Palo Alto Networks, Inc. v. Centripetal Networks, LLC

United States Court of Appeals for the Federal Circuit

December 16, 2024, Decided

2023-1636

Reporter
122 F.4th 1378 *; 2024 LX 99887; 2024 U.S.P.Q.2D (BNA) 2178

PALO ALTO NETWORKS, ***INC***., Appellant ***v***. ***CENTRIPETAL NETWORKS***, ***LLC***, FKA ***CENTRIPETAL NETWORKS***, ***INC***., Appellee

Prior History: Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in No. IPR2021-01150.

Disposition: VACATED AND REMANDED.

Counsel: ANDREW T. RADSCH, Ropes & Gray LLP, East ***Palo Alto***, CA, argued for appellant. Also represented by JAMES RICHARD BATCHELDER; DOUGLAS HALLWARD-DRIEMEIER, Washington, DC; BRIAN LEBOW, New York, NY.

DANIEL NOAH LERMAN, Kramer Levin Naftalis & Frankel LLP, Washington, DC, argued for appellee. Also represented by JASON A. SHAFFER; PAUL J. ANDRE, JAMES R. HANNAH, Redwood Shores, CA; JEFFREY PRICE, New York, NY; JOHN R. HUTCHINS, SCOTT M. KELLY, BRADLEY CHARLES WRIGHT, Banner & Witcoff, Ltd., Washington, DC.

Judges: Before DYK, STOLL, and STARK, Circuit Judges.

Opinion by: STOLL

Opinion

[*1380] STOLL, *Circuit Judge*.

Palo Alto Networks, ***Inc***. ("PAN") successfully petitioned for *inter partes* review (IPR) of claims 1-18 of ***Centripetal Networks***, ***LLC***'s ("***Centripetal***'s") U.S. Patent No. 10,530,903 (the "'903 patent"), asserting unpatentability for obviousness based on three prior-art references, two of which are relevant here. PAN appeals the final written decision of the United States Patent and Trademark Office Patent Trial and Appeal Board (the "Board"), which concluded that PAN had not established by preponderant evidence that the claims would have been obvious over the relevant prior art combination. Because the Board erred by failing to explain its holding and reasoning regarding motivation to combine, we vacate and remand.

BACKGROUND

I

The '903 patent is titled "Correlating Packets In Communications ***Networks***" and discloses a "computing system" that may: (1) "identify packets received by a ***network*** device from a host located in a first ***network***," (2) "generate log entries corresponding to the packets received by the ***network*** device," (3) "identify packets transmitted by the ***network*** device to a host located in a second ***network***," (4) "generate log entries corresponding to the packets

transmitted by the ***network*** device," and (5) "correlate the packets transmitted by the ***network*** device with the packets received by the ***network*** device." U.S. Patent No. 10,530,903 at Title, Abstract. These packets are "small segments **[*1381]** that together make up a larger communication." Appellant's Br. 5.

The ***network*** device may include a device that alters the packets in a way that obfuscates the association of the packets received from the host with the corresponding packets generated by the ***network*** device. '903 patent col. 5 ll. 16-22. Correlating the packets transmitted by the ***network*** device with the packets received by the ***network*** device may enable the computing system to determine that the packets transmitted by the ***network*** device are associated with a distinct end-to-end communication. *Id.* col. 1 ll. 53-62. In other words, the packet correlation technique de-obfuscates the identity of an obfuscated host. The specification notes "there is a need for correlating packets in communications ***networks***." *Id.* col. 1 ll. 27-28.

"While such obfuscation may be done without malice, it may also be performed with malicious intent. For example, [a] ***network*** device[] . . . may be employed by a malicious entity to attempt to obfuscate, spoof, or proxy for the identity or location of [the] host . . . ." *Id.* col. 6 ll. 5-9. After correlation, the packet correlator may notify a host user and/or ***network*** administrator of a communication with a malicious entity. *Id.* col. 13 ll. 7-15.

Independent claim 1 of the '903 patent is illustrative of the challenged claims (claims 1-18) and recites:

> 1. A method comprising:
>
> determining, by a computing system, that a ***network*** device has received, from a first host located in a first ***network***, a plurality of first packets corresponding to first requests for content from a second host located in a second ***network***, wherein the ***network*** device comprises a proxy;
>
> determining, by the computing system, that the ***network*** device has generated a plurality of second packets corresponding to second requests, wherein the second requests correspond to the first requests, and wherein the second requests are configured to cause the second host to transmit, to the ***network*** device, the content;
> generating, by the computing system, a first plurality of log entries corresponding to the plurality of first packets, wherein each of the first plurality of log entries comprises a receipt timestamp indicating a packet receipt time, and wherein the first plurality of log entries comprise first data from the first requests;
> generating, by the computing system, a second plurality of log entries corresponding to a plurality of second packets, wherein each of the second plurality of log entries comprises a transmission timestamp indicating a packet transmission time, and wherein the second plurality of log entries comprise second data from the second requests;
> determining, by the computing system and for each transmission timestamp, differences between at least one packet transmission time indicated by transmission timestamps and at least one packet receipt time indicated by receipt timestamps;
> correlating, based on the differences and by comparing the first data and the second data, at least a portion of the plurality of first packets and at least a portion of the plurality of second packets; and
>
> *responsive to the correlating*:
>
> *generating, by the computing system, an indication of the first host; and*
>
> *transmitting, by the computing system, the indication of the first host*.

Id. col. 15 ll. 21-60 (emphasis added to highlight the disputed limitation).

[*1382] II

PAN's IPR petition included one ground of unpatentability, asserting that claims 1-18 would have been obvious over U.S. Patent Application Publication No. 2014/0280778 ("Paxton") and U.S. Patent No. 8,413,238 ("Sutton") in view

of U.S. Patent No. 8,219,675 ("Ivershen").[1] In its petition, "PAN relied on Paxton for all but one element of independent claim[] 1." Appellant's Br. 15. For the final limitation of claim 1—transmitting an indication of the first host responsive to the correlating—PAN "relied on Sutton's teaching of notifying ***network*** administrators about devices suspected of association with malicious activity." Appellant's Br. 17; *see* J.A. 105 ("A [person of ordinary skill in the art] would have been motivated to transmit the indication of the first host, e.g., to an administrator, as taught by Sutton, responsive to the correlating disclosed by Paxton.").

Paxton is titled "Tracking ***Network*** Packets Across Translational Boundaries" and "relates generally to identifying ***network*** packets, and more particularly, to determining the identity of ***network*** packets as they traverse boundaries that perform ***Network*** Address Translation (NAT)." J.A. 2514; J.A. 2518 ¶ 2. Paxton's background section provides that "[w]hen NAT is implemented, the source address of a packet changes from the original sender of the packet to the address of the boundary performing NAT." J.A. 2518 ¶ 3.

Paxton's system for tracking packets across translation boundaries operates as follows: (1) packets are sent from a client across a boundary to a server; (2) as a packet is transmitted from the client, the inside sensor can calculate a hash of the payload and store it alongside the header; and (3) after the packet traverses the boundary, the outside sensor can calculate a hash of the payload along with the header data of the packet. "Payloads can be matched based on at least three criteria: hash, time, and IP address. When an identical hash is observed on the outside sensor [] and inside sensor [], there is a high probability that the hashes belong to the same payload," "contain the same message," and "are sent from the same source." J.A. 2519 ¶ 21.

Paxton explains that "[t]he ability to identify the true source of packet transmission through a boundary can provide significant benefits to ***network*** security . . . [e.g.,] quickly identify[ing] nodes that are infected with malicious content, which can allow the ***network*** administrator to better identify the scope of the malicious incident." J.A. 2520 ¶ 30. Paxton discloses that its technique "can [be] utilize[d] . . . to attribute malicious activity sensed at the edge of a ***network*** back to its original source." *Id.*

Sutton is titled "Monitoring Darknet Access To Identify Malicious Activity" and "relates to identification of potentially malicious activity based upon access attempts to darknet addresses." J.A. 2556; J.A. 2561 col. 2 ll. 7-9. "Darknets [are] those IP addresses which are either unassigned or unused. Such darknets typically only receive traffic for one of three reasons: accident/mistake, backscatter, and malicious scanning." J.A. 2561 col. 1 ll. 24-27. One embodiment of Sutton's disclosure is:

> [A] method that includes . . . identifying a list of darknet addresses; monitoring communications originating from a protected ***network***; comparing destination addresses of the monitored communications **[*1383]** originating from the protected ***network*** to the list of darknet addresses; and if a match is found between the destination addresses and the list of darknet addresses, providing notification of potential malicious activity originating from the protected ***network***.

J.A. 2561 col. 2 ll. 9-19. The "notification of potential malicious activity originating from the protected ***network*** . . . can be provided to an administrator of a protected enterprise ***network***." J.A. 2566 col. 12 ll. 57-65. "Additionally, traffic may be automatically blocked, redirected or filtered based on predefined rules. Other responses can be provided to such notifications." J.A. 2567 col. 13 ll. 7-9.

As for the motivation to combine Paxton and Sutton, PAN made the following arguments in its petition:

> [A person of ordinary skill in the art] would have been motivated to modify Paxton's computing system to, after the correlating, notify administrators of devices involved with the malicious activity . . . and generate rules to be provisioned to a packet-filtering device . . . and used for identifying, filtering, and/or blocking host devices' future packet communications . . ., as taught by Sutton . . . . Thus, when a packet is detected as communicated

---

[1] While Paxton and Sutton remain relevant on appeal, "Ivershen is not directly relevant to this appeal because the Board did not reach this aspect of the claims." Appellant's Br. 16 n.3. Accordingly, we do not further describe or discuss Ivershen.

> to/from a darknet address (post-boundary), and Paxton discloses the ability to identify the hosts transmitting/receiving the packet (pre-boundary), Sutton teaches making that identification known to administrators and/or implementing rules to identify or drop future packets to prevent further malicious communications. Accordingly, it would have been obvious to a [person of ordinary skill in the art] to add Sutton's functionality . . . to Paxton's computing system . . . to improve ***network*** security . . . .
>
> Paxton leaves, to a [person of ordinary skill in the art], remedial steps (e.g., uses of the correlation results), which are taught by Sutton.

J.A. 86-87.

III

In its final written decision, the Board explained that "the argument that must be evaluated is whether Paxton as modified by Sutton would have taught the recited transmitting responsive to the correlation." J.A. 24. The Board correctly identified the combination asserted: one in which "a packet is detected as communicated to/from a darknet address (post-boundary)," where "Paxton discloses the ability to identify the hosts transmitting/receiving the packet (pre-boundary)," and where "Sutton teaches making that identification known to administrators and/or implementing rules to identify or drop future packets to prevent further malicious communications." J.A. 24-25 (citation omitted).

The Board acknowledged that PAN "contends that 'Paxton expressly teaches creating a log and notifying a ***network*** administrator of the identified host'" but the Board was "not persuaded that this argument was articulated sufficiently in the Petition." J.A. 26. The Board "f[ound] no argument in the Petition that asserts 'allow[ing] the ***network*** administrator to better identify the scope of malicious content' means that a transmission is made (or any other action is taken) responsive to the correlation." *Id.* (second alteration in original). The Board then found that "Sutton also fails to fill in this gap." J.A. 27.

The Board explained that it was left "with a correlation from Paxton with no specific actions taken post-correlation, and a transmission from Sutton unrelated to any correlation, but without the necessary bridge showing that one of ordinary skill in the art would have appreciated that the **[*1384]** transmission would be responsive to the correlation." *Id.* The Board thus concluded that PAN "ha[d] not provided [it] with argument and evidence sufficient to establish by a preponderance of the evidence that claim 1 would have been obvious." *Id.*

PAN appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(4)(A).

DISCUSSION

For the reasons explained below, we conclude that the Board erred by not clearly explaining its holding or rationale regarding motivation to combine and whether the proposed combination teaches the final limitation of claim 1: transmitting an indication of the first host responsive to the correlating.

"Obviousness is a question of law with underlying factual issues . . . ." *Elekta Ltd. **v**. ZAP Surgical Sys., Inc.*, 81 F.4th 1368, 1373-74 (Fed. Cir. 2023). The "test for obviousness is not . . . that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art." *MCM Portfolio **LLC** **v**. Hewlett-Packard Co.*, 812 F.3d 1284, 1294 (Fed. Cir. 2015) (quoting *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)). "[T]here must exist a motivation to combine various prior art references in order for a skilled artisan to make the claimed invention." *Virtek Vision Int'l ULC **v**. Assembly Guidance Sys., Inc.*, 97 F.4th 882, 887 (Fed. Cir. 2024). "Whether a skilled artisan would have been motivated to combine references" is a "question[] of fact reviewed for substantial evidence." *Elekta*, 81 F.4th at 1374. "Substantial evidence is such relevant evidence as a reasonable mind might accept as adequate to support a conclusion." *Meridian Prods., **LLC** **v**. United States*, 851 F.3d 1375, 1381 (Fed. Cir. 2017) (citation omitted). Although "we review decisions, not opinions, . . . a Board opinion must contain sufficient findings and reasoning to permit meaningful appellate scrutiny." *Gechter **v**. Davidson*, 116 F.3d 1454, 1458 (Fed. Cir. 1997).

I

The parties disagree on whether the Board found a motivation to combine Paxton and Sutton, and what the Board meant when it said that "the necessary bridge" was missing. PAN argues that "the Board did not dispute that a motivation existed to combine Paxton and Sutton," Appellant's Br. 3, and that "the Board[] [improperly] search[ed] for a 'bridge' within the confines of Paxton and Sutton," Appellant's Br. 37. ***Centripetal*** asserts that the Board found that "PAN established no motivation to combine," Appellee's Br. 38, and that "PAN had not established 'the necessary bridge' between the prior art and the claimed limitation," Appellee's Br. 34.

"Our precedent dictates that the [Board] must make a finding of a motivation to combine when it is disputed." *In re Nuvasive, Inc.*, 842 F.3d 1376, 1382 (Fed. Cir. 2016). The "'factual inquiry whether to combine references must be thorough and searching,' and '[t]he need for specificity pervades [our] authority' on the [Board's] findings on motivation to combine." *Id.* at 1381-82 (first two alterations in original) (quoting *In re Lee*, 277 F.3d 1338, 1343 (Fed. Cir. 2002)). "Although identifying a motivation to combine 'need not become [a] rigid and mandatory formula[],' the [Board] must articulate a *reason why* a [person of ordinary skill in the art] would combine the prior art references." *Id.* at 1382 (citation omitted) (first two alterations in original). "If the Board finds that there would have been no motivation to combine [references] . . ., it must **[*1385]** expressly say so with an adequate explanation." *Vicor Corp. **v**. SynQor, Inc.*, 869 F.3d 1309, 1324 (Fed. Cir. 2017).

We hold that the Board failed to make the requisite finding on motivation to combine, and that it failed to explain what it meant by "necessary bridge." The Board summarized PAN's arguments regarding motivation to combine, J.A. 20-24, and recited a statement on motivation to combine from its Institution Decision and ***Centripetal***'s response thereto, J.A. 22, but it never made a clear finding on whether a person of ordinary skill in the art would have been motivated to modify Paxton by adding Sutton's step of transmitting a notification of malicious activity after Paxton's correlation step as proposed by PAN. *See* J.A. 20-27. Relatedly, we cannot discern with any confidence what the Board meant when it said that it was left "with a correlation from Paxton . . ., and a transmission from Sutton . . ., but without the necessary bridge showing that one of ordinary skill in the art would have appreciated that the transmission would be responsive to the correlation." J.A. 27. If the Board meant to say that it found no motivation to combine—and we do not know whether it did—it certainly failed to explain why a person of ordinary skill in the art would not have been motivated to modify Paxton to provide the recited notification as taught by Sutton in response to the correlation disclosed in Paxton.

PAN argues that "it was known in the art that, to address, quarantine, or otherwise respond to the source of malicious activity once identified, a ***network*** administrator or other actor must be notified of that original source." Appellant's Br. 27. As PAN notes, Paxton explains that identifying "the true source of packet transmission through a boundary can provide significant benefits to ***network*** security . . . . It can provide a way to quickly identify nodes that are infected with malicious content, which can *allow the **network** administrator to better identify the scope of the malicious incident*." J.A. 2520 ¶ 30 (emphasis added); *see, e.g.*, Appellant's Br. 27, 29. Logically, continues PAN, to identify the scope of the malicious incident, Paxton's ***network*** administrator would need to be informed of the identity of the infected nodes. *See, e.g.*, Appellant's Br. 38 ("[W]ithout such a notification no action could be taken to correct the identified problem."). PAN then notes that Sutton provides that "a notification of potential malicious activity . . . can be provided to an administrator of a protected enterprise ***network***." J.A. 2566 col. 12 ll. 57-65; *see, e.g.*, Appellant's Br. 27, 29.

PAN asserts that, like Paxton, Sutton also seeks to enhance ***network*** security and prevent malicious activity. Sutton explains that "[m]alicious code typically attempts to exploit security loopholes on various devices connected to the Internet," J.A. 2561 col. 1 ll. 7-8, and goes on to describe a "distributed security system" that "includes content processing nodes . . . that detect and preclude the distribution of security threats, e.g., malware, spyware, and other undesirable content." J.A. 2561 col. 2 ll. 41-46; *see, e.g.*, Appellant's Br. 38 ("Paxton teaches that its correlation techniques should be employed to benefit ***network*** security and Sutton teaches notifying an administrator for that same reason—to benefit ***network*** security.").

Given this evidence and argument by PAN, the Board erred by not addressing the evidence and the argument for the motivation to combine and by failing to provide an adequate explanation for its finding. *See Vicor*, 869 F.3d at 1324.

II

In addition to its failure to make the required motivation-to-combine finding **[*1386]** in this case, the Board failed to resolve the very issue it had identified: "whether Paxton as modified by Sutton would have taught the recited transmitting responsive to the correlation." J.A. 24. Instead, it erred by looking at the references individually. The Board found that Paxton alone did not meet the "transmitting responsive to the correlation" limitation. J.A. 24; J.A. 26. It then found that "Sutton also fails to fill in this gap." J.A. 27. Immediately after its summary of Sutton, the Board provided its determination regarding the missing "necessary bridge." *Id.* This analysis constitutes legal error.

"The question in an obviousness inquiry is whether it would have been obvious to a person of ordinary skill in the art to combine the relevant disclosures of the two references, not whether each individual reference discloses all of the necessary elements." *Game & Tech. Co. **v**. Wargaming Grp. Ltd.*, 942 F.3d 1343, 1352 (Fed. Cir. 2019). Where, as here, the grounds for obviousness are based on a specific combination of references, arguments that "attack the disclosures of the two references individually" lack merit. *Bradium Techs. **LLC** **v**. Iancu*, 923 F.3d 1032, 1050 (Fed. Cir. 2019). Here, Paxton and Sutton must be read together, not in isolation. *See, e.g., Randall Mfg. **v**. Rea*, 733 F.3d 1355, 1362 (Fed. Cir. 2013) (explaining that in *KSR International Co. **v**. Teleflex Inc.*, 550 U.S. 398, 127 S. Ct. 1727, 167 L. Ed. 2d 705 (2007), the Supreme Court "[r]eject[ed] a blinkered focus on individual [prior art references]" and "required an analysis that reads the prior art in context"). Specifically, the Board must consider whether the particular combination argued by the Petitioner—modifying Paxton by adding Sutton's notification step after Paxton's correlation step—would meet the claim limitations at issue.

Centripetal asserts that the Board "considered Paxton and Sutton in combination" but "agreed with ***Centripetal*** 'that this combination is insufficient to teach the disputed limitation.'" Appellee's Br. 33 (citing J.A. 25). We reject this argument. The language that ***Centripetal*** quotes is not the Board's analysis, but rather the Board's recital of ***Centripetal***'s own position. The Board explained: "*Patent Owner argues* that this combination is insufficient to teach the disputed limitation." J.A. 25 (emphasis added). Mere summation of ***Centripetal***'s argument does not constitute the Board's adoption or agreement. It is telling that the only support ***Centripetal*** cites in arguing that the Board analyzed the combination of Paxton and Sutton is ***Centripetal***'s own argument. In our review, we see no such analysis by the Board. By reading Paxton and Sutton in isolation, the Board erred.

CONCLUSION

For the foregoing reasons, we vacate and remand for the Board to clarify and explain its holding on whether a person of ordinary skill in the art would have been motivated to transmit the identity of the first host (e.g., to an administrator) as taught by Sutton, responsive to the correlating disclosed by Paxton to improve ***network*** security.

VACATED AND REMANDED

COSTS

Costs to Appellant.

End of Document