

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

HEADWATER PARTNERS I LLC,
Patent Owner.

Case IPR2024-01051
Patent 8,639,811

PETITIONER'S REPLY TO
PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	PATENT OWNER’S TREATMENT OF “WHEN THE FIRST APPLICATION RUNS AS A BACKGROUND PROCESS” IS WRONG	1
III.	PATENT OWNER’S INTERPRETATION OF “PREVENTING COMMUNICATION” IS OVERLY NARROW	3

I. INTRODUCTION

The Petition’s arguments regarding claim 4 are straightforward: the Rao-Jones Device (“RJD”) “evaluates policies relating to factors including ‘whether an application is running in the foreground or the background.’” Pet., 38 (citing SAMSUNG-1005, [0182]; §III.A.1.a; SAMSUNG-1003, ¶[315]). The Petition explains that the application can be a backup application¹ and “RJD prevents network access when the application runs as a background process.” *Id.*, 38 (citing SAMSUNG-1006, 5:13-32), 39 (internal citations omitted). Faced with the Rao-Jones combination, Patent Owner’s (“PO”) only recourse is to mischaracterize the technical operation of backup applications and offer overly-narrow interpretations of an application “run[ning]” as a background process. PO further offers an overly-narrow interpretation of “preventing communication” unsupported by the evidence.

II. PATENT OWNER’S TREATMENT OF “WHEN THE FIRST APPLICATION RUNS AS A BACKGROUND PROCESS” IS WRONG

PO’s argument that the Petitioner does not “provide[] any evidence or reasoning that the backup application would be running or executing when it is not supposed to be communicating over the network” (POPR, 10) is based on a mischaracterization of the nature of backup processes and an overly narrow

¹ Petitioner also argues the “first application” can be a video streaming application. Pet. 38-39; SAMSUNG-1003, ¶¶315-317; SAMSUNG-1005, [0088], [0179].

interpretation of “run[ning] as a background process.”

First, PO mischaracterizes how background processes execute on conventional computing systems. Namely, PO alleges that a POSITA “would not have understood that the data protection software would be *constantly* running in the background (i.e., even when no data backups or other network communication was desired),” and its expert alleges that “a niche application such as a data backup process would only need to run when it is actually performing network communications.” POPR, 10; Ex. 2001, ¶41. Jones itself, however, contradicts this argument, stating that “a first rule may prohibit data transfers over a modem connection,” and, “[i]n 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*.” SAMSUNG-1006, 5:25-29 (emphasis added); *see* Pet., 38 (citing SAMSUNG-1006, 5:13-32). That is, Jones teaches that, even if a rule prevents data backup over a modem connection, the application nonetheless continues to run in the background as it “allow[s] local backup copying to continue.” *Id.* Moreover, minimally, a background backup process periodically executes to determine whether a backup is actually needed (e.g., files have changed). Given Jones’s clarity that “data protection software ... may execute in the background to perform data backups,” (Pet., 39 (citing SAMSUNG-1006, 3:45-51)), no further explanation is needed to inform a POSITA.

Second, PO's arguments rely on an overly narrow interpretation of what it means for an application to be "run[ning] as a background process." PO implies that a data backup application does not run "when no data backups or other network communication was desired." POPR, 10. Its expert further implies that "a niche application such as a data backup process" is only running if "it is actually performing network communications." Ex. 2001, ¶41. Not only are these statements technically wrong, as discussed above, they also require an interpretation of "run[ning]" that necessitates that a data backup application is only running if it is actively performing a data backup over a network. PO offers no support from the '811 patent for such an interpretation, nor does such support exist. *See* POPR, 8-11.

III. PATENT OWNER'S INTERPRETATION OF "PREVENTING COMMUNICATION" IS OVERLY NARROW

Next, PO asserts "there is no indication that there *would* be any communication (such as, e.g., a data packet) [in the RJD] to even arguably prevent other than when the backup process is configured to execute." POPR at 8-9. But, this assertion relies on an overly narrow interpretation of "preventing communication."

Illustrating its narrow interpretation of "preventing communication," PO alleges that "'communication[s] associated with' a backup application would *only* exist when the backup application is attempting to perform communications for data backup, so scheduling the backup process to only at certain times or under certain conditions as the Petition suggests (e.g., according to 'enterprise policies') would

cause the application to not generate any communications that *could be* prevented at other times.” *Id.*, 9 (citing Ex. 2001, ¶39). That is, PO implies that “preventing communication” requires that data packets must first be generated and then blocked. *Id.*, 8-9. PO cites to its expert as explaining that the ’811 patent “discusses blocking *packets* that were previously generated by an application.” *Id.*, 9 (citing ¶¶39-40).

However, the ’811 patent is not limited to PO’s narrow interpretation of “preventing communication” as “blocking packets that were previously generated by an application.” While PO’s expert characterizes the ’811 patent as “mak[ing] clear that the system is operable to prevent communications issued by applications” (*see* Pet., 9 (citing Ex. 2001, ¶40)), the ’811 patent itself is not so limited. For instance, PO alleges the ’811 patent “makes clear that [its] system is operable to prevent communications issued by applications” (POPR, 9 (citing Ex. 2001, ¶40)), but this is just one example of preventing communications in the ’811 patent. Notably, PO’s expert acknowledged “that communication prevention capabilities can be implemented, *for example*,” via a number of different ways. Ex. 2001, ¶40 (emphasis added). Indeed, each cited example from the ’811 patent relates to a non-limiting *example* of preventing communication rather than a strict requirement that preventing communication necessitates blocking data packets generated by an application. POPR, 9; Ex. 2001, ¶40 (citing SAMSUNG-1001, 51:40-43, 56:11-34, 103:54-58). However, the ’811 patent also describes alternatives where, like Jones,

the service is blocked from accessing the network. For example, the '811 patent explains that "FIGS. 42A through 42J provide tables summarizing various service policy control commands in accordance with some embodiments," including an "[a]ccess control block list" that is a "[l]ist of service usage activities that are blocked." SAMSUNG-1001, 4:4-6, FIG. 42G. Indeed, in the '811 patent, preventing communication does not necessitate blocking previously-generated packets.

Moreover, despite PO's narrow interpretation, claim 4 only requires "preventing communication associated with the first application over the first wireless network" and says nothing of blocking data packets generated by the application. SAMSUNG-1001, 164:11-16. The Federal Circuit has cautioned, "[i]t is important not to import into a claim limitations that are not part of the claim." *Superguide Corp. v. DirecTV Enterprises, Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) ("a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment."); *Cont'l Circuits LLC v. Intel Corp.*, 915 F.3d 788, 797 (Fed. Cir. 2019) ("avoid improperly importing limitations into the claims"). Thus, the Board should reject PO's overly narrow interpretation that attempts to rewrite "preventing communication" as "blocking generated packets." Consistent with disclosure in the '811 patent, Jones' teaching of prohibiting a network backup service usage activity discloses claim 4's "preventing communication." SAMSUNG-1006, 5:26-29; Pet., 35, 38.

Date: October 18, 2024

/Jennifer J. Huang/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Jennifer J. Huang, Reg. No. 64,297
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on October 18, 2024, a complete and entire copy of this Petitioner's Reply to Patent Owner's Preliminary Response was provided by email, to the Patent Owner, by serving the correspondence address of record as follows:

Reza Mirzaie
Marc A. Fenster
Dale Chang
Amy E. Hayden
James A. Milkey
Neil Rubin
Philip X. Wang
Russ, August & Kabat
12424 Wilshire Blvd. 12th Floor
Los Angeles, CA 90025

Email: rak_headwater@raklaw.com
rmirzaie@raklaw.com
mfenster@raklaw.com
dchang@raklaw.com
ahayden@raklaw.com
jmilkey@raklaw.com
nrubin@raklaw.com
pwang@raklaw.com

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667