

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT AND APPEAL BOARD

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

v.

SECURE WI-FI LLC,
Patent Owner.

IPR2024-01367
Patent 10,694,384

PETITIONER'S REPLY TO
PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	Page
I. Patent Owner Interprets “‘Authenticated’ Access Point” in a way that is Inconsistent with its Interpretation of that Term in its Infringement Contentions	1
II. Patent Owner’s Characterization of the Co-Pending Litigation is Misleading	4

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Amazon.com, Inc. v. Barnesandnoble.com, Inc.</i> , 239 F.3d 1343 (Fed. Cir. 2001)	2
<i>Solas OLED Ltd. v. Samsung Display Co., Ltd.</i> , No. 2:19-CV-00152- JRG, 2020 WL 4040716 (E.D. Tex. Mar. 17, 2020)	4

LISTING OF EXHIBITS

<u>Exhibit No.</u>	<u>Exhibit Title</u>
Exhibit 1001	U.S. Patent 10,694,384, filed Mar. 30, 2018
Exhibit 1002	Declaration of Dr. Harry Bims
Exhibit 1003	Prosecution File History for U.S. Patent 10,694,384
Exhibit 1004	WO 2007/086705 (Yun), filed January 26, 2007
Exhibit 1005	[Reserved]
Exhibit 1006	US Application Publication 2012/0076072 (Jalfon), filed September 24, 2010
Exhibit 1007	U.S. Patent 8,126,476 (Vardi), filed July 25, 2008
Exhibit 1008	[Reserved]
Exhibit 1009	IEEE Std 802.11TM-2012 (<i>IEEE802.11</i>), dated March 29, 2012
Exhibit 1010	[Reserved]
Exhibit 1011	Infringement Contentions for U.S. Patent 10,694,384
Exhibit 1012	U.S. Patent 7,885,639 (Satish), filed June 29, 2006
Exhibit 1013	[Reserved]
Exhibit 1014	Prosecution File History for U.S. Patent 9,717,005
Exhibit 1015	Merriam-Webster's Collegiate Dictionary, 10 th Edition, 1999 (Excerpts)
Exhibit 1016	Email from Trials@uspto.gov, dated January 23, 2025, Re: IPR2024-01366, -01367

Exhibit 1017	Patent Owner Secure Wi-Fi's P.R. 4-2 Disclosure of Proposed Claim Constructions
Exhibit 1018	Petitioner Samsung's P.R. 4-2 Disclosure of Proposed Claim Constructions

CLAIM LISTING

Element Designation	Claim Language
Claim 1	
1[pre]	A method performed under control of an end device, the method comprising:
1[a]	generating, by the end device, a fake media access control (MAC) address for the end device;
1[b]	transmitting, by the end device to an access point, a probe request that includes the fake MAC address;
1[c]	receiving, by the end device from the access point, a probe response that includes information regarding the access point;
1[d]	determining, by the end device, that the access point is an authenticated access point based, at least in part, on the information in the probe response being indicative that the access point was connected with the end device previous to when the access point received the probe request transmitted by the end device; and
1[e]	transmitting, by the end device to the access point determined to be the authenticated access point, a connection request that includes an authentic device identifier for the end device.
Claim 2	
Claim 2	The method of claim 1, wherein the fake MAC address is distinct from an actual original MAC address of a hardware network interface of the end device.
Claim 3	
Claim 3	The method of claim 1, wherein information in the probe request is insufficient to identify the end device, so as to prevent leakage of present location information of the end device to non-authenticated access points.
Claim 4	
Claim 4	The method of claim 1, wherein generating the fake MAC address includes generating the fake MAC address from one or more characters that are selected randomly.
Claim 5	
Claim 5	The method of claim 1, wherein the authentic device identifier for the end device includes an authentic MAC address for a hardware network interface of the end device.

Claim 6	
6[pre]	The method of claim 1, further comprising:
6[a]	receiving, by the end device from the access point, an approval of the connection request; and
6[b]	connecting, by the end device, to a wireless local area network provided by the access point.
Claim 7	
Claim 7	The method of claim 6, wherein the access point includes a Wi-Fi access point, and wherein the wireless local area network includes a Wi-Fi network.
Claim 8	
8[pre]	The method of claim 1, further comprising:
8[a]	receiving, by the end device, a list of authenticated access points that includes information regarding one or more access points,
8[b]	wherein determining that the access point is the authenticated access point is further based on determining that the access point is included in the list of authenticated access points.
Claim 9	
9[pre]	A method performed by an end device, the method comprising:
9[a]	obtaining, by the end device, an authenticated access point list that includes information regarding one or more access points;
9[b]	generating, by the end device, a media access control (MAC) address for the end device that is distinct from an actual MAC address for a hardware network interface of the end device;
9[c]	transmitting, by the end device to at least one access point, a probe request that includes the generated MAC address;
9[d]	receiving, by the end device from the at least one access point in response to the probe request, a probe response that includes information regarding the at least one access point;
9[e]	determining, by the end device based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point,
9[f]	wherein determining that the at least one access point is the authenticated access point includes determining that the information regarding the at least one access point is included in the authenticated access point list; and

9[g]	transmitting, by the end device to the at least one access point after determining that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the end device.
Claim 10	
Claim 10	The method of claim 9, wherein information in the probe request is insufficient to identify the end device, so as to prevent leakage of present location information of the end device to non-authenticated access points.
Claim 11	
Claim 11	The method of claim 9, wherein generating the MAC address includes generating the MAC address from one or more characters that are selected randomly.
Claim 12	
Claim 12	The method of claim 9, wherein the information regarding the one or more access points includes at least one of a MAC address of each of the one or more access points, or a service set identifier (SSID) of each of the one or more access points.
Claim 13	
Claim 13	The method of claim 9, wherein determining that the at least one access point is the authenticated access point further includes determining that the at least one access point is the authenticated access point if the end device was previously-connected to the at least one access point.
Claim 14	
Claim 14	The method of claim 9, further comprising: receiving, by the end device from the at least one access point, an approval of the connection request; transmitting, by the end device to the at least one access point after receiving the approval of the connection request, an association request; receiving, by the end device from the at least one access point, an association response to the association request; and connecting to a communication network via the at least one access point in accordance with the association response.
Claim 15	
Claim 15	The method of claim 14, wherein the at least one access point includes a Wi-Fi access point, and wherein the communication network includes a Wi-Fi network that is accessible through the Wi-Fi access point.

Claim 16	
Claim 16	The method of claim 9, wherein the authentic device identifier for the end device includes the actual MAC address for the hardware network interface of the end device.
Claim 17	
17[pre]	An end device, comprising:
17[a]	a hardware network interface associated with an actual media access control (MAC) address;
17[b]	a processor coupled to the hardware network interface and operable to generate a MAC address for the end device that is distinct from the actual MAC address;
17[c]	a transmitter coupled to the processor and operable to transmit to an access point, a probe request that includes the generated MAC address; and
17[d]	a receiver coupled to the processor and operable to receive, from the access point, a probe response that includes information regarding the access point,
17[e]	wherein the processor is further operable to determine that the access point is an authenticated access point based, at least in part, on the information regarding the access point being indicative that the access point was connected with the end device previous to when the access point received the probe request transmitted from the transmitter, and
17[f]	wherein the hardware network interface is operable to connect, in response to determination that the access point is the authenticated access point, the end device to a wireless local area network provided by the access point.
Claim 18	
Claim 18	The end device of claim 17, wherein the access point includes a Wi-Fi access point, and wherein the wireless local area network includes a Wi-Fi network.
Claim 19	
Claim 19	The end device of claim 17, wherein the processor is operable to generate the MAC address from one or more characters that are selected randomly.

Claim 20	
20[pre]	The end device of claim 17, wherein:
20[a]	the transmitter is further operable to transmit, to the access point in response to the determination that the access point is the authenticated access point, a connection request that includes an authentic device identifier for the end device,
20[b]	The receiver is further operable to receive, from the access point, an approval of the connection request, and
20[c]	The hardware network interface is operable to connect the end device to the wireless local area network after the receiver receives the approval of the connection request.
Claim 21	
Claim 21	The end device of claim 20, wherein the authentic device identifier for the end device includes the actual MAC address.
Claim 22	
Claim 22	The end device of claim 17, further comprising a memory coupled to the processor and operable to store a list of authenticated access points that includes the information regarding the access point, wherein the information regarding the access point includes at least one of a MAC address of the access point, or a service set identifier (SSID) of the access point.
Claim 23	
Claim 23	The end device of claim 17, wherein the end device includes one of a cell phone, a personal data assistant (PDA), a personal media player device, a wireless web-watch device, a personal headset device, an application specific device, or a hybrid device.
Claim 24	
Claim 24	The end device of claim 17, wherein information in the probe request is insufficient to identify the end device, so as to prevent leakage of present location information of the end device to non-authenticated access points.

Pursuant to the Board's January 23, 2025, authorization (EX1016), Petitioner hereby files this Reply to address Patent Owner's arguments regarding the construction of the term "'authenticated' access point" and the record for the parallel district court action between Patent Owner and Petitioner ("Co-Pending Litigation") (see Paper 1 at 1-2 (Related Matters)).

I. PATENT OWNER INTERPRETS "'AUTHENTICATED' ACCESS POINT" IN A WAY THAT IS INCONSISTENT WITH ITS INTERPRETATION OF THAT TERM IN ITS INFRINGEMENT CONTENTIONS

In the current IPR proceeding, with validity at issue, Patent Owner proposes interpreting "authenticated access point" as an access point that has been "authenticated" by a "process of verifying the identity of an entity, using known, trusted, and verifiable information, before granting access to a resource" or that has been proven to be "real, true, or what people say it is." Paper 7 at 20-21. And according to Patent Owner, *Vardi* does not disclose such an "authenticated access point." Paper 7 at 21-27. But Patent Owner interpreted the same term much differently in its infringement contentions from the Co-Pending Litigation.¹

¹ To provide a complete record, Petitioner hereby includes Patent Owner's and Petitioner's respective Disclosures of Proposed Claim Construction exchanged in the Co-Pending Litigation. See EX1017 (Patent Owner); EX1018 (Petitioner).

[1d] determining, by the end device, that the access point is an authenticated access point based, at least in part, on the information in the probe response being indicative that the access point was connected with the end device previous to when the access point received the probe request	The Accused Products determine that the access point is an authenticated access point (e.g., a whitelisted and/or previously connected Wi-Fi access point) based, at least in part, on the information in the probe response being indicative that the access point was connected with the end device previous to when the access point received the probe request transmitted by the end device. As an example, the Accused Product confirms the received SSID information and/or other information from probe responses with access point information stored in its memory. Once confirmed that there is a probe response from an access point with which the Accused Product was connected previously, the Accused Product initiates a connection to the access point using an authenticated device identifier, such as a persistent MAC address that was used for a prior connection with the access point. The Accused Products maintain a list of previously-connected access points which is matched to the access point's SSID received in the probe response. Each previously-connected access point is linked to a persistent MAC address for connecting to that access point.
--	---

EX1011 at 30 (annotated). As demonstrated in the above excerpt from Patent Owner's infringement contentions, Patent Owner explicitly stated that determining an access point is an authenticated access point only requires "confirm[ing]" the SSID and/or other information from the probe response with access point information stored in its memory. *Id.* That is, an end device checks its memory using the received SSID and other information to see whether the access point previously provided connectivity to the end device. Patent Owner identified no further step was necessary to "verify the identity of an entity, using known, trusted, and verifiable information" or "to prove that something is real, true, or what people say it is."

Patent Owner cannot interpret a claim term one way for infringement and another for validity. *Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343, 1351 (Fed. Cir. 2001) ("A patent may not, like a 'nose of wax,' be twisted one way to avoid anticipation and another to find infringement."). When applying Patent

Owner's infringement contentions logic to *Vardi*, it is clear that *Vardi* teaches an “‘authenticated’ access point.”

For example, *Vardi* discloses its user terminal obtains and stores lists of access points that previously provided connectivity to the end device, including the MAC addresses and/or SSIDs those access points. *See* Paper 1 at 42-44 (Claim Element 9[a]); EX1007, 12:24-30, 14:52-57, 13:4-23, EX1002, ¶¶131-33. The information on the list is generated through scans from the user terminal by caching information from previous connections (*id.* at 42) or by conducting scans of available access points, providing the information to a server, and receiving the list back from the server (*id.* at 42-43). EX1007, 12:24-30, 14:52-57, 13:4-23. Then, during a network connection process, the information obtained from the IEEE 802.11 scan is compared to the list of access points that provided connectivity to the end device and is used to confirm the access point had previously provided connectivity to the user terminal, based on, for example MAC address and SSID. *See, e.g.*, EX1007, 12:24-30, 14:42-57, 13:4-18, 13:19-23 (“If a list of previously successfully used access points is available (locally stored) and some APs on the list are available...the client can select the AP with the highest RSSI value for connection”); EX1002, ¶¶ 115-20, 143-45; Paper 1 at 31-33 (Claim Element 1[d]). In that sense, applying Patent Owner's infringement-motivated interpretation, *Vardi* authenticates the access point before using it to provide connectivity to the user terminal.

II. PATENT OWNER'S CHARACTERIZATION OF THE CO-PENDING LITIGATION IS MISLEADING

As detailed below, Patent Owner's arguments regarding *Fintiv* factors 1 and 3 are misleading.

Factor 1: Patent Owner wrongly asserts that it is unlikely the district court will grant a stay due to the previously rejected stay motion. Paper 7 at 44-45. This mischaracterizes the issue. The initial stay motion was filed within a week of the Petition. As recognized by the Court, it is not unusual for courts to deny a motion to stay without prejudice before institution. EX2001 at 2. But the Co-Pending Litigation Court still invites parties to file early motions to stay because the Court awards weight to the timing of the moving party's *initial* motion to stay making the renewed post-institution stay more likely to be granted. *See Solas OLED Ltd. v. Samsung Display Co., Ltd.*, No. 2:19-CV-00152-JRG, 2020 WL 4040716, at *2 (E.D. Tex. Mar. 17, 2020) (acknowledging that "the Court must accord some weight to the timing of Samsung's Original Motion").

Factor 3: The parties' investment in the parallel proceedings is not as extensive as Patent Owner asserts. The parties' claim constructions were just exchanged this week, with opening briefs not due until March 31, 2025, which ultimately will result in a *Markman* order after **May 12, 2025** (hearing). And only after *Markman* will the parties be submitting Final Infringement and Invalidity

Contentions. Indeed, Patent Owner has yet to even serve its necessary supplemental infringement contentions based on Petitioner's confidential information. Significant work remains by the parties in the Co-Pending Litigation, including fact discovery, *Markman*, Final Invalidity Contentions, and expert discovery. All to occur after the Board's **March 26, 2025** Institution Decision deadline.

Respectfully submitted,

Dated: January 30, 2024

By: /Walter D. Davis, Jr/

Walter D. Davis, Jr.
Registration No.: 45,137
BLANK ROME LLP
1825 Eye Street, NW
Washington, DC 20006-5403
Tel: (202) 420-4847
Fax: (202) 478-0914
Email: walter.davis@blankrome.com

Counsel for Petitioner

CERTIFICATE OF SERVICE

I hereby certify that on January 30, 2025, a true and correct copy of the foregoing *PETITIONER'S REPLY TO PATENT OWNER'S PRELIMINARY RESPONSE* including exhibits was filed with the Patent Trial and Appeal Board Case Tracking System (P-TACTS), with a copy served via electronic mail to the following email addresses, as authorized in Patent Owner's Mandatory Notice (Paper 6):

jtice@bdiplaw.com

SecureWiFi_Samsung@bdiplaw.com

Dated: January 30, 2025

By: /Walter D. Davis, Jr./

Walter D. Davis, Jr.
Registration No.: 45,137
BLANK ROME LLP
1825 Eye Street, NW
Washington, DC 20006-5403
Tel: (202) 420-2200

Counsel for Petitioner