

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.
and MOTOROLA MOBILITY LLC,
Petitioners,

v.

HEADWATER RESEARCH LLC,
Patent Owner.

IPR2024-01337
Patent 8,588,110 B2

PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	Introduction	1
II.	Overview of the '110 Patent.....	2
III.	Claim Construction.....	3
IV.	The Petition fails to show unpatentability of claim 1, claim 26, or claim 27.	4
	A. None of the Petition's three alleged service policies would have been obvious.....	5
	1. The Petition's First Theory: Reducing Frequency of Jones' Backups	5
	2. The Petition's Second Theory: Prohibiting Jones' Backups on GSM Networks While Allowing Backups on CDMA Networks	8
	3. The Petition's Third Theory: Assigning Packets to Different Queues Between GSM and CDMA Networks	12
	B. The Petition also fails to establish obviousness of providing a user interface to modify the alleged policies satisfying limitation [1.7]. ..	14
	C. The Petition's failures with respect to claim 1 apply equally to claims 26 and 27.....	17
V.	The Petition fails to show obviousness of claim 4.	18
VI.	The petition fails to show obviousness of claims 5 and 28.	19
VII.	The petition fails to show obviousness of claim 6.	20
VIII.	The Petition fails to show obviousness of claim 25.	21
	A. Overview of the Petition's Motivation to Combine	21
	B. The Petition's actual combination is not motivated.....	24
IX.	Conclusion.....	26

PATENT OWNER'S EXHIBIT LIST

No.	Description
Ex. 2001	Declaration of Dr. Michael C. Brogioli in Support of Patent Owner's Response
Ex. 2002	<i>Curriculum Vitae</i> of Dr. Brogioli
Ex. 2003	June 6, 2025 Deposition Transcript of Dr. Patrick McDaniel
Ex. 2004	Sun Microsystems, System Administration Guide: IP Services (2009), available at https://docs.oracle.com/cd/E19120-01/open.solaris/819-3000/819-3000.pdf
Ex. 2005	Application Layer, https://en.wikipedia.org/wiki/Application_layer (last visited June 20, 2025)
Ex. 2006	Real-time Transport Protocol, https://en.wikipedia.org/wiki/Real-time_Transport_Protocol (last visited June 20, 2025)
Ex. 2007	Windows Server, <i>Understanding the Remote Desktop Protocol (RDP)</i> (Jan. 1, 2025) available at https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol
Ex. 2008	Independent Computing Architecture, https://en.wikipedia.org/wiki/Independent_Computing_Architecture (last visited June 20, 2025)
Ex. 2009	Data Link Layer, https://en.wikipedia.org/wiki/Data_link_layer (last visited June 20, 2025)

I. Introduction

All challenged claims require a policy that enables control service activities over a wireless network traffic vary between two different wireless networks. For this theory, the Petition primarily relies on data backups disclosed in the Jones reference, and alleges that there would be two different backup policies applicable to two different wireless networks. But Jones does not teach that the types of policies the Petition relies on would vary based on wireless network type, and the Petition provides no motivation to modify Jones such that those policies would vary based on wireless network type.

The Petition also fails to explain the motivation to provide a user interface on the wireless device to obtain an input modifying the alleged policies, as required by all challenged claims. In Jones, the only user disclosed as modifying Jones' backup policies is a system administrator, and Jones does not disclose that individual users of the devices would be allowed to modify their backup policies (which are for security of data on an enterprise network). A POSITA would not have been motivated to allow individual, non-administrator users to modify policies in the manner the Petition alleges, because that would create significant security concerns in the context of Jones.

As explained in further detail below, the Petition also fails to establish the obviousness of numerous dependent claims (including claims 4-6 and 25).

II. Overview of the '110 Patent

The challenged claims of the '110 Patent (claims 1–30) are directed at a high level 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. Ex. 2001, ¶¶33–35.

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.

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. Ex. 2001, ¶38.

III. Claim Construction

The Petition identifies several terms for construction, but none of these constructions need to be addressed to evaluate the issues presented in this Response.

IV. The Petition fails to show unpatentability of claim 1, claim 26, or claim 27.

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. Ex. 2001,

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.”

In order to satisfy the “first service policy” that meets the requirements of limitation [1.7], the Petition points to three different alleged policies. As explained below, none of those policies would have been obvious in view of Jobs, Jones, and Rao. However, even if those policies *would have been* obvious, it would not have been obvious to allow a user of the device to have “input specifying at least an aspect of the first service policy,” because there is no motivation to provide a *user of the*

device (as opposed to a system administrator that oversees network policies more generally) a user interface on the device to modify the policies the Petition relies upon. Ex. 2001, ¶¶36-38.

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

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), the Petition identifies three separate theories, each of which fails.

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

First, the Petition alleges that it would have been 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).” Pet. 34. Under this theory, the policy would “specify that, when JJRD is on a GSM network, backup frequency is adjusted according to the connection bandwidth, per Jones,” and when “JJRD is on a second network (e.g., CDMA cellular),⁵ the backup frequency is also adjusted [according to the connection

bandwidth], but since the bandwidth of CDMA and GSM networks differ, the frequency of backup will also differ.” Pet. 34.¹

However, the Petition’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, the Petition alleges that the control would be different because the bandwidth of these two networks would differ. Pet. 34 (“since the bandwidth of CDMA and GSM networks differ, the frequency of backup will also differ”). In other words, the Petition alleges that the “first service activity” would be controlled ***in exactly the same way*** across both networks: according to the available bandwidth. A POSITA would not understand this to meet 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*. Ex. 2001, ¶¶39-41.

¹ Footnote 5 of the Petition specifies that for this theory: “The second network can be other [wireless] network types (e.g., WLAN); in such cases, JJRD differentiates cellular and WLAN.”

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. 2001, ¶42; 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 the Petition does not present a theory where backup frequency would be adjusted based on network *type* (as opposed to available bandwidth on the network). *See* Pet. 34 (alleging only that “the frequency of backup will... differ” “since the bandwidth of CDMA and GSM networks differ”).

And Dr. McDaniel confirmed at his deposition that the *type* of connection (e.g., GSM or CDMA) is different from (and not itself determinative of) 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.

Accordingly, a POSITA would understand that for a design goal of adjusting bandwidth according to frequency (as the Petition's theory entails), the frequency would be adjusted not based on wireless network *type* (such as GSM, CDMA, or WLAN), but rather based on the *observed* or *measured* bandwidth available over any particular connection, because bandwidth for wireless networks varies based on a variety of factors including wireless signal strength and other environmental factors. Ex. 2001, ¶¶40-43.

Accordingly, 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 the Petition's theory as claim 1 requires, in view of Jones (the only reference the Petition relies upon for this theory of limitation [1.7]). Instead, the Petition has at most shown the obviousness of controlling backup frequency across *all* wireless networks according to the available bandwidth at any given point in time, rather than according to the actual network type. Ex. 2001, ¶44.

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

Second, the Petition alleges a different theory for limitation [1.7]: *prohibiting* data backups on one wireless network, while allowing data backups on another wireless network. *See* Pet. 34-35 ("In another example, a first policy (applicable to

GSM networks) can specify that data backup is not permitted, and a second policy (applicable to CDMA networks) can specify that backup is permitted.”). However, as explained below, the Petition fails to show that the prior art discloses or renders obvious such an implementation. Ex. 2001, ¶¶48-53

However, the Petition does not show that Jones (or any other reference) teaches prohibiting data backup transfers over one wireless network while allowing them over another wireless network. The Petition specifically cites *only* 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”); Ex. 2001, ¶¶48-49.

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. Ex. 2001, ¶50; 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. Ex. 2001, ¶50 & n.1. A POSITA would be confident that Jones’ discussion of modems was limited to 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....”); Ex. 2001, ¶51.

In other words, Jones’ sole example of differential treatment of network types is by disfavoring a particular type of *wired* connection, rather than drawing a distinction between any two *wireless* connections as the claims require. Ex. 2001, ¶52. Jones thus does not disclose this limitation, either explicitly or inherently.²

² In offering his opinions on Jones, Dr. McDaniel incorrectly interpreted what Jones meant by a “modem connection” as opposed to a “non-modem connection.” Specifically, Dr. McDaniel interpreted Jones as including *any* connection that uses *any* modem (Ex. 2003, 16:9-19:8), as opposed to Jones’ disclosure of a “modem connection” as being public switched telephone network modem (e.g., dial-up modem), as opposed to “non-modem connections” which include “wireless local area network,” “direct wired LAN, wireless connection through a wide area network... or direct through a WAN.” Ex. 1006 at 1:17-22 (describing a modem connection as an *alternative* to the other forms of connection); *see also, e.g., id.* at 3:14-25 & FIG. 1 (describing a “modem bank 150” for a “public switched telephone network” connection); *id.* at 3:26-32 (again distinguishing “modem banks” from “direct LAN connections, wireless connections, WAN links, etc.”). Accordingly, Dr. McDaniel’s opinions supporting the Petition on this point are inconsistent with Jones’ teachings, and they should be given little if any weight.

Nor does the Petition or Dr. McDaniel provide any *motivation* (or other obviousness rationale) to implement Jones such that data backups would be prohibited over any particular wireless connection. The Petition's second theory implicates only two different network types: GSM and CDMA. And nowhere in the Petition or Dr. McDaniel's expert declaration 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). *See generally* Pet.; Ex. 2001 ¶53.

In sum, because the Petition shows neither how the prior art discloses nor renders obvious prohibiting data backups over GSM networks while simultaneously permitting data backups over CDMA networks (Pet. 34-35), the Petition's second theory as to limitation 1.7 also fails.

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

Third, the Petition's final theory for limitation 1.7 is that "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. *See* Pet. 35.

However, again, the Petition fails to show that the prior art discloses this configuration or renders it obvious. For instance, the Petition cites to no teaching in Rao that discloses assigning similar packets different priority *depending on the network connection type*, as the Petition’s theory would require. The only prior art cited in support of this theory is Rao at paragraphs [0182] and [0184]. *See* Pet. 35 (citing Ex. 1007 at [0182], [0184]). But neither of these paragraphs has *anything* to do with prioritizing packets differently based on network type. Ex. 2001, ¶¶54-55

For instance, paragraph [0182] does specify that policies can be specified according to factors *other than* network connection type: “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]. This paragraph *never* teaches or implies, however, 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 the Petition’s theory entails. Ex. 2001, ¶56.

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]. And nowhere else in Rao is there any discussion of handling prioritization of packets differently depending on the type of network connection. Ex. 2001, ¶57.

Nor does the Petition set forth any obviousness rationale for varying packet priority according to wireless network connection. Accordingly, the Petition fails to set forth the obviousness of such an implementation.

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

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 Section IV.A, the Petition 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. At least for these data backup policies, 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 the Petition’s theories, because these are not

the types of policies suitable for end-user (as opposed to system administrator control). Ex. 2001, ¶¶66-73.

According to the Petition's theory, each individual user would be able to influence data backup policies by modifying those policies through a user input on the device. Petitioner's expert 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.

In particular, Jones does not disclose a user input *on the wireless device itself* for adjusting backup policies. The only teaching that the Petition 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." Pet. at 23 & 38 (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 primarily 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, but rather 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. Ex. 2001, ¶¶67-69.

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, 5:49-43 (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); Ex. 2001 ¶70.

Because Jones is non-specific about *where* the user interface is located, Jones does not disclose (either expressly or inherently) that the user interface for modifying Jones' backup policy would be located on the device itself such that each individual user could modify the policy.

And the Petition presents no motivation to place agents for modifying the policy onto each individual device. Nor would such an approach 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. Ex. 2001, ¶¶71-73.

For example, individual users given control over backup policies would likely choose for less frequent backups, as Jones teaches that “users may be frustrated” if bandwidth is reduced due to backup operations. Ex. 1006, 1:54-57. Accordingly, Jones is 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. Ex. 2001, ¶72.

Accordingly, the fails to show that user modifications via a user interface provided by agents on the JJRD devices for the proposed “first service control policy” would have been obvious, at least for the Petition’s theories in which the first service control policy is a policy that controls data backup operations.

C. The Petition’s failures with respect to claim 1 apply equally to claims 26 and 27.

Claim 26 includes similar requirements to claim 1, except expressed as “means for” accomplishing the recited functionality. The Petition, throughout its claim 26 analysis, relies entirely on its claim 1 analysis except to show the alleged structure applying to the recited means. *See generally* Pet. 85-94. Accordingly, the Petition’s claim 26 theory fails for at least the same reasons as the Petition’s claim 1 theory.

The Petition likewise relies on its analysis of limitations [1.5]-[1.7], and [1.9]-[1.12] for its claim 27 theory. *See* Pet. 60. The Petition’s theory with respect to claim 27 is thus deficient for the same reasons as discussed above for claim 1.

V. The Petition fails to show obviousness of claim 4.

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.

The Petition 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. While the Petition further alleges that “[t]he second policy can be further specified based on user priority” (Pet. 44), the Petition 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 the Petition identifies no motivation to deviate from Jones' teaching in this regard. Ex. 2001, ¶¶74-75.

VI. The petition fails to show obviousness of claims 5 and 28.

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. The Petition's theory with respect to claim 5 is the same as the Petition'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 Section IV.A.2, the Petition fails to establish the obviousness of prohibiting data transfers on one wireless network connection type, and allowing data transfers on another wireless network connection type. Nor does the Petition 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. Ex. 2001, ¶76.

Furthermore, claim 28 includes a substantially similar requirement to claim 6, and the Petition relies solely on its analysis of limitations [1.4] and [5] for its claim 28 analysis, and the Petition's claim 28 theory fails for the same reasons as its theories for claim 1 and 5.

VII. The petition fails to show obviousness of claim 6.

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.

The Petition’s theory for claim 6 is largely the same as its theory for claim 5, and fails for the same reasons. *See* Pet. 47 (relying a rule prohibiting backup transfers on a particular network type).

However, the Petition also discusses a rule where “data backup frequency can be adjusted based on network type.” Pet. 47. As discussed above in Section IV.A.1, the Petition fails to show the obviousness of adjusting frequency differently between two wireless network types. But in any event, the Petition fails to explain how 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. Ex. 2001, ¶¶77-80; Nor does the Petition establish the obviousness of providing agents on the device with a user interface to obtain an aspect of such a frequency-adjusting policy, as claim 1 requires. *Id.* ¶80.

VIII. The Petition fails to show obviousness of claim 25.

The Petition's combination for claim 25 adds a new reference (Ibrahim, Ex. 1012) to the Jobs-Jones-Rao combination relied upon for claims 1, 4, 5, and 6. The Petition calls the resulting combination JJRID, for "Jobs-Jones-Rao-Ibrahim Device." *See* Pet. 79.

The Petition's theory for claim 25 fails because it entails a modification to the prior art that is not taught by (or obvious in view of) any of the four references the Petition relies upon. Specifically, the Petition proposes that Jones' mobile device would be modified so that it would *not* backup data either "locally and/or on a backup server over network 100" as Jones teaches (Ex. 1006, 3:42-55), but would *instead* be backed up to a wireless device that is neither *local* nor a backup server. Specifically, the Petition contends that in the proposed combination, the system would "back[] up personal data (contacts, favorites, etc.) to *another* 'wireless device,' such as a laptop assigned to the same employee." Pet. 83. As explained below, neither Jones nor Ibrahim (nor any other of the Petition's combination references) actually disclose such an implementation, and the Petition makes no plausible showing that a POSITA would have found it obvious to do so. Ex. 2001, ¶¶81-86.

A. Overview of the Petition's Motivation to Combine

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* Pet. 79. This functionality is shown, for example, in FIG. 4A of Ibrahim, reproduced below:

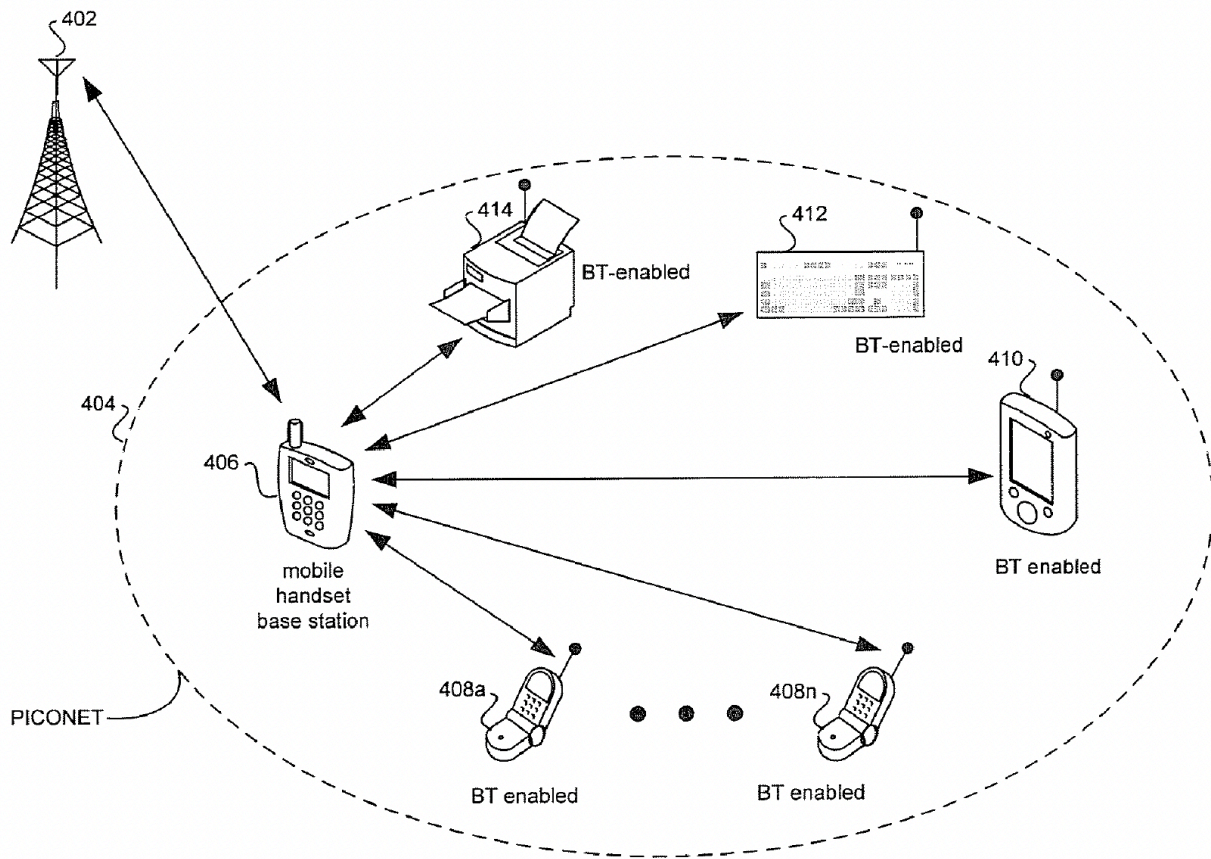


FIG. 4A

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”); Ex. 2001, ¶81.

This feature of Ibrahim is the core of the Petition’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, the Petition makes clear 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.” Pet. 80. The Petition’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.*

In other words, the motivation to combine JJRD with Ibrahim to arrive at JJRID is to allow more devices to connect to a cellular network. *See generally* Pet. 79-81.

B. The Petition’s actual combination is not motivated.

In attempting to defend the obviousness of its combination, the Petition asserts that “the components of JJRID each operate as they would in isolation.” Pet. 81. That assertion is incorrect; the Petition significantly modifies the operation of Jones’ backup software, with no even alleged motivation to deviate from Jones’ teachings in relevant respect. Ex. 2001, ¶¶83-89.

Specifically, the Petition proposes that “JJRID backs up personal data (contacts, favorites, etc.) to the ‘other wireless device,’ such as a laptop assigned to the same employee.” Pet. 83 (quoting Ex. 1003, ¶407). But the Petition does not 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.).”

The Petition’s *only* cited evidence for its assertion that JJRID is a citation to paragraph 407 of Dr. McDaniel’s expert declaration. *See* Pet. 83. But 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).

Dr. McDaniel’s allegations, however, 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). Ex. 2001, ¶¶83-86.

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, neither the Petition nor Dr. McDaniel provides *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. Ex. 2001, ¶¶87.

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). Ex. 2001 ¶¶88, 91.

In short, the Petition alleges a particular feature—backing up data from a mobile handset to a laptop—for which the Petition cites *no* documentary evidence regarding obviousness. The only apparent rationale to propose this implementation appears to be based on hindsight, as the documentary evidence available to a POSITA does not justify the Petition’s proposed deviation to Jones’ teachings regarding how data is backed up. Ex. 2001 ¶¶83-89. And because this particular feature of the Petition’s JJRID combination is necessary to the Petition’s claim 25 theory, the Petition’s obviousness theory with regard to claim 25 cannot succeed.

IX. Conclusion

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

Date: June 20, 2025

Respectfully submitted,

/James A. Milkey/

Reza Mirzaie, Reg. No. 69,138

Marc A. Fenster, *pro hac vice* forthcoming

Dale Chang, Reg. No. 61,476

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

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

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

RUSS, AUGUST & KABAT
12424 Wilshire Blvd., 12th Floor
Los Angeles, CA 90025

Counsel for Patent Owner

CERTIFICATION REGARDING WORD COUNT

Pursuant to 37 C.F.R. §42.24(d), Patent Owner certifies that there are 6,865 words in the paper excluding the portions exempted under 37 C.F.R. §42.24(a)(1).

Date: June 20, 2025

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

Counsel for Patent Owner

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

The undersigned hereby certifies that the above document was served on June 20, 2025, by filing this document through the Patent Trial and Appeal Case Tracking System as well as delivering a copy via electronic mail upon the following attorneys of record for the Petitioner:

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Jennifer J. Huang, Reg. No. 64,297
IPR39843-0179IP1@fr.com
PTABInbound@fr.com
axf-ptab@fr.com,
jjm@fr.com
jjh@fr.com

Date: June 20, 2025

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

Counsel for Patent Owner