

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

**DECLARATION OF DR. ZYGMUNT J. HAAS IN SUPPORT OF PATENT
OWNER'S RESPONSE TO THE PETITION**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND AND QUALIFICATIONS	2
III.	LEGAL PRINCIPLES	6
A.	Claim Construction	6
B.	Burden of Proof	7
C.	Anticipation	7
D.	Obviousness	7
IV.	PERSON OF ORDINARY SKILL IN THE ART	9
V.	BACKGROUND OF THE '578 PATENT.....	10
VI.	CLAIM CONSTRUCTION.....	12
VII.	DR. MCDANIEL DOES NOT DEMONSTRATE THAT HIS PROPOSED COMBINATION DISCLOSES OR RENDERS OBVIOUS A “DIFFERENTIAL TRAFFIC CONTROL POLICY” MEETING ALL OF THE CLAIM 1 REQUIREMENTS.	13
A.	Rao does not disclose a “differential traffic control policy” such that any particular applications are only allowed to access the WWAN when they’re classified as interacting in the foreground.....	17
1.	Rao’s prioritization scheme relied on by Dr. McDaniel does not disclose this requirement.	17
2.	Rao’s teachings of discarding packets (not relied upon by Dr. McDaniel) also do not meet the claim requirements.	22
B.	Oestvall (alone or in combination with Rao) does not cure the deficiencies of Rao discussed above.....	30
1.	Oestvall does not disclose a “differential traffic control policy” applicable to WWAN but not WLAN.....	30

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.	32
3. Dr. McDaniel provides no motivation to allow a user to select which applications should be classified as “untrusted.”	36
VIII. DR. MCDANIEL DOES NOT SHOW THAT HIS PROPOSED COMBINATION DISCLOSES OR RENDERS OBVIOUS CLAIM ELEMENT [1E].	39
A. Dr. McDaniel’s reliance on Rao alone does not satisfy limitation [1e].....	40
1. Dr. McDaniel’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.	40
2. Dr. McDaniel’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.	42
3. Dr. McDaniel fails to motivate inclusion of Rao’s remote access client within an application subject to any differential traffic control policy, as Dr. McDaniel’s theory for limitation [1e] would require.....	43
B. Oestvall/Dive-Reclus do not cure the deficiencies of Rao’s API-related disclosures.....	46
C. Montemurro also does not cure the deficiencies of Rao and Oestvall/Dive-Reclus’s alleged API-related disclosures.	49
IX. CONCLUSION.....	52

I, Zygmunt J. Haas, hereby declare as follows:

I. Introduction

1. I am over the age of eighteen (18) years and otherwise competent to make this declaration.

2. I have been retained as an expert witness on behalf of Patent Owner for the above-captioned *inter partes* review (“IPR”). I understand that the petition for *inter partes* review involves U.S. Patent No. 9,521,578 (“the ’578 Patent”).

3. I make this declaration based on my personal knowledge, educational background and training, consideration of the materials I discuss herein, and my expert opinions.

4. I am being compensated at a rate of \$550 per hour for my time in this matter, in addition to reimbursement for expenses. My compensation does not depend on the outcome of this proceeding, and I have no financial interest in its outcome.

5. In preparing this Declaration, I have reviewed and considered the ’578 Patent, the ’578 Patent’s prosecution history, the Petition, the declaration submitted by Dr. McDaniel in this proceeding, the deposition transcript of Dr. McDaniel in this proceeding, and each document cited in this declaration.

II. Background and Qualifications

6. My qualifications for forming the opinions given in this declaration are summarized here and are addressed more fully in my curriculum vitae, which I understand is submitted as Exhibit 2007.

7. I am a Professor and Distinguished Chair in Computer Science at the Computer Science department of the University of Texas at Dallas. I also hold the title of Professor Emeritus at the School of Electrical and Computer Engineering at Cornell University. Over the years, I provided technical consulting services in intellectual property matters, which have included writing expert reports and providing deposition and trial testimony in the areas of my expertise, including wireless communication technologies.

8. I received my Doctor of Philosophy (Ph.D.) degree in the field of Electrical Engineering from Stanford University in 1988. As part of my Ph.D. program, I authored the thesis titled “Packet Switching in Fiber–Optic Networks.” I received my Masters of Science (M.Sc.) degree in Electrical Engineering, *summa cum laude*, from Tel-Aviv University in 1985 and my Bachelor of Science (B.Sc.) degree in Electrical Engineering *summa cum laude*, from Technion.

9. After receiving my Ph.D. degree from Stanford University, I worked in industry as a member of the technical staff at AT&T Bell Laboratories from 1988 to 1995, initially in the Network Research Department in Holmdel, New

Jersey. There, I performed research in the fields of wireless communications, mobility management, fast protocols, optical networks, and optical switching. During my tenure at AT&T, I also worked for the AT&T Wireless Center of Excellence, in Whippany, NJ. There, I studied various aspects of wireless and mobile networks.

10. After my work at AT&T Bell Laboratories, I joined the faculty of Electrical & Computer Engineering at Cornell University in 1995, and over time was promoted to Tenured Full Professor. While at Cornell, I headed my research group – the Wireless Networks Lab – which has had extensive contributions in the area of wireless communication systems and networks. In 2013, I retired from Cornell University with the title of Emeritus Professor, and subsequently I joined the Computer Science Department at the University of Texas at Dallas with the title of Professor and Distinguished Chair in Computer Science. Both, at Cornell University as well as at the University of Texas at Dallas, I have taught numerous courses related to computer network (at the undergraduate and graduate levels) and wireless communications. As part of my academic career, I have also served on numerous and various committees for the benefit of the scientific community.

11. In 2007, I was elevated to an IEEE Fellow, and in 2022, I was elevated to an ACM Fellow, both well-known distinctions. For example, the total number of IEEE Fellows which are selected in any given year does not

exceed 0.1% of the total number of voting members of IEEE. Alike, with respect to the ACM Fellow grade, ACM states that “ACM's most prestigious member grade recognizes the top 1% of ACM members for their outstanding accomplishments in computing and information technology and/or outstanding service to ACM and the larger computing community.” See <https://awards.acm.org/fellows>.

12. In 2016, I received the IEEE ComSoc AHSN Recognition Award for “outstanding contribution to securing ad hoc and sensor networks” from the IEEE Communication Society in 2016. In 2012, I have received the IEEE ComSoc WTC¹ Recognition Award, which recognizes individuals for outstanding technical contributions in the field for their service to the scientific and engineering communities. As another example, I received the “Best Paper Award” for the paper “Optimal Resource Allocation for UWB Wireless Ad Hoc Networks” from the IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC) conference in 2005. Finally, in 2003, I received the “Highly Commended Paper Award” for co-authoring “Performance Evaluation of the Modified IEEE 802.11 MAC for Multi-Channel Multi-Hop Ad Hoc Network,” directed at advanced information networking and applications. Furthermore, many of my papers have been extensively cited by other authors, as indicated by various

¹ Wireless Communications Technical Committee

citation indices. For example, my paper on “Securing Ad Hoc Networks,” co-authored with a Ph.D. student at the time, has been cited over 4000 times by other publications according to the *Google Scholar* index. I have been invited to many international conferences to make keynote speeches.

13. I am a named author on many book chapters, including “A Decision-Theoretical Approach to Resource Allocation in Wireless Multimedia Networks,” in *Resource Allocation in Next Generation Wireless Networks*, Volume 5, W. Li and Y. Pan, Editors, Nova Science Publishers, 2006, chapter 1, pp.1-23; “Providing Ad-Hoc Connectivity with the Reconfigurable Wireless Networks,” in *Ad-Hoc Networks*, edited by Charlie Perkins, Addison Wesley, 1998; and “Mobile-TCP: An Asymmetric Transport Protocol Design for Mobile Systems,” in *Mobile Multimedia Communications*, edited by D. J. Goodman and D. Raychadhuri, Plenum Publishing, 1997.

14. I am an inventor or co-inventor on over twenty issued patents, which are primarily in the fields of high-speed networking, wireless networks, and optical switching.

15. I have served on the editorial board for a number of professional journals including *Wireless Communications and Mobile Computing*, *Wireless Networks Journal*, and the *Journal of High Speed Networks*. I have served as guest

editor for the IEEE Journal on Selected Areas in Communications on several occasions.

III. Legal Principles

A. Claim Construction

16. I have been informed by counsel that the first step in performing a validity analysis of patent claims is to interpret the meaning and scope of the claims by construing the terms and phrases found in those claims. I have been informed by counsel that the appropriate construction of a claim term is its ordinary and accustomed meaning as would have been understood by one of ordinary skill in the art at the time of the invention in the context of the entire patent and the prosecution history.

17. I have been informed by counsel that standard for claim construction in an *inter partes* review is the same standard as is applied in district court proceedings.

18. I have been informed by counsel that a determination of the meaning and scope of the claims is a matter of law. I have been informed by counsel that to determine the meaning of the claims, one should consider the intrinsic evidence, which includes the patent's claims, written description, and prosecution history.

B. Burden of Proof

19. I have been informed by counsel that in an *inter partes* review, the petitioner has the burden of proving unpatentability by a preponderance of the evidence.

C. Anticipation

20. I have been instructed by counsel and understand that a reference is anticipated if a single prior art reference discloses each and every claim element, either explicitly or inherently, as arranged in the same way as in the claim. I have been informed by counsel that where even one claim element is not disclosed in a reference, a contention of anticipation fails.

21. I further have been informed by counsel that when a reference fails to explicitly disclose a claim element, that reference inherently discloses that element only if the reference must *necessarily* include the undisclosed claim element.

D. Obviousness

22. I have been instructed by counsel and understand that a combination of prior art references may render a claim obvious if, at the time of the invention, a person of ordinary skill in the art would have selected and combined those prior-art elements in the normal course of research and development to yield the claimed invention.

23. I have been informed by counsel that in an obviousness analysis, one should consider the *Graham* factors, including: the scope and content of the prior art; the differences between the claimed inventions and the prior art; and the level of ordinary skill in the art. I further been informed by counsel the obviousness analysis is to be performed on a claim-by-claim basis. I have been informed by counsel that a person of ordinary skill in the art is a person of ordinary creativity, not an automaton.

24. I have been instructed by counsel and understand that obviousness requires more than a mere showing that the prior art includes separate references covering each separate limitation in a claim under examination. I have been informed by counsel that obviousness requires the additional showing that a person of ordinary skill at the time of the invention would have been motivated to combine those references in a manner that would include all limitations of the challenged claim, and, in making that combination, a person of ordinary skill in the art would have had a reasonable expectation of success (i.e., would have reasonably expected to arrive at the proposed modification without undue experimentation).

25. I also have been informed by counsel that an obviousness analysis must be conducted with awareness of the distortion caused by hindsight bias and with caution of arguments reliant upon *ex post* reasoning. For instance, I

understand that when considering obviousness, I should put myself in the position of a person of ordinary skill in the field at the time of the invention, rather than considering new information that is known today, but was not known at the priority date of the challenged patent.

26. I have been informed and understand from counsel that the Supreme Court has recognized that inventions are nearly always “combinations of what, in some sense, is already known.” As a safeguard against hindsight bias, I thus understand that an obviousness determination should take into account whether any proposed modification to the prior art is more than the predictable use of prior art elements according to their established functions. I have been informed by counsel that if the proposed modification *is* more than the predictable use of prior art elements according to their established functions, that is an indication that the proposed modification is inventive, not obvious.

IV. Person of Ordinary Skill in the Art

27. Dr. McDaniel alleges that a person of ordinary skill in the art, as of the priority date of the '578 Patent, “would have had (1) at least a bachelor’s degree in computer science, electrical engineering, or 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 (McDaniel Decl.) ¶ 18. I agree with Dr. McDaniel that a POSITA would have had (1) at least a bachelor's degree in computer science, electrical engineering, or related field, and (2) at least three years of additional experience (including graduate experience) with networking, power consumption of networked computing devices, and/or wireless digital communication systems.

28. I have at least the qualifications of a person of ordinary skill in the art, and had such qualifications prior to January 28, 2009 (the date that Dr. McDaniel applies as the priority date of the '578 Patent—*see* Ex. 1003 ¶17).

V. Background of the '578 Patent

29. At a high level, the '578 Patent is 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.

30. 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 1.²

31. 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 (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”).

VI. Claim Construction

32. I am informed by counsel that claim construction is an exercise of interpreting disputed terms, to the extent needed to resolve any controversy between the parties; unless there are particular disputes that need resolution to

² All emphases in cited materials herein are added in this document, unless otherwise noted.

resolve a controversy between parties, terms are to be given their plain meaning in view of the specification. As explained below, it is my opinion that the theories raised by Dr. McDaniel fail because the proposed modifications would not have been obvious, and thus I do not provide any explicit constructions of any claim terms because that analysis is not necessary to evaluate Petitioner's and Dr. McDaniel's failure to show the obviousness of its proposed combination of references.

VII. Dr. McDaniel does not demonstrate that his proposed combination discloses or renders obvious a “differential traffic control policy” meeting all of the claim 1 requirements.

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

34. 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.

35. A POSITA would thus understand that Claim 1 requires that aspects of the differential traffic control policy be modifiable (user-settable) through a user interface such that one or more 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 application(s) “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].

36. The claim also 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.

37. This understanding, in which the application (selectable through a user interface) must be *blocked* from accessing the WWAN modem (such that the application is “only allow[ed]... to utilize the at least one WWAN” when that application is classified as interacting in the foreground), 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. 1001 at 13:37-42 (“block/allow” is 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 “queu[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).

38. Overall, in order for Dr. McDaniel to establish that claim 1 is obvious, he 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 he must **further** show that that same differential traffic control policy would be applicable to data for activities using the WWAN and is **not** applicable to data for activities using the WLAN. Dr. McDaniel

at paragraphs 96-100 of his declaration 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).

39. As explained below, Dr. McDaniel’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.

A. Rao does not disclose a “differential traffic control policy” such that any particular applications are only allowed to access the WWAN when they’re classified as interacting in the foreground.

1. Rao’s prioritization scheme relied on by Dr. McDaniel does not disclose this requirement.

40. 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, Dr. McDaniel asserts 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 (i) 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*.” Ex. 1003 ¶96.

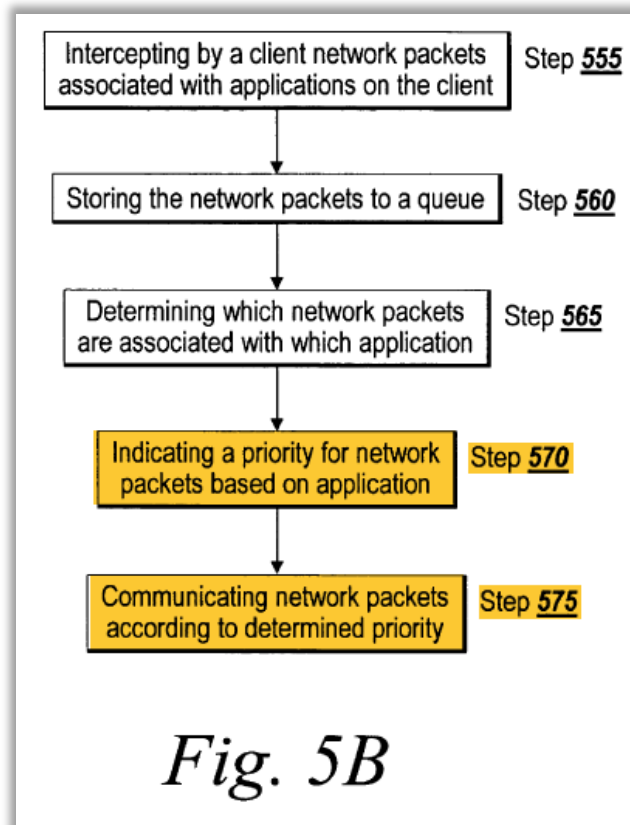
41. However, this is not what the claim requires. Rather, the claim requires access to the WWAN modem is allowed to a particular user-selectable application *only if* that particular claimed application is classified as interacting with a user in the foreground. If that condition is not met (e.g., if the application is not classified as interacting with a user in the foreground), the application is not permitted to access the WWAN modem at all (rather than merely assigned a lower priority within a queue as Rao teaches).

42. Contrary to this requirement, Dr. McDaniel recognizes that even in his 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.* ¶96. Dr. McDaniel 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 Rao's prioritization scheme does not.

43. Rather, 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. 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.

44. 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").

45. Indeed, as noted above, Dr. McDaniel 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. Ex. 1003 ¶96. In other words, Dr. McDaniel 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, there appears to be no dispute 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.

2. Rao's teachings of discarding packets (not relied upon by Dr. McDaniel) also do not meet the claim requirements.

46. As shown above, Dr. McDaniel's theory as set forth in his declaration relies only on Rao's queuing system for the claim element [1d]. *Id.* at 32-33. Notably, Dr. McDaniel does *not* rely on disclosures in Rao that address circumstances when an individual packet may be *discarded* to show claim element [1d] is satisfied. *Id.* However, I have been asked to explain why Rao's teachings regarding discarding packets would still not satisfy the claim elements [1d], even though I do not understand Dr. McDaniel to set forth any such theory.

47. Rao limits its discussion to discarding individual network packets in scenarios where (1) a network disruption or congestion occurs, or (2) network disruption/congestion is *not* occurring, but a packet is classified as "unwanted." As

explained in further detail below, even if discarding of individual network packets when the application that generated the packets is not running in the foreground could satisfy this claim limitation, neither of these two scenarios does so, and Dr. McDaniel does not allege any motivation to modify Rao's teachings regarding discarding packets.

48. Turning to the first of these scenarios, Rao teaches that certain packets can be discarded during a network disruption. *See* Ex. 1005 ¶[0207]. However, discarding packets **during a network disruption** does not constitute “**only allow[ing specified applications] to utilize the at least one WWAN when those applications are classified as interacting with the user in the device user interface foreground,**” and otherwise disallowing access, as required by claim 1. At most, it would teach only allowing particular applications to access the WWAN **when the WWAN network is not disrupted**. Specifically, network disruption is caused by factors in the network, and not by whether particular applications are running in the foreground or background on the device.

49. Furthermore, even assuming that the entirety of certain applications' packets were discarded during a network disruption on the basis of that application not being classified as interacting with a user in the foreground (something Rao does not teach or render obvious), Rao does not teach that it would **only** allow those applications to access the WWAN network when they're not classified as

interacting in the foreground; to the contrary, Rao teaches that it attempts to reestablish connectivity without reference to the foreground or background classification of any application, such that no policy would prevent any background applications from accessing the WWAN modem. *See id.* at Fig. 6B, ¶¶[0208]-[0209] (discussing re-establishing the “network connection” and “[c]ontinuing with session” automatically and without checking on the foreground or background status of any application).

50. In sum, as soon as the network disruption concludes and Rao has reestablished connectivity, all applications (regardless of foreground/background status) are allowed to utilize the WWAN. Thus, there is no policy in Rao such that any applications are *only* allowed to utilize the WWAN “when classified as interacting with the user in the device user interface foreground,” as required by limitation [1d].

51. Another instance where Rao teaches discarding packets is where certain network packets may not be communicated due to “network[] factors, such as congestion, even though the network packets may have a higher priority than other network packets in a queue.” *Id.* ¶[0195]. Again, Dr. McDaniel does not rely on this teaching of Rao in his discussion of the “applications ... only allowed to utilize the at least one WWAN *when those applications are classified as interacting with the user in the device user interface foreground*” limitation (*see*

Ex. 1003 ¶¶96-100). In my opinion, Rao’s teaching of discarding packets due to network factors would not satisfy this claim requirement. Specifically, Dr. McDaniel’s theory is based on an allegation that in Rao, an application’s background status leads to *low-priority* queuing of that application’s packets, as compared with packets from applications running in the foreground. In contrast, Rao’s teaching of discarding packets due to network factors (e.g., Ex. 1005 ¶[0195]) teaches discarding packets for reasons *other than* priority. *See* Ex. 1005 ¶[0195] (discussing discarding particular network packets “even though the network packets may have a higher priority than other network packets in a queue”). Thus, Rao does not teach discarding packets on the basis that they are background packets (which would be low-priority packets under Dr. McDaniel’s theory) as would be required for this discarding of packets to even potentially satisfy the claim language. Accordingly, Rao’s network congestion scenario does not teach or suggest *only* allowing any applications to access the WWAN “when those applications are classified as interacting with the user in the device interface foreground,” as claimed.

52. Turning to the second scenario mentioned above, where the network is *not* disrupted or congested, Rao provides only the following disclosure:

The filter 322 may use a filter table for filtering packets. The filtering table is used to determine what action to take against packets,

such as packets intercepted by the packet capture mechanism 365. *The filter 322 can inspect the contents of the packets, such as routing information, to determine the action to take based on the filtering table.* In some embodiments, the *filter 322 may drop or accept the network packets **depending on their content**.* In other embodiments, the filter 322 may route the network packets to the agent 326 based on the packets content and/or the filtering table. *The filter table may also be used to ensure that **unwanted packets are discarded**.* The filter 322 may be used to *deny access to **particular protocols** or to prevent unauthorized access from remote computers by **discarding packets to specified destination addresses**.*

Id. ¶[0102]. As shown above, this disclosure of discarding “unwanted” packets teaches three categories of information on which a decision is made that a packet should be discarded—the “content” of the packet, the packet’s “protocols,” and the packet’s “destination address[.]” *Id.* None of these are disclosed as being based in any part on whether an application is not interacting with a user in the foreground (as claim 1 of the ’578 Patent would require), and Dr. McDaniel does not supply any motivation to modify Rao’s operation in this respect.

53. First, Rao teaches that packets may be discarded “depending on their content” (e.g., “routing information”). *Id.* However, there is no teaching in Rao or allegation by Dr. McDaniel that the “content” of a packet would indicate whether the packet was from an application not interacting with a user in the foreground;

for example, an application may transmit a packet having a given content (e.g., routing information) while interacting with a user in the foreground; likewise, that same application could transmit a packet having *identical* content (e.g., routing information) while running in the background. Because the foreground or background status of an application in Rao does not affect the content of packets from that application, discarding packets in this scenario could not constitute only allowing an application access to the WWAN modem when the application is interacting with a user in the foreground.

54. Rao also teaches that packets may be deemed “unwanted” and thus discarded if they are using “particular protocols” and packets directed to “specified destination addresses.” *Id.* But again in Rao, neither which protocol is used for communication, nor the destination address of a given packet, depends on whether the corresponding application was not interacting with a user in the foreground. For instance, applications can use the same protocols and destination addresses when running in either the foreground or the background. Accordingly, discarding packets based on a specified protocol or destination address does not constitute only allowing application access to the WWAN modem when the application is interacting with a user in the foreground.

55. Further, Rao discusses filtering out “unwanted packets,” which are discarded entirely, as a mechanism wholly distinct from assigning packets a

priority for eventual communication. *Compare id.* ¶[0102] (discussing packets being “unwanted” by virtue of the “protocols” they use or their “destination addresses”) *with 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.”); *id.* ¶[0194] (“[T]he 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”).

56. More generally, there is no allegation or disclosure that packets would be considered “unwanted packets” based on a determination that the corresponding application was not interacting with a user in the foreground. While Rao *is* alleged to teach that packets generated by applications not running in the foreground (for example, those running in the background) may be given lower priority than packets generated by applications running in the foreground (*see* Pet. at 31; *see also* Ex. 1005 ¶¶[0046], [0189]), this is in the context of assigning packets from applications running in the foreground a higher queuing priority than packets from

applications running in the background. Rao never suggests **discarding** packets of an application based on a determination that the application is not running in the foreground. Indeed, as mentioned above, Rao is explicit that “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** in a manner according to or consistent with the determined priorities” (Ex. 1005 ¶[0194]), and Rao never suggests that its system is configured to **discard** low-priority packets, including those from applications not running in the foreground, when there is no network disruption.

57. Accordingly, Dr. McDaniel fails to show that a POSITA would have found it obvious to use Rao’s alleged differential traffic control policy to “only allow[applications] to utilize the at least one WWAN for Internet service activities when those applications are classified as interacting with the user in the device user interface foreground,” as required by all challenged claims. As shown above, the mechanism of queueing packets relied on by Dr. McDaniel does not satisfy that limitation. And Dr. McDaniel does not rely on a theory that discarding packets satisfies that limitation for good reason, because Rao’s discarding of certain packets would not satisfy that limitation either.

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

58. As noted above, Dr. McDaniel 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” (Ex. 1003 ¶96) 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.

59. I note that Dr. McDaniel additionally relies on Oestvall’s “prevent[ing] the untrusted [background application] from running” (Ex. 1006 ¶[0023]; *see* Ex. 1003 ¶97 (citing same)) as constituting “activity associated with [an untrusted background application] being *allowed only when* the application is running in the foreground.” Ex. 1003 ¶97 (emphasis in original). As explained below, I disagree that Oestvall cures the shortcomings of Rao in this manner.

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

60. For the requirement that particular applications be allowed to access the WWAN modem only when they are 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).

61. As Dr. McDaniel acknowledges, in his Rao-Oestvall combination, where Rao’s application 338 is an untrusted application presently in the background, the Oestvall-like scheduler “would *‘prevent[] the [application 338] from running,’* e.g., ‘operate so as to *never allocate any services or resources to the [application 338].*” Ex. 1003 ¶97 (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. 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].

62. However, Dr. McDaniel presents no evidence or allegation that preventing applications from running somehow *would* have been applicable to prevent only WWAN activity but *wouldn't* have been applicable to prevent WLAN activity. Accordingly, even assuming Oestvall's preventing untrusted applications from running altogether constituted a "differential traffic control policy" (something I do not understand Dr. McDaniel to allege), 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 Dr. McDaniel acknowledges, preventing applications from running in the background would have operated "so as to never allocate *any services or resources* to the [application].'" Ex. 1003 ¶97 (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, and Dr. McDaniel 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.

63. 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, Dr. McDaniel does not explain *how* a POSITA would have arrived at such a combination—for example, he 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.

64. My best understanding of Dr. McDaniel’s theory 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. For instance, Dr. McDaniel 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.” *See, e.g.*, Ex. 1003 ¶67 (discussing the “Combination of Rao and Oestvall” combination in the Dr. McDaniel’s Section XI.A).

65. 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) would be applicable to prevent background untrusted applications from receiving *any* services that consume resources, including WLAN services.

66. Other than simply preventing background untrusted applications from running, Dr. McDaniel 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, Dr. McDaniel 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.

67. Dr. McDaniel’s failure to provide such a theory is unsurprising, because in his 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.” *See* Ex. 1003 ¶67.

68. Dr. McDaniel's theory is 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]. Dr. McDaniel 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* Ex. 1003 ¶67 ("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 Dr. McDaniel's proposed combination.

69. 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 using a differential traffic control policy applicable only to data communicated over the WWAN modem.

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

70. 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, Dr. McDaniel 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* Ex. 1003 ¶97 (explaining that the “Oestvall-like scheduler” would apply to “an untrusted application presently in the background”).

71. 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.” However, Dr. McDaniel provides no motivation to place this important classification into the hands of the user, and indeed, Oestvall counsels against such a modification.

72. Specifically, Oestvall teaches that whether an application is trusted or not should **not** be decided by a user. 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].

73. Dr. McDaniel 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. 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. *Id.* ¶¶[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].

74. In my opinion, a POSITA would have understood 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]). For example, a POSITA would recognize that 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 id.* ¶[0019]. Thus, a POSITA would understand that a typical 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].

75. Indeed, a POSITA would recognize that 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 potential security risks. A POSITA would thus realize it would 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].

76. Accordingly, Dr. McDaniel 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.

VIII. Dr. McDaniel does not show that his proposed combination discloses or renders obvious claim element [1e].

77. 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.

78. As explained below, it is my opinion that Dr. McDaniel does not point to anything in Rao, Oestvall, or Montemurro that teaches this limitation, or identify how the combination of these references would render this limitation obvious.

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

1. Dr. McDaniel’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.

79. Dr. McDaniel’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]). Dr. McDaniel 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.

80. Put more simply, Dr. McDaniel’s logic is that, based on Rao’s teachings, some application could include a 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.

81. 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.*” 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.*”

82. Accordingly, for Dr. McDaniel’s Rao-based theory to succeed, he 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 further detail below, Rao does not disclose placing the remote access client within an application that is governed by

the differential traffic control policy, and in my opinion Dr. McDaniel does not show that such a solution would have been obvious because he does not provide any motivation for doing so.

2. Dr. McDaniel’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.

83. Despite Dr. McDaniel’s reliance on Rao teaching that “remote access client 120” “may be included within an application” (Ex. 1003 ¶104) (quoting Ex. 1005 ¶[0115]), Rao does not specify how this would be configured—for example, Rao does not specify which application a remote access client would be included within. For instance, Rao does not teach that the remote access client would be included within an application that is actually subject to a policy that the remote access client is responsible for enforcing.

84. My opinion is supported by Dr. McDaniel’s testimony at his deposition, in which he testified that Rao does not expressly teach *which* application the “remote access client” would be included within, in particular stating that “*Rao is sort of non specific about which application*” Dr. McDaniel proposes that the remote access client would be included within. Ex. 2008 at 6:16-7:6.

85. Accordingly, because Rao is “non specific” (as Dr. McDaniel testified) about which applications would include a remote access client within them (*see, e.g.*, Ex. 2008 at 6:22-7:6), Dr. McDaniel 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.

86. However, as explained in the following subsection, Dr. McDaniel does not 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.

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

87. As explained above, Dr. McDaniel’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 be included within such an application.

88. Dr. McDaniel also does not show (or 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)

within an application that is subject to the differential traffic control policy. *See* Ex. 1003 ¶¶101-104 (no discussion of any motivation to pursue such an implementation in Rao). Rather, Dr. McDaniel merely asserts that “the API allows the application 338 to access one or more of the policies 520 that are configured for that application.” Ex. 1003 ¶104 (citing Ex. 1005, FIG. 5A). But Figure 5A of Rao does *not* show that any API allows an application to access one or more policies configured for that application—for example, the bidirectional arrow of FIG. 5A between application 338a and Rao’s remote access client 120 simply represents that *data* (not necessarily information about the policies applicable to the application) is transmitted between the application and the remote access client, which is obviously necessary because the application relies on the remote access client to send and receive data via the modem and network.

89. Furthermore, it is my opinion that placing a remote access client within an application subject to Rao’s prioritization policies would have made no sense, because it would place responsibility for enforcement of the policy within the applications that are subject to the policy. A POSITA would recognize that this would be problematic because it would allow the application to circumvent, disregard, or take advantage of, 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. 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.

90. 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 Dr. McDaniel'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. In my opinion, no POSITA would have pursued such an implementation.

91. Finally, Dr. McDaniel 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.” Ex. 1003 ¶107. But Dr. McDaniel does not allege that Rao discloses any “Java sockets API,” and indeed Rao does not. Dr. McDaniel 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.

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

92. Dr. McDaniel 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.” Ex. 1003 ¶¶105-106 (citing Ex. 1006 ¶[0020]; Ex. 1026 at 16:23-17:28, 20:1-12) (footnote omitted)). However, Dr. McDaniel 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 Dive-Reclus does not. Instead, 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. I do not see how this disclosure is relevant to whether

limitation [1e] is obvious, because it says nothing about the application accessing aspects of a differential traffic control policy via an API.

93. Based on the above irrelevant disclosure of Dive-Reclus, Dr. McDaniel asserts 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” (Ex. 1003 ¶106), with no explanation of what API he 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, Dr. McDaniel simply provides no *motivation* to arrive at the claim’s API limitation in view of Dive-Reclus.

94. 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 somehow part of 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 Dr. McDaniel 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 aspect of the policy only allows the application to utilize WWAN when those applications are classified as interacting in the foreground), and he likewise does not allege that Oestvall (or Dive-Reclus) renders doing so obvious. For example, Dr. McDaniel provides no motivation to pursue such an implementation of Dive-Reclus’ API or any other API. Accordingly, it is my opinion that Dr. McDaniel provides no evidence 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.”

95. Dr. McDaniel also alleges that (a) “based on disclosure of API usage in Rao and Oestvall, the improved agent in Rao-Oestvall-Montemurro would have leveraged several types of APIs in *regulating applications*,” and (b) “a POSITA would have understood found obvious that APIs leveraged by the improved agent of Rao-Oestvall-Montemurro includes [sic] those described in Rao and Oestvall, as well as 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.” Ex. 1003 ¶¶106, 108. Not only are these allegations not supported by

any specific evidence, in my opinion they are also not relevant to the claim limitation at hand. For instance, Dr. McDaniel does 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” as limitation [1e] requires. Notably, the claim does not simply require an API, but requires an API “that allows a particular application to access one or more aspects of the differential traffic control policy applicable to that application.”

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

96. Dr. McDaniel further asserts that “a POSITA would have understood and found obvious that Montemurro’s API (e.g., socket-based API 206), implemented by the processor, operates to allow a particular application 204 to access ‘various factors’ (*aspects*) of one of ‘a set of rules/policies’ (*differential traffic control policy*) in the rules engine 206A, which is applicable to that particular application.” Ex. 1003 ¶109 (emphases in original).

97. However, it is my opinion that Montemurro contains no such disclosure or suggestion. 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 the reference 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).

98. Dr. McDaniel 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.” Ex. 1003 ¶109 (quoting Ex. 1007 ¶[0035], claim 7) (alteration in original). Dr. McDaniel, however, 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. Ex. 1007 ¶[0035].

99. Finally, Dr. McDaniel 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.

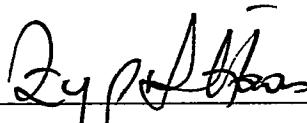
100. Accordingly, because Dr. McDaniel does not establish that Montemurro discloses limitation [1e] or that a POSITA would have been motivated to modify any APIs disclosed in Montemurro to arrive at limitation [1e], he does not show that Montemurro (alone or in combination with Rao, Oestvall, or Dive-Reclus) discloses or render limitation [1e] obvious.

IX. CONCLUSION

101. In signing this declaration, I understand that the declaration will be filed as evidence in contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

102. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable under Section 1001 of Title 18 of the United States Code.

July 2, 2024



Dr. Zygmunt Haas