scheduler activity."); *id.* ¶¶[0019-0021] (explaining

that background untrusted applications can include "games or similar types of applications and, when these execute, the CPU is often running at full speed to update graphics, sounds etc."; accordingly preventing such applications from running "preserves power, as well as unnecessary CPU activity associated with the untrusted application in the background").

Thus, while the Petition alleges that discarding packets generated by untrusted background applications (supposedly motivated by Oestvall) may conserve some network resources, the Petition fails to motivate such a deviation from the solution actually taught by Oestvall. A POSITA would readily recognize that the Petition's approach (as compared to Oestvall's approach) would drain numerous additional resources such as resources associated with CPU and scheduler activity (including CPU activity required to generate the packets that Rao's filter would later spend energy to evaluate and discard, as well as battery-draining CPU activity ***not*** associated with network activity).[2] The Petition's proposal of a less power-efficient

[2] The Petition implies that Oestvall's power-saving goals could be equally achieved by the Petition's combination because "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." Pet. 14. Even if one were to assume this assertion to be true,

solution with no actual benefit of more granular network control is particularly unfounded because the Petition's alleged motivation to combine Rao with Oestvall in the first place is to "reduce battery drain." *See* Pet. 14 (section heading (b)). A POSITA motivated by the goal of reducing battery drain would have actively avoided replacing Oestvall's core teaching—preventing untrusted background

---

it is an admission that there is ***some*** power usage involved in generating network packets, and thus an admission that Petition's proposed combination is ***less*** battery-efficient than if background untrusted applications were prevented from running altogether. And in any event, the Petition completely ignores system resources that would be consumed by untrusted background applications for ***non-network*** activity under the Petition's proposed solution, which Oestvall teaches would have a significant and detrimental impact on battery consumption. *See* Ex. 1006 at ¶[0019]-[0020] (explaining that third party applications, which can come from "'untrusted' sources," can be "games or similar types of applications and, when these execute, the CPU is often running at full speed to update graphics, sounds, etc.," and thus "there is a risk that [these] application[s] will still run in the background and thus drain the battery"). The Petition does not dispute that allowing such applications to run would have a significant impact on battery consumption, even if these applications ***never*** attempted to use the network.

applications from doing ***anything***—with the Petition's significantly more battery-intensive approach that achieves the same non-granular restriction on network activities of untrusted background applications—having untrusted background applications run in the background only to have their network packets discarded anyways.

As another example, the Petition's approach also requires consuming system resources for untrusted applications running in the background in the form of the resources needed to select the appropriate network for the network traffic from such applications, which is yet another reason that a POSITA would not be motivated to pursue the Petition's proposed combination. For instance, the Petition requires "modifying Rao's system to first perform Montemurro's network selection prior to prioritizing network traffic according to the Rao-Oestvall combination." Pet. 22. The Petition explains that Montemurro's network selection involves selecting a specific network "from among multiple networks to transmit an application's network traffic," and it is only after the application is allowed to access a specific type of network that a decision regarding whether to discard the subsequently-generated network packets is made. The fact that the combined system would expend unnecessary resources routing packets from untrusted background applications that will eventually be discarded is visually shown in the Petition's annotation and revision to Rao's FIG. 5A (reproduced below), which makes clear that a packets are

first intercepted, then a routing table is used to select a network for transmitting those packets, and ***only then*** are those packets discarded.

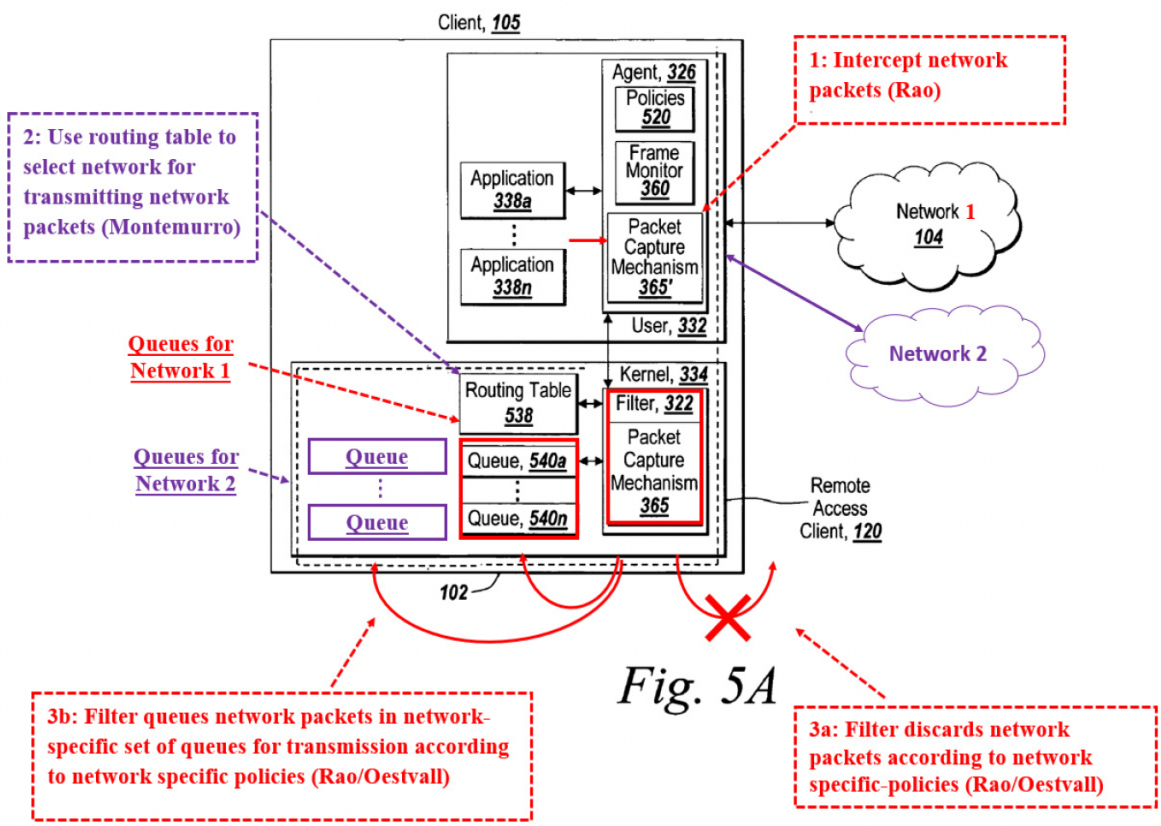


Fig. 5A

Pet. 21 (Petition's annotations and revisions).

Thus, under the Petition's theory, Montemurro's network selection step is performed ***first***, and it involves a modified routing table selecting the appropriate network for transmitting network packets from an application (based on "application type," "destination IP address," and "protocol"), and it is only upon successfully selecting a particular network that individual network packets are subsequently provided to the filter for prioritization or discarding. Pet. 20-21 ("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).”).

Accordingly, the Petition’s theory requires selecting a particular network appropriate for network packets for untrusted applications running in the background using a modified version of Rao’s routing table 338, only to discard the packets anyway. A POSITA motivated by the goal of reducing battery drain and the teachings of Oestvall would have prevented untrusted background applications from doing ***anything***, rather than adopt the Petition’s significantly more battery-intensive approach that still achieves the same non-granular restriction on network activities of untrusted background applications, albeit by expending considerably more power to do so.

It is apparent in view of Oestvall themselves that if a POSITA ***actually*** followed the teachings of Oestvall in a combination with Rao and Montemurro (rather than abandoning those teachings with the hindsight motivation of arriving at the claims of the ’445 Patent as the Petition does), the POSITA would have simply implemented Rao’s existing traffic prioritization policies while ***also*** preventing untrusted background applications from running, as required by Oestvall. In fact,

Petitioner has elsewhere argued the obviousness of that exact implementation of Rao in view of Oestvall, which implementation does ***not*** have the problem of ignoring Oestvall's stated "need" to actively prevent untrusted background applications from running. *See* Ex. 2001 (IPR2023-01253 Petition) Paper No. 2 at 11-13 (arguing that a "POSITA would have found obvious integration of Oestvall's resource conservation techniques into the Rao system," and that ***it would have been obvious to configure "the improved agent to prevent an untrusted application in the background from running"***); Ex. 2002 (IPR2023-01337 Petition) Paper No. 2 at 13-14 (same); Ex. 2003 (IPR2023-01336 Petition) at 13-14 (presenting the same theory that it would have been obvious to modify Rao in view of Oestvall to prevent background untrusted applications from running).

Notably, in each of IPR2023-01253, IPR2023-01336, and IPR2023-01337, Petitioner alleged that "[t]he elements of the resulting Rao-Oestvall system would each perform functions they had been known to perform prior to the combination." *See* Ex. 2001 (IPR2023-01253 Petition) at 15-16; Ex. 2002, IPR2023-01337 Petition at 16 (same); Ex. 2003, IPR2023-01336 Petition at 16 (same). Petitioner in those proceedings was able to allege as much, because the theories presented in those proceedings did ***not*** require disregarding Oestvall's teachings of preventing background untrusted applications from running. Tellingly, Petitioner is unable to make the same allegation in ***this*** proceeding, because the instant Petition proposes

modifying the functionality of Rao (to discard packets from background untrusted applications) and Oestvall (to allow background untrusted applications to run in the first place) in ways not taught or suggested by either reference, and explicitly taught away from by Oestvall.

The fact that the Petition does not identify any disclosure in the prior art that would suggest its proposed disregard for Oestvall's teachings of allowing untrusted background applications to run, and further presents no alleged benefit to that implementation (other than simply being a different way to achieve a lesser portion of the same benefits already achieved by Oestvall's technique as disclosed), is strongly suggestive of impermissible hindsight. *See* MPEP § 2142 ("[I]mpermissible hindsight must be avoided and ***the legal conclusion must be reached on the basis of the facts gleaned from the prior art***."); *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007) (stating that a "factfinder… must be cautious of arguments reliant upon ex post reasoning"). The only plausible reason to combine Oestvall with Rao to ***allow*** background untrusted applications to consume significant resources causing network packets to be generated (in addition to other resources unrelated to network activity)—only for those packets to be ultimately ***discarded*** en masse—is Petitioner's hindsight desire to point to the eventual discarding of those packets as allegedly satisfying limitation [1g]. *See* Pet. 37 (pointing to "selectively

'discard[ing]' network packets… from applications that are 'untrusted'… and running in the background" as allegedly satisfying limitation [1g]).

In sum, the Petition does not provide any reasoned analysis or evidentiary support for why a POSITA would have been motivated to modify Rao in view of Oestvall to allow background untrusted applications to run and then subsequently discard packets generated by those background untrusted applications. Thus, the Petition cannot show that it would have been obvious to modify Rao to "'discard' network packets… from applications that are 'untrusted'… and running in the background," which is the only aspect of the proposed combination that even allegedly satisfies the requirements of claim limitation [1g].

B. The Petition's theory also fails because prioritizing and discarding network packets after an application's Internet service access request has been granted does not constitute blocking the application's Internet service access request.

Even assuming counterfactually that a POSITA would have been motivated to modify Rao and Oestvall in the illogical way the Petition proposes, the Petition would still fail. This is because the Petition fails to show how its alleged Rao-Oestvall-Montemurro combination involves blocking any application's internet service ***access request***. The Petition's theory for limitation [1g] does not involve Internet service access requests at all, but instead only involves transmission or

prioritization of network packets after an access request ***has already been granted***. See, e.g., Pet. 12 (alleging "Rao's system controls each of the applications' access to the network by intercepting packets of network traffic by the applications…and selectively communicating the packets to the network based on the determined priority"); Pet. 28 (discussing "transmitting packets" as constituting an "attempt to access an Internet service"); *id.* 32 (alleging "the Internet service access request" is "an applications' network traffic"); *id.* 34-35 (alleging "the Internet service access requests embodied by those network packets" are controlled by "block[ing] the network packets from being transmitted"); *id.* 37 (alleging "selectively '<u>discard</u>[ing]' network packets" to be "block[ing] the Internet service access request)" to satisfy limitation [1g]).

The plain meaning of blocking an application's Internet service access request, however, requires blocking an application's "request" to access an Internet service, such as a request by the application to open a network connection or obtain an IP address. This is separate from discarding network packets ***after*** the Internet service access request has already been granted, and a corresponding network connection has been opened. In addition, the Petition's generic accusation of a "network packet" as an "access request" is insufficient, because sending a packet is merely sending data, and is not inherently a "request" for Internet access. Although

the Petition fails to address this fundamental distinction, it is readily apparent from the evidence accompanying the Petition, including the '445 Patent and Rao itself.

For example, Claim 1 of the '445 Patent clearly distinguishes between an "Internet service access request" and "data for Internet service activities." '445 Patent, Claim 1 (distinguishing a particular application's "Internet service access request" from its "Internet service activities" more generally). This distinction is likewise supported throughout the specification. For example, the '445 Patent separately discusses "***network access requests (e.g., IP address requests)***" and "network capacity/resources usage (e.g., bandwidth usage)" such as transmitting packets. Ex. 1001 11:27-32. The '445 Patent provides a further example of blocking a network access request (i.e., a request to connect to the network such as by opening a socket), such that the application needs to submit its network access request later: "As yet another example, ***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*** and a message is sent back to the application… **to** ***try again later for the requested network access.***" *Id.* 91:41-49.

Rao also makes clear that intercepting "network packets" occurs after an Internet services access request was previously granted. For instance, Rao clearly distinguishes between a ***request*** that opens a connection and the network ***packets***

communicated as payloads over that connection (after the connection has opened as a result of the access request being granted):

> The filter process intercepts the first and second packets from the application and forwards the intercepted packets to the tunnel process. ***The tunnel process requests the opening of a TCP connection*** between the first device and a second device. ***The request to open the TCP connection indicates to the first and second device that the TCP connection will transport packets*** intended to be transmitted with an unreliable transport protocol. ***The tunnel process forwards the first and second packets as payloads in a first and second TCP packet*** to the second device.

Ex. 1005 ¶[0030]; *see also id.* at ¶[0156] (describing FIG. 3B, in which step 365 will first "***establish a lossless protocol based connection***, such as a TCP connection, ***by which lossless protocol packets are communicated***" before communicating the packets in step 390).

Moreover, Rao is alleged to intercept network packets which include destination IP addresses and port numbers obtained over the Internet, meaning that Internet access was previously granted, and a connection opened, for the associated application. *Id.* ¶[0192] ("For example, intercepted network packets for an application communicating to a first destination IP address and a first destination port may be placed in a first queue 540a"); *id.* ¶[0187] (disclosing the comparison of "destination IP addresses and ports numbers with the IP addresses and ports

numbers of the network packet" to identify that a "network packet is associated with an application 338-338n").

Likewise, Rao teaches that connection sessions are established (such as by opening a socket) *before* data packets are communicated. *Id.* ¶[0050] (describing an embodiment in which first, "the method includes ***establishing the session*** via the first protocol of one of the following: 1) secure socket layer (SSL) protocol, 2) a transport layer security (TLS) protocol, and 3) a tunneling protocol. ***Additionally***, the method of the present invention may include ***communicating***, by the agent, ***real-time data via the session***…"), ¶[0159] (describing "a traditional TLS session where ***the session is first negotiated*** and ***the same socket is used for data communication***").

Accordingly, both the '445 Patent and Rao make clear that ***transmitting*** individual packets is distinct from ***granting*** *an Internet service access request*. Thus, selectively ***discarding*** (and thus *not* transmitting) a packet is likewise distinct from "***block[ing] an Internet service access request***" so that the requested Internet service (such as opening a network connection) is denied to the requesting application.

As noted above, the Petition's theory asserts that discarding network packets constitutes blocking the Internet service access request. *See* Pet. at 37 ("Specifically, the 'filter 322' would selectively '<u>discard</u>' network packets (***block the Internet service access request***)." This theory fails. As the Petitioner has acknowledged in

IPR2023-01361,[3] "an application's requests to access the Internet" are separate from "the network packets generated by that application" once the "application is permitted to access the Internet." Ex. 2004 (IPR2023-01361 Petition) at 25. Indeed, the Petitioner has explicitly and affirmatively argued that intercepting and discarding network packets with Rao's filter occurs only if "***an application is permitted to access the Internet.***" *Id.* 25 ("If an application is permitted to access the Internet…the network packets generated by that application would be filtered in accordance with the Rao-Oestvall combination, as described above…."). Accordingly, the fact that network packets are being filtered shows that the application's request to access Internet services was ***granted***—not ***blocked***, as all claims require. *Id.*

The fact that discarding of network packets requires that the application's access request was already granted is also confirmed by Rao, because in Rao,

[3] In IPR2023-01361, involving the same Petitioner and Patent Owner and involving U.S. Patent No. 9,271,184, the Petitioner also maps selectively ***discarding*** network packets to satisfy claim language requiring "***blocking the Internet service access request***" based on a theory of invalidity based on Rao combined with Oestvall. Ex. 2004 at 42 (alleging selective ***discarding*** of "***network packets***" to be "block[ing] the Internet service access request").

transmission of (or conversely, discarding) a network packet necessarily occurs after the Internet service access request (e.g., opening a connection) has already been granted. *See* Ex. 1005 ¶[0030] (***The tunnel process requests the opening of a TCP connection*** between the first device and a second device. ***The request to open the TCP connection indicates to the first and second device that the TCP connection will transport packets***); *see also id.* at ¶[0050] (describing "establishing the session" separately from "communicating… real-time data via the session"); *id.* at ¶[0156] (describing FIG. 3B, in which step 365 will first "***establish a lossless protocol based connection***, such as a TCP connection, ***by which lossless protocol packets are communicated***" before communicating the packets in step 390); ¶[00159] (describing "a traditional TLS session where ***the session is first negotiated*** and ***the same socket is used for data communication***"). Accordingly, discarding network packets does not constitute blocking any Internet service access request, and the fact that packets were even generated in the first place shows that any access request was previously ***granted***.

In sum, the Petition's Rao-Oestvall-Montemurro theory fails to show blocking an Internet services ***access request,*** as required by [1g]. And as for Montemurro, this additional reference does not cure the deficiencies in the Petition's theory. The Petition does not rely on Montemurro to show "block the Internet service access

request," and indeed, Montemurro's teachings are not relied upon in the Petition for any relevant aspects of [1g]. *See* Pet. at 15, 37-38.

VI. CONCLUSION

Patent Owner respectfully requests that the Board deny institution, as each of the Petition's grounds fails on the merits.

Date: January 4, 2024

Respectfully submitted,

/Reza Mirzaie/

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
James A. Milkey, Reg. No. 79,503
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 6,283 words in the paper excluding the portions exempted under 37 C.F.R. §42.24(a)(1).

Date: January 4, 2024

/Reza Mirzaie/

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
James A. Milkey, Reg. No. 79,503
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 January 4, 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)
FISH & RICHARDSON P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
IPR39843-0162IP1@fr.com
PTABInbound@fr.com
ptab@fr.com
jjm@fr.com
devoto@fr.com

Date: January 4, 2024

/Reza Mirzaie/
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
James A. Milkey, Reg. No. 79,503
RUSS, AUGUST & KABAT
12424 Wilshire Blvd., 12th Floor
Los Angeles, CA 90025

Counsel for Patent Owner