

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD., GOOGLE LLC,
and SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioners,

v.

HEADWATER RESEARCH LLC,
Patent Owner.

Case IPR2024-01337
Patent 8,588,110 B2

**DECLARATION OF DR. MICHAEL C. BROGIOLI IN SUPPORT OF
PATENT OWNER'S RESPONSE**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND AND QUALIFICATIONS	2
III.	LEGAL PRINCIPLES	6
A.	Claim construction	6
B.	Burden of Proof	6
C.	Anticipation	7
D.	Obviousness	7
IV.	PERSON OF ORDINARY SKILL IN THE ART	9
V.	CLAIM CONSTRUCTION.....	9
VI.	OVERVIEW OF THE '110 PATENT	10
VII.	OPINIONS REGARDING CLAIMS 1, 26, AND 27	11
A.	None of the Dr. McDaniel's three alleged service policies would have been obvious.	12
1.	The Petition's First Theory: Reducing Frequency of Jones' Backups	13
2.	Dr. McDaniel's Second Theory: Prohibiting Jones' Backups on GSM Networks While Allowing Backups on CDMA Networks	17
3.	Dr. McDaniel's Third Theory: Assigning Packets to Different Queues Between GSM and CDMA Networks	20
B.	Dr. McDaniel also fails to establish obviousness of providing a user interface to modify the alleged policies satisfying limitation [1.7].	26
VIII.	CLAIM 4	30
IX.	CLAIMS 5 AND 28.....	31
X.	CLAIM 6	31

XI.	CLAIM 25	32
A.	Overview of Dr. McDaniel’s Motivation to Combine.....	32
B.	Dr. McDaniel provides no motivation to modify Ibrahim/Jones as he alleges.	34

I, Michael C. Brogioli, PhD, 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 Headwater Research LLC (“Headwater”) for the above-captioned *inter partes* review (“IPR”). I understand that the petition for *inter partes* review involves U.S. Patent No. 8,588,110 (“the ’110 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 \$750 per hour for my time in this matter. 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 ’110 patent, the ’110 patent’s prosecution history, the Petition, Dr. McDaniel’s declaration submitted in this proceeding, Dr. McDaniel’s deposition transcript, and each document cited in my 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 is submitted as Exhibit 2002. That exhibit also includes a list of my publications.

7. I am currently an Adjunct Professor of Electrical and Computer Engineering at Rice University in Houston, TX, teaching Ph.D. candidate level courses in wireless telecommunications, embedded computing software, embedded computing hardware, and software/hardware design. I have held this position since July 2009. I am also currently the Managing Director of Polymathic Consulting in Austin, TX, a company that advises a variety of clients on engineering, research and development, intellectual property, and other technical leadership matters, and I have held this position since October 2011.

8. I am a named inventor on multiple issued and pending patent applications. The subject matter of these applications includes, but is not limited to, embedded processing, edge computing, and various aspects of distributed systems including computation, interconnectivity and hardware/software design and implementation.

9. From November 2009 to October 2011, I was Chief Architect, Senior Member Technical Staff at Freescale Semiconductor in Austin, TX (formerly Motorola), responsible for management of technology, engineering roadmaps,

design lead on compiler infrastructure and optimizations for mobile and embedded computing solutions, including the types of security and encryption technologies involved in this matter. From 2007 to 2009, I was a Senior Engineer working with high performance compiler design and next generation baseband compiler design and next generation baseband microprocessor and microcontroller architecture at Freescale Semiconductor in Austin, Texas, including regarding communications networks and how mobile device architecture and design interacts with network elements.

10. From June 2006 to August 2007, I worked as the Technical Co-Founder of Method Seven LLC, in Boston, MA, working with high performance software and hardware systems architecture. I am currently the co-founder, co-inventor, and Chief Technology Officer of Network Native, an Internet of Things hardware and software company. I have also served on multiple advisory boards for technology companies over the past 10 years.

11. While at Rice University, I developed various computer architecture designs. For example, from 2002 to 2004, I developed Spinach, a simulator design toolset for modeling programmable network interface architectures, which models system components common to all programmable computing environments as well as components relating to embedded computing, wireless and mobile devices. From 2004 to 2009, I developed Spinach DSP-FPGA, a modular and composable

simulator design infrastructure for programmable and reconfigurable embedded SOC architectures specifically targeting mobile, embedded and portable computing devices. From 2005 to 2009, I developed and published a retargetable compiler infrastructure for software and systems related to mobile and embedded computing technologies. Many of these tools have been used at U.S. universities in the area of electrical and computer engineering research.

12. I am recognized as an expert in the field of communications systems, including computer architecture, hardware, and software as they relate to the subject matter at hand. I am a member of the Institute of Electrical and Electronics Engineers (IEEE). I am currently the Program Chair of Design Automation Conference in the areas of Embedded and Wireless Solutions. I have been a Program Committee member for the IEEE and ACM Design Automation Conference from 2011 to the present, as well as other IEEE and ACM conferences. I have published, co-published and contributed to numerous works on wireless and mobile computing, digital networking, Internet of Things technology, software and hardware optimizations, and digital signal processing and related architectures among other topics.

13. I have previously served as an engineering consultant and testifying witness on matters related to, and including Internet and communications technologies such as those at hand in this matter. This experience is encompassed

in my work in academia and as a faculty member, my time in industry as a system designer and architect, as well as my work as an engineering consultant and expert witness over the past 15 years.

14. Over the past 20+ years, I have authored numerous peer reviewed publications in the area of embedded and high performance computing, interconnect technologies, computer networking at the server and mobile handset level, and optimization at the hardware and software design level. I have also been a committee member, and chair of Design Automation Conference in areas of technology related to the '110 Patent, often reviewing and vetting submissions from major industry players often related to technologies at issue in this matter.

15. During my tenure at Freescale Semiconductor, I was in charge of system developer tools for baseband processor design, both in the hardware and software spaces. This work included hardware and software design issues of next generation wireless networking equipment, including system level programming models, interconnect technology, heterogeneous computing, various hardware acceleration technologies and related components.

16. My current curriculum vitae, provided in Exhibit 2002, contains more information on my background and experience, as well as the cases in which I have served as an expert witness the past four years.

17. No part of my compensation is contingent upon the outcome of this litigation. I have no other interests in this litigation or with any of the parties.

III. LEGAL PRINCIPLES

A. Claim construction

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

19. I understand that standard for claim construction in an *inter partes* review is the same standard as is applied in district court proceedings.

20. I understand that a determination of the meaning and scope of the claims is a matter of law. I have been informed 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

21. I understand that in an *inter partes* review, the petitioner has the burden of proving unpatentability by a preponderance of the evidence. I further understand that for an *inter partes* review to be instituted, the petitioner must show

a reasonable likelihood that the petitioner would prevail with respect to at least one of the claims challenged in the petition.

C. Anticipation

22. 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 understand that where even one claim element is not disclosed in a reference, a contention of anticipation fails.

23. I further understand 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

24. 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.

25. I understand that in an obviousness analysis, one should consider the *Graham* factors: the scope and content of the prior art; the differences between the claimed inventions and the prior art; the level of ordinary skill in the art; and

certain secondary considerations, identified below. I further understand the obviousness analysis is to be performed on a claim-by-claim basis. I understand that a person of ordinary skill in the art is a person of ordinary creativity, not an automaton.

26. 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 understand 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*.

27. I also understand 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 before the priority date of the challenged patent.

28. In particular, I understand that it is improper to use the challenged patent's disclosure or invention as a roadmap to find its prior-art components,

because such an approach discounts the value of combining various existing features or principles in a new way to achieve a new result.

IV. PERSON OF ORDINARY SKILL IN THE ART

29. Dr. McDaniel states that a POSITA would have had “(1) at least a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in wireless communication security. Additional advanced education could compensate for a deficiency in work experience, and *vice versa*.” Ex. 1003, ¶24.

30. For purposes of this declaration, I do not dispute Dr. McDaniel’s proposed level of skill in the art.

31. I further note that I am a person of ordinary skill in the art, and was such a person as of the priority date of the ’110 patent.

V. CLAIM CONSTRUCTION

32. Dr. McDaniel proposes construction of various “means” terms. Because my opinions are not dependent on the meaning of any of those terms, I do not offer any opinion on Dr. McDaniel’s proposed constructions. For each claim limitation at issue, I apply what I believe would have been the plain and ordinary meaning to a POSITA in light of the specification and file history of the ’110 patent.

VI. OVERVIEW OF THE '110 PATENT

33. The challenged claims of the '110 Patent (claims 1–30) are directed to wireless devices that store a service policy that controls a specific service activity on one wireless network differently than how the service activity is controlled on a second wireless network, and which also have agents configured to obtain user inputs specify an aspect of the claimed service policy.

34. Independent claim 1 is generally representative, and recites:

[1.1] A wireless device comprising:

[1.2] one or more modems for enabling the wireless device to communicate over at least two wireless networks, the at least two wireless networks comprising a first wireless network and a second wireless network;

[1.3] a user interface;

[1.4] memory configured to store:

[1.5] a first service policy associated with the first wireless network, the first service policy configured to at least assist in reducing data usage associated with a first service activity over the first wireless network,

[1.6] the first service activity being less than all service activities available to the wireless device,

[1.7] the first service policy for enabling control of the first service activity on the first wireless network that is different from how the first service activity is controlled on the second wireless network; and

[1.8] one or more processors for executing one or more agents, the one or more agents configured to:

[1.9] obtain, through the user interface, a user input specifying at least an aspect of the first service policy,

[1.10] identify that the wireless device is connected to the first wireless network,

[1.11] identify an intended, attempted, or successful data communication over the first wireless network, the intended, attempted, or successful data communication over the first wireless network being associated with the first service activity, and

[1.12] apply the first service policy.

Ex. 1001, claim 1.

35. As shown above, the “first service policy” must be “for enabling control of the first service activity on the first wireless network that is different from how the first service activity is controlled on the second wireless network,” and an aspect of that policy must be obtainable through agents executed by the processor which “obtain... a user input specifying” the aspect of the policy. For instance, if the activity is controlled in the *same way* between the first and second wireless networks, this limitation would not be satisfied.

VII. OPINIONS REGARDING CLAIMS 1, 26, AND 27

36. Claim 1 of the ’110 patent recites “[a] wireless device” comprising certain limitations. Limitation [1.5] of claim 1 of the ’110 patent requires memory configured to store “a first service policy associated with [a] first wireless network.” Limitation [1.7] further specifies that this “first service policy” must be

“for enabling control of [a] first service activity on the first wireless network that is different from how the first service activity is controlled on [a] second wireless network.” In other words, there must be a service policy specifically associated with the first wireless network which specifies that a first service activity is controlled *differently* between two different wireless networks.

37. Claim limitation [1.9] further requires that there be “processors for executing one or more agents, the one or more agents configured to: obtain, through [a] user interface, a user input specifying at least an aspect of the first service policy.”

38. In order to satisfy the “first service policy” that meets the requirements of limitation [1.7], the Dr. McDaniel points to three different alleged policies. As explained below, it is my opinion that none of those policies would have been obvious in view of Jobs, Jones, and Rao. But even if any of those policies would have been obvious, it is also my opinion that the user input requirements (i.e., providing an agent on the device to obtain a user input specifying an aspect of the policy) would have been obvious.

A. None of the Dr. McDaniel’s three alleged service policies would have been obvious.

39. In alleging a “first service policy” that satisfies the requirements of limitation [1.7] (which requires that the policy cause differential treatment of a first

activity between two different wireless networks), Dr. McDaniel identifies three separate theories. In my opinion, none of them would have been obvious as discussed below.

1. The Petition’s First Theory: Reducing Frequency of Jones’ Backups

40. Dr. McDaniel’s first theory is that it would be obvious to implement “a first service policy [which] enables a first control (reducing frequency) of a first service activity (e.g., backup) when JJRD is on a first wireless network (e.g., GSM cellular).” Ex. 1003, ¶228.

41. However, Dr. McDaniel’s proposal does *not* “enabl[e] control of the first service activity on the first wireless network that is different from how the first service activity is controlled on the second wireless network,” as the claim requires. Specifically, Dr. McDaniel alleges that the control would be different because the bandwidth of these two networks would differ. Ex. 1003 ¶231 (“since the bandwidth of CDMA and GSM networks differ, the frequency of backup will also differ”). In other words, Dr. McDaniel acknowledges that the alleged “first service activity” would be controlled in the *same* way across both networks: according to the available bandwidth. A POSITA would not understand this to satisfy the claim requirement of “control[ing]... the first service activity on the first wireless network” in a manner “that is different from how the first service

activity is controlled on the second wireless network,” because the algorithm for control (i.e., adjusting backup frequency according to available bandwidth) would be exactly the *same* between both wireless networks.

42. Indeed, Jones itself draws a distinction between adjusting policies according to “the *type* of the connection” as opposed to “the *bandwidth* of the connection.” Ex. 1006, 1:60-67 (discussing an “enterprise data protection strategy” which may adjust “frequency of data backups according to the identity of the user, *the type of connection, and/or the bandwidth of the connection*”). And Dr. McDaniel does not present a theory where backup frequency would be adjusted based on network *type* (as opposed to available bandwidth on the network). *See* Ex. 1003, ¶231 (alleging only that “the frequency of backup will... differ” “since the bandwidth of CDMA and GSM networks differ”).

43. Dr. McDaniel himself acknowledged that there is a significant difference between the *type* of wireless connection (e.g., GSM or CDMA) and the *bandwidth* of the connection. For instance, he testified that available bandwidth “really just depends on the environment, the underlying technology, [and] what the interference is,” such that even for “a device connecting to the same network, the bandwidth might vary depending on environmental factors.” Ex. 2003 at 13:2-15. Accordingly, while the “bandwidth of the GSM, CDMA, and wi-fi networks” “*can be*” different,” “[i]t’s difficult to characterize” whether one type of network “has

higher bandwidth” than the other, because it depends on a variety of different factors including environmental factors and interference that change over time. *See id.* at 12:24-13:11. I agree with his testimony in this regard, and this is knowledge that would have been readily understood by a POSITA.

44. Accordingly, a POSITA would understand that for a policy that had the goal of modifying frequency based on available bandwidth for wireless transmissions bandwidth would need to be measured in real time for networks such as GSM, CDMA, or WLAN, because bandwidth for wireless networks varies based on a variety of factors including wireless signal strength and other environmental factors. Given the bandwidth variations inherent to wireless networks, a POSITA would not have found it obvious to simply assume their bandwidth and control backup frequency on that basis, but would instead have wanted to actually measure bandwidth and control backup frequency according to measured bandwidth.

45. To the extent Dr. McDaniel contends that Jones teaches that certain connection types have set connection speeds (e.g., Ex. 1003 ¶229, asserting that “connection speed is a key characteristic of each network type”), a POSITA would not understand this to be true for wireless networks for the reasons addressed above. Instead, as discussed in more detail in the following sections, Jones teaches that *wired* connections such as (dial-up) modem connections may have a fixed

connection speed, and because the connection speed for those dial-up connections is relatively fixed, it may make sense to implement a blanket rule, for example, banning all data backup activity over modem connections. But Jones never teaches that any wireless connection would be generally disfavored in this regard (separate from the bandwidth of that connection), and given the significant variation in bandwidth across even the exact same connection type, a POSITA would not have found it obvious to look to connection *type* (instead of observed bandwidth available) in creating data control policies.

46. I note, for example, that the portions of Jones that Dr. McDaniel relies on (e.g., claim 7) recite that connection speed must be taken into account in applying the policy. And while network type may be taken into account, Jones does not disclose doing so other than to distinguish between modem vs non-modem connections (because of the relatively slow, and relatively stable, speed of modem connections). I disagree with his conclusion that “Jones... teaches that connection type is used at least to determine connection speed)” (Ex. 1003, ¶229), because Jones is explicit that connection speed and connection type are two independent variables that can *separately* influence policy behavior (as Jones teaches, e.g., with respect to non-wireless modem connections).

47. Accordingly, it is my opinion that it would not be obvious to implement a policy that controls frequency of data backups in a different manner

for one wireless network (GSM) as for another wireless network (CDMA) under Dr. McDaniel's theory as claim 1 requires, in view of Jones (the only reference Dr. McDaniel relies upon for this theory of limitation [1.7]). A more sensible implementation of the Jones system in Dr. McDaniel's combination would be to simply measure connection speed for a given period of time, and the slower the connection speed, the more time the system will allow between the last data backup. This solution would account for the important variable (connection speed) and adjust frequency of backup on that basis, and would not lead to suboptimal results (such as providing more frequent backups on a slower wireless connection, simply because the slower wireless connection is of a type that was incorrectly assumed to be faster than another wireless connection type).

2. Dr. McDaniel's Second Theory: Prohibiting Jones' Backups on GSM Networks While Allowing Backups on CDMA Networks

48. Dr. McDaniel additionally alleges that limitation [1.7] would be satisfied in an implementation where "a first policy (applicable to GSM networks) can specify that backup is not permitted, and a second policy (applicable to CDMA networks) can specify that backup is permitted." Ex. 1003, ¶237. Dr. McDaniel provides only a short paragraph of analysis in this regard. *See id.*

49. Dr. McDaniel does not provide any evidence that Jones (or any other reference) teaches prohibiting data backup transfers over one wireless network

while allowing them over another wireless network. Dr. McDaniel specifically cites to Jones 5:25-26 as evidence supporting its theory in this regard. But Jones does not teach disabling data backup over *any* wireless network. Instead, Jones teaches that a “rule may prohibit data transfers over a *modem* connection” while allowing data transfer over *any* “non-modem connection”:

For instance a first rule may prohibit data transfers over a modem connection. In the case of data backup, this rule may be further interpreted to prohibit copying files to a remote network share over a modem connection, while allowing local backup copying to continue. If the client connection changes to a non-modem connection, the modem policy rule prohibiting data transfers may no longer apply and remote copying may resume.

Ex. 1006, 5:25-32. Jones gives further examples of rules, each of which disfavor modem connections over non-modem connections (or are at best neutral toward modem connections). *See, e.g.*, Ex. 1006, 5:33-43 (disclosing two additional examples including (a) limiting the size of data transfer over a modem connection while allowing larger files to be transferred over non-modem connections, and (b) providing that “full data transfer capabilities” are equally applicable to modem and non-modem connections when data backup is “imperative”).

50. And in Jones, a POSITA would readily understand that a modem connection is a *wired* PSTN connection, because Jones directly contrasts them with

wireless connections.¹ Ex. 1006 (distinguishing modem connections from wireless connections, and noting that “modem connections are generally slower than wireless connections”). Specifically, Jones teaches that its system may be connected to a “public switched telephone network (PSTN) 160 via modem bank 150,” thus making clear to a POSITA that a modem connection is a wired connection via a public switched telephone network modem bank.

51. It is further my opinion that a POSITA would be confident that Jones’ discussion of modems was limited to consistently slow, public switched telephone network (i.e., dialup) modems because Jones consistently teaches that modem connections are generally slower than wireless connections. *See, e.g.*, 1:25-27 (“For example, modem connections are generally slower than wireless connections, which may be slower than directly cabled connections.”); *id.* at 1:54-58 (“However, if the connection type is slow, such as via a modem, a user who is attempting to access e-mail or browse the internet may be frustrated....”).

52. In other words, a POSITA would understand that Jones’ sole example of differential treatment of network types is by disfavoring a particular type of

¹ I note that “modem connection” may, in some contexts, be broad enough to refer to all connections that make use of a modem, which would include virtually all types of network connections. However, Jones makes clear that this is not what it means by a modem connection, because Jones explicitly differentiates a “modem connection” from a “wireless connection.”

wired connection, rather than drawing a distinction between any two *wireless* connections as the claims require. Jones thus does not disclose prohibiting data transfer over one wireless network while allowing it on another wireless network.

53. Nor does Dr. McDaniel provide any motivation or other obviousness rationale to implement Jones such that data backups would be prohibited over any particular wireless connection. His theory in this regard implicates only two different network types: GSM and CDMA. And nowhere in his analysis is there any rationale for prohibiting data backups on one of these networks, particularly in light of Jones' teaching that data transfers would be *allowed* on any non-modem connection (which would include all connections that are not via a PSTN/dial-up modem, including wireless connections). I also note that there is no evidence, for example, that there would be any other reason to prohibit data transfers on one of GSM and CDMA but not the other, and in my opinion a POSITA would not have been aware of any reason to distinguish between CDMA and GSM networks.

3. Dr. McDaniel's Third Theory: Assigning Packets to Different Queues Between GSM and CDMA Networks

54. Dr. McDaniel additionally alleges that limitation 1.7 would be satisfied by an implementation where "a first policy (applicable to GSM networks as determined by protocol, per Rao) can specify that packets are assigned to one queue, and a second policy (applicable to CDMA networks as determined by

protocol per Rao) can specify that packets are assigned to a different queue. Ex. 1003 ¶238.

55. Like with Dr. McDaniel's previous theory, this theory is contained only in a brief paragraph. And he also fails to show that the prior art discloses this configuration or renders it obvious. For example, despite basing his theory on Rao's disclosure, Dr. McDaniel provides no evidence that discloses assigning similar packets different priority depending on the network connection type, as Dr. McDaniel's theory would require. The only prior art cited in support of this theory is Rao at paragraphs [0182] and [0184]. *See* Ex. 1003, ¶238. I have reviewed both of those paragraphs, and conclude that neither of those paragraphs relate to prioritizing packets differently based on network type.

56. For instance, paragraph [0182] does specify that policies can be specified according to factors other than connection type: they can be specified, for example "by the name of the application," "type of application," "type of one or more protocols used by the applications," the "size of the payload of the network packet," "whether an application is running in the foreground or the background of the client," and/or "based on the destination network address." Ex. 1007, [0182]. However, there is no teaching or implication here (or in Rao more generally) that prioritization would vary across network types, such that a particular type of packet

would, for example, be assigned one type of priority on a GSM network, and another type of priority on a CDMA network as Dr. McDaniel's theory entails.

57. Likewise, paragraph [0184] of Rao says nothing about prioritization being handled differently across different types of *networks*. Rather, it talks about prioritizing various *types of data* to be passed over *any* network, such as “prioritiz[ing] the real-time data communications of application 338a ahead of other applications, such as non-real-time data communication applications.” Ex. 1007, [0184]. Nowhere in Rao is there any discussion of handling prioritization of packets differently depending on the type of network connection, and in my opinion a POSITA would not have viewed this as an obvious implementation.

58. I also note that a POSITA would understand the “one or more protocols used by the application” in Rao would not include, for example, GSM and CDMA network connection types. Dr. McDaniel does not allege as much, and a POSITA would understand that GSM and CDMA network types are used by the *device* to communicate data over the network layer of the TCP/IP protocol architecture model (“TCP/IP model”), and are not specific to any application. And GSM and CDMA are not relevant to the application's operation, in the sense that application operation can be (and usually is) entirely agnostic to which network protocol a device is connected to. For example, an application on a user's phone that wants to carry out an operation (such as downloading music) is typically

agnostic to the specific network type used, and the actual application implementation of that data transfer will not depend on the nuances of GSM network specifications as opposed to CDMA network specifications. Instead, the application is responsible for initiating the data requests through the types of protocols that *applications* typically interact with.

59. Rao itself makes this clear, when it discusses, for example, that “a type of protocol used by the application 338a-338n” includes “RTP or UDP,” or “a remote display protocol, such as ICA or RDP.” Ex. 1007, [0192]. RTP, UDP, ICA, and RDP are all protocols that are used by *applications* within the Internet protocol suite, because they are all “application” layer or “transport” layer protocols in the context of the TCP/IP protocol architecture model. *See* Ex. 2004 at 33 (introducing the “TCP/IP Protocol Architecture Model”); *id.* at 35-36 (making clear that transport-layer protocols such as UDP are used by applications: “applications that send small amounts of data use UDP”).

60. A POSITA would understand that the “application layer” is for “process-to-process” (e.g., application-to-application) communications across an Internet Protocol computer network (Ex. 2005, https://en.wikipedia.org/wiki/Application_layer). A POSITA would further understand that application layer protocols include RTP for delivering audio and video across networks and RDP for allowing a graphical interface to be utilized

across networks. Ex. 2006 (https://en.wikipedia.org/wiki/Real-time_Transport_Protocol) (“The design of RTP is based on the architectural principle known as application-layer framing where protocol functions are implemented in the application as opposed to the operating system's protocol stack.”); Ex. 2007 (<https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol>) (“RDP was developed to be entirely independent of its underlying transport stack, in this case TCP/IP,” thus making clear that RDP is above the transport stack (i.e., is application layer)). A POSITA would also understand that ICA is an application layer protocol, as it “is an alternative to Microsoft’s Remote Desktop Protocol (RDP)” which is itself an application layer protocol. *See* Ex. 2008 (https://en.wikipedia.org/wiki/Independent_Computing_Architecture).²

61. And while Rao discusses UDP, which a POSITA would understand to be part of the transport layer (Ex. 2004 at 35), a POSITA would understand that applications also make use of transport layer protocols. *See id.* at 36

² While these Wikipedia references and Microsoft documentation are not prior art, they reflect my pre-existing understanding of these protocols, and the information I rely upon them for would have been knowledge readily available to a POSITA as of the priority date of the ’110 patent. Wikipedia references like this are helpful for high-level understanding of the purposes and uses of these protocols, rather than precise implementation details.

(“[A]pplications that send small amounts of data use UDP.”); *id.* at 35–36 (explaining how applications use other transport layer protocols such as TCP and SCTP).

62. The application and transport layers of the TCP/IP protocol architecture model are the top-most two layers of that protocol. *See* Ex. 2003, 33. In contrast the data link and physical layers are the primary layers in which standards associated with network connections (such as Ethernet and WiFi) operate. *See* https://en.wikipedia.org/wiki/Data_link_layer (“Examples of data link protocols are Ethernet, the IEEE 802.11 WiFi protocols, ATM and Frame Relay.”). A POSITA would also understand that CDMA and GSM primarily operate at these lower layers, and would not be used directly used by applications in the context of Rao’s teachings.

63. Notably, all of the protocols used by applications discussed in Rao operate the same way, regardless of what sort of network connection is utilized. In contrast, GSM and CDMA standards are types of networks, and are not tied to any particular application. Thus, Rao does not disclose varying packet priorities according to network type, as Dr. McDaniel alleges.

64. Nor does Dr. McDaniel set forth any obviousness rationale for varying packet priority according to wireless network connection.

65. I also note that, although Dr. McDaniel has set forth no rationale for modifying the prior art to prioritize packets, it is my opinion that this would *not* have been motivated in view of the art he relies upon. For instance, if a packet is deemed as a high-priority packet (or conversely, is deemed as a low-priority packet), there is no obvious motivation to *change* that determined priority based on network type. By way of analogy, a high-priority vehicle (e.g., an ambulance) is given higher priority over other types of traffic, regardless of the what type of road (e.g., highway or residential) the ambulance is driving on. Likewise, there is no obvious reason to modify the priority that a high-priority packet (e.g., real-time traffic) is given based on the type of connection (e.g., GSM or CDMA) that the packet is transported using.

B. Dr. McDaniel also fails to establish obviousness of providing a user interface to modify the alleged policies satisfying limitation [1.7].

66. Limitations [1.8] and [1.9] require “one or more processors for executing... one or more agents configured to: obtain, through the user interface [of the wireless device comprising memory configured to store and apply the first service policy], a user input specifying at least an aspect of the first service policy.” As noted above in the preceding subsection, Dr. McDaniel sets forth three different theories regarding what the claimed “first service policy” might be. The first and second theories relate to Jones’ data backup policies.

67. At least for the data backup policies alleged by Dr. McDaniel, it is my opinion that a POSITA would not have found it obvious to provide agents on the wireless device that stores and applies the service policy configured to obtain a user input specifying an aspect of the service policy under Dr. McDaniel's theories, because these are not the types of policies suitable for end-user (as opposed to system administrator control).

68. According to Dr. McDaniel's theory, each individual user would be able to influence data backup policies by modifying those policies through a user input on the device. Dr. McDaniel confirmed as much during his deposition, when testified that his proposal would allow for "**any** user that would... want to be setting policy" to adjust the backup policies, such that "different users within the same network... to set their own desired backup policies." Ex. 2003, 14:4-25. That would presumably be the purpose of providing a user interface via agents on the device, as oppose to allowing modifications through a centralized mechanism such as a website or terminal interface.

69. However, a POSITA would understand that Jones does not disclose a user input on the wireless device itself for adjusting backup policies. The only teaching that Dr. McDaniel cites from Jones regarding a user interface is a generic statement that "a user ***such as a system administrator*** may configure policies for data transfers such as backups, updates, etc.," and that "a user may be presented

with a graphical user interface through which each policy may be selected and configured in successive operations.” Ex. 1003, ¶246 (quoting Ex. 1006, 5:15-29, 6:38-41). Jones never specifies *where* this user interface is located, but in the context of Jones (which is primary concerned with data backups operating in enterprise computing environments), a POSITA would have understood that the user interface would *not* be provided on each individual device. Instead, a POSITA would have understood that the user interface would be *separately* provided (e.g., via a web interface) and be restricted to a system administrator, such that the policy would *not* be modified through a UI provided by agents on the specific wireless devices in Jones’ network, but would instead only be accessed by an authorized user able to set policies broadly applicable to *each* of Jones’ client devices.

70. For example, Jones repeatedly teaches that the user modifying the policies can modify policies applicable to numerous clients, and never discloses modifying the policies on a per-client basis. *See, e.g.*, Ex. 1006, 5:40-43 (discussing “the case when a system administrator determines that it is imperative to backup data from *all clients* as soon as possible”); *id.* at 5:63-6:12 (discussing a policy set by a user such as a system administrator that applies to *multiple users* and *multiple clients*, because it “considers one or more attributes of the user with whom the client is associate[d] rather than the connection type,” such that “an important user” may have data backed up more often). Accordingly, it is my

opinion that Jones does not disclose (or imply) that the user interface for modifying Jones' backup policies would be on the device itself.

71. Dr. McDaniel also presents no motivation to place agents for modifying the policy onto each individual device. And in my opinion, such an approach would not have been obvious, because a POSITA would have understood that Jones' data backup operations are for the security of an enterprise computing environment, and allowing individual users to vary their data backup policies would lead to potential for security violations.

72. For example, a POSITA would recognize that users tend to choose user-friendly settings, such that they would reduce frequency of backups or disable them if given the opportunity, because Jones teaches that "users may be frustrated" if bandwidth is reduced due to backup operations. Ex. 1006, 1:54-57. This is precisely why Jones teaches concerned with developing a comprehensive "enterprise data protection strategy" that accounts for a variety of factors including bandwidth. Id. at 1:60-67. Nowhere does Jones imply that individual users should be able to adjust Jones' backup policies to their own individual preferences, and a POSITA would not have found such an implementation to be obvious because a POSITA would not have viewed individual-user-chosen policy implementations to be part of a "comprehensive enterprise data protection strategy" which is an important aspect of Jones' teachings.

73. Accordingly, it is my opinion that it would not have been obvious to modify the proposed JJRD device to allow user modifications to backup policies via a user interface provided by agents on the JJRD devices for the proposed “first service control policy” would have been obvious.

VIII. CLAIM 4

74. Claim depends from claim 1, and additionally requires, *inter alia* that “the memory is further configured to store a second service policy associated with the second wireless network,” and that “the one or more agents are further configured to” apply the second service policy.

75. The Dr. McDaniel identifies only policies applying to GSM and CDMA as constituting the first and second policies, and those policies fail for the same reason as discussed above with respect to claim 1. Ex. 1003, ¶¶270-271. While Dr. McDaniel further alleges that “[t]he second policy can be further specified based on user priority” (*id.* ¶272), he presents no reason why the second policy (where whether backup is prohibited is dependent on user priority) would be applicable to CDMA but not GSM, for example. As discussed above, Jones only discloses prohibiting data backup on *modem* connections, which are distinct from wireless connections, and Dr. McDaniel identifies no motivation to deviate from Jones’ teaching in this regard.

IX. CLAIMS 5 AND 28

76. Claims 5 recites:

5. The wireless device recited in claim 1, wherein reducing data usage comprises blocking the first service activity.

Ex. 1001, Claim 5. Dr. McDaniel's theory with respect to claim 5 is the same as the Dr. McDaniel's theory with respect to claim 1, except it is limited to "a first rule" that "prohibit[s] data transfers" on a particular network type. As explained above in my analysis for limitation [1.7] above, the Dr. McDaniel fails to establish the obviousness of prohibiting data transfers on one wireless network connection type while allowing data transfers on another wireless network connection type. Nor does the Dr. McDaniel establish the obviousness of providing agents on the device with a user interface to obtain an aspect of such a policy, as claim 1 requires.

X. CLAIM 6

77. Claim 6 recites:

6. The wireless device recited in claim 1, wherein reducing data usage comprises blocking the first service activity when the wireless device is connected to the first wireless network and allowing the first service activity when the wireless device is connected to the second wireless network.

Ex. 1001, Claim 6.

78. Dr. McDaniel's theory for claim 6 is largely the same as its theory for claim 5, and fails for the same reasons. *See* Ex. 1003 ¶283 (relying a rule prohibiting backup transfers on a particular network type).

79. However, Dr. McDaniel also discusses a rule where “data backup frequency can be adjusted based on network type.” *Id.* As discussed above for limitation [1.7], this type of policy distinguishing between two different wireless network types would not have been obvious in the context of Jones.

80. But even assuming adjusting frequency of backup would have been obvious, I disagree that adjusting the frequency of data backup activities constitutes “blocking” a backup activity. Scheduling an activity for a specific time (which adjusting frequency of backup would entail) does not constitute “blocking” that activity in the context of Jones’ disclosure, because the activity is simply scheduled in a certain way—adjusting a schedule is not “blocking.” Nor does Dr. McDaniel establish the obviousness of providing agents on the device with a user interface to obtain an aspect of such a frequency-adjusting policy, as I have previously explained.

XI. CLAIM 25

A. Overview of Dr. McDaniel’s Motivation to Combine

81. Ibrahim, unlike any of Jobs, Jones, and Rao, is focused on having a mobile handset 406 “serv[e] as a base station relaying traffic between other wireless devices and a cellular network or WLAN.” *See* Ex. 1003, ¶199. This functionality is shown, for example, in FIG. 4A of Ibrahim, reproduced below:

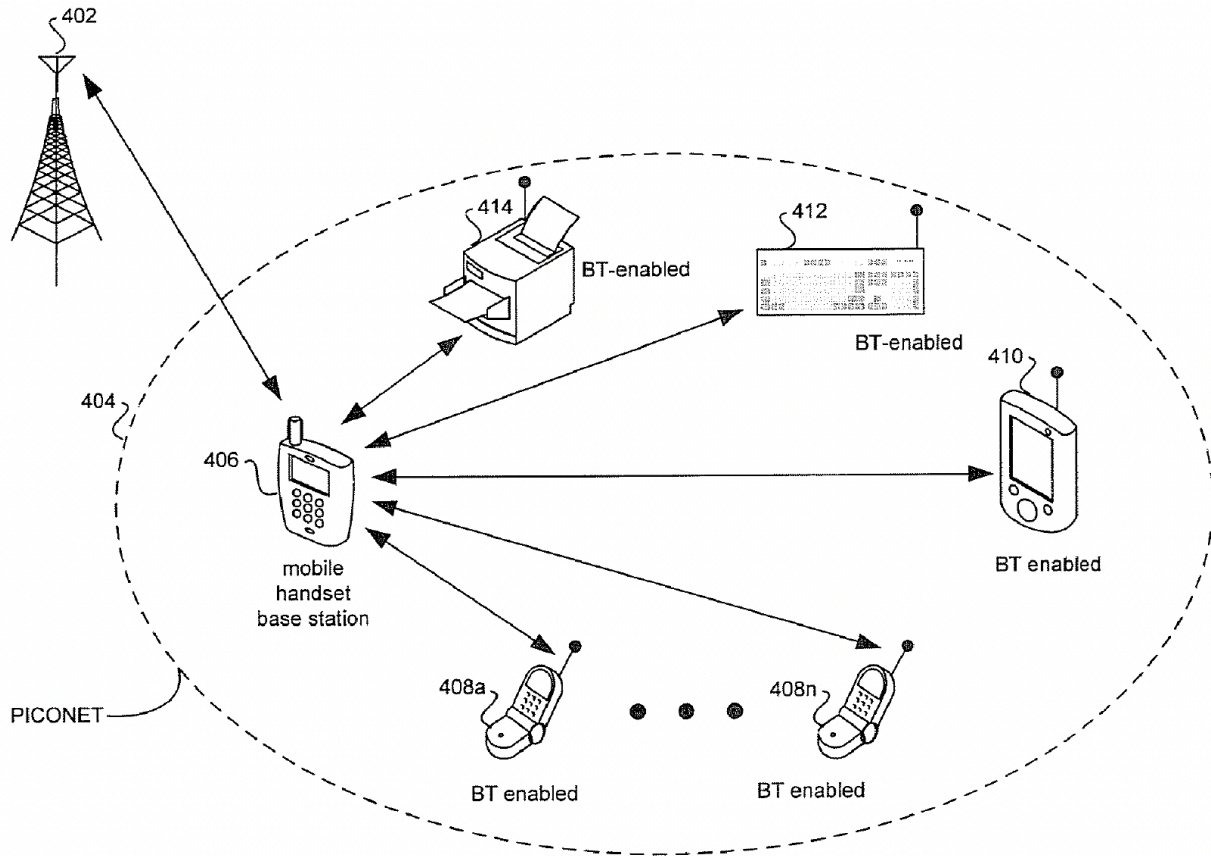


FIG. 4A

Ex. 1012, FIG. 4A. As shown above, Ibrahim depicts Bluetooth (“BT”) enabled devices (408, 410, 42, and 414) using the “mobile handset” as a piconet “base station” so that they can communicate with the cellular network 402 and each other. *See* Ex. 1012, [0050] (“In this regard, the closely located wireless devices [408, 410, 412, and 414]] may also communicate with the cellular network via the mobile handset base station 406.”); *id.* at [0050] (“The mobile handsets 408[] may communicate with other closely located wireless devices via the mobile handset base

station 406.”); *id.* at [0049] (listing the “closely locates wireless devices” as including 408, 410, 412, and 414, and distinguishing them from “mobile handset base station 406”).

82. This feature of Ibrahim underlies Dr. McDaniel’s motivation to combine Ibrahim with Jobs, Jones, and Rao (the “JJRD” references) to arrive at the Jobs-Jones-Rao-Ibrahim combination (“JJRID”). For instance, Dr. McDaniel asserts that “JJRID” benefits from the disclosed “base station functionality” of Ibrahim” “when other devices, including devices owned by the same enterprise, are able to connect to the network through JJRID.” Ex. 1003 ¶199. Dr. McDaniel’s only disclosed motivation to pursue this combination is that “a POSITA would have understood that including the base station functionality (per Ibrahim) benefits the enterprise computing environment by enabling devices lacking cellular capability to connect to a wireless network.” *Id.*

B. Dr. McDaniel provides no motivation to modify Ibrahim/Jones as he alleges.

83. Although Dr. McDaniel contends that “the components of JJRID each operate as they would in isolation” (Ex. 1003 ¶201), that is inconsistent with his actual theory which modifies Jones’ backup functionality significantly.

84. Specifically, Dr. McDaniel proposes that “JJRID backs up personal data (contacts, favorites, etc.) to the ‘other wireless device,’ such as a laptop

assigned to the same employee.” Ex. 1003, ¶407. But he doesn’t allege that Jones or Ibrahim discloses the functionality of either (1) backing up *any* data to another wireless device that is not Jones’ backup server, or (2) having particular backup rules applicable to “personal data (contacts, favorites, etc.).”

85. Dr. McDaniel also cites to no evidence in the prior art that teaches (or suggests) backing up data to a non-local device such as a laptop. Instead, Dr. McDaniel acknowledges that backing up data to a laptop would be generally sub-optimal, but asserts with no supporting evidence that laptops “are well-suited for backing up things like personal files where they are easily accessible if it is necessary to restore the files from the laptop to the mobile device.” Ex. 1003, ¶407 (acknowledging that “backing up to a laptop might not be optimally suited for all types of data).

86. In my opinion, Dr. McDaniel’s allegations provide no reason why a POSITA would have been motivated to *modify* Jones’ teachings of backing up data either locally (i.e., to the Jones device itself) or to a backup server (i.e., a server on Jones’ enterprise network).

87. And Dr. McDaniel also does not explain why a POSITA would have even thought of the idea of having a separate backup location for “personal files” as opposed to other “types of data (e.g., for data subject to regulatory control such as HIPAA, or enormous files, such as large software projects).” Ex. 1003, ¶407.

For example, Dr. McDaniel does not provide any evidence that a POSITA implementing Jones would have sought to have different rules applicable to “personal files” as opposed to other types of data that would be ill-suited for laptop backup, or explain how a POSITA would implement such rules in a way that would mitigate the security risk that security-sensitive data would be inadvertently included in what are nominally “personal files.” Nor is there any need to have different backup rules applicable to these types of data, because under Jones’ teachings, all data can be backed up either locally or to a backup server.

88. Ibrahim does not help fill this gap in Jones’ teachings, as Ibrahim does not disclose any backup operations initiated by the mobile handset base station. Nor does Ibrahim disclose any data transfer between mobile handset base station and the “other wireless device” such as a laptop at all, other than to act as a base station that allows the “other wireless device” to interact with various networks and various other wireless devices (other than mobile handset base station).

89. In short, Dr. McDaniel’s theory relies on a particular feature—backing up data from a mobile handset to a laptop—for which he provides no evidence that a POSITA would have actually been motivated to implement.

90. I also note that Dr. McDaniel states that “things like personal files” might not present significant security risks. Ex. 1003, ¶407. But even *if* there were a way to accomplish his proposed modification in a way that did not flagrantly

violate security requirements, that is not itself a *motivation* to implement the modification. Furthermore, a POSITA would recognize that even personal files can inadvertently contain security-sensitive data, and even the possibility of such a result would have been avoided in the context of JJRD. And Dr. McDaniel does not explain how the proposed JJRID combination would have reasonably been expected to succeed in complying with security protocols in the context of an enterprise network. It is also not clear why, if a network connection is available to the JJRD device, it would not just back up data as taught by Jones itself—i.e., it would back up data directly to the enterprise network, which a POSITA would recognize would not pose security concerns (since Jones’ enterprise network is presumably fully security compliant, as required by the enterprise).

91. A POSITA would also understand that in Ibrahim, there is no disclosure of the mobile handset acting as a base station storing data on the “other wireless device[s],” or otherwise relying on those devices to accomplish its own functionality. Instead, in Ibrahim, the other wireless devices make use of the mobile handset to gain enhanced functionality, not the other way around.

I declare under penalty of perjury 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.

June 20, 2025



Michael C. Brogioli, Ph.D.