

United States Court of Appeals for the Federal Circuit

APPLE INC.,
Appellant

v.

MPH TECHNOLOGIES OY,
Appellee

2021-1532, 2021-1533, 2021-1534

Appeals from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos. IPR2019-00823, IPR2019-00824, IPR2019-00826.

Decided: March 9, 2022

JOSEPH R. PALMORE, Morrison & Foerster LLP, Washington, DC, argued for appellant. Also represented by SETH W. LLOYD, BRIAN ROBERT MATSUI; LENA HUGHES; New York, NY; RICHARD HUNG, San Francisco, CA; BITA RAHEBI, Los Angeles, CA.

BRIAN ERIK HAAN, Lee Sheikh Megley & Haan LLC, Chicago, IL, argued for appellee. Also represented by ASHLEY E. LAVALLEY, CHRISTOPHER LEE, RICHARD BURNS MEGLEY, JR.; JAMES CARMICHAEL, STEPHEN TERRY SCHREINER, Carmichael IP, PLLC, Tysons Corner, VA.

Before MOORE, *Chief Judge*, PROST and TARANTO, *Circuit Judges*.

MOORE, *Chief Judge*.

Apple appeals from three Patent Trial and Appeal Board *inter partes* review final written decisions collectively holding Apple failed to show claims 2, 4, 9, and 11 of U.S. Patent No. 9,712,494; claims 7–9 of U.S. Patent No. 9,712,502; and claims 3, 5, 10, and 12–16 of U.S. Patent No. 9,838,362 would have been obvious. For the following reasons, we affirm.

BACKGROUND

I

The challenged patents share a written description and purport to improve secure messaging between arbitrary hosts (e.g., messaging across local area networks (LANs), private and public wide area networks (WANs), or the internet) utilizing Internet Protocol (IP) security protocols. '494 patent at 1:54–57; 7:38–45.¹ IP security protocols require establishing a security association, *id.* at 2:39–49, that costs computation time and increases network latency, *id.* at 4:44–45. They are purportedly designed for static connections and, thus, not well suited for communications with mobile computers, leading to poor quality of service for communication over wireless links. *Id.* at 4:39–43; 5:7–14. To solve these problems, systems commonly utilize an intermediate host that facilitates communication between a mobile terminal and its communication target (e.g., a security gateway). *Id.* at 5:15–6:14. These common solutions, however, heavily rely on a concept known as tunneling. In tunneling, typically an entire data packet, including its outer header, is encapsulated and a new outer

¹ For simplicity, we cite to the '494 patent.

header is added. *Id.* at 3:21–49. The use of tunneling in the known solutions can cause extra packet size overhead, or require the intermediate computer to decrypt the packet, which could cause potential security problems. *Id.* at 6:21–24.

The patents disclose a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network that purportedly avoids these disadvantages. *Id.* at Abstract; 6:28–31. Preferably, a first computer “processes [a] formed message using a security protocol and encapsulates the message at least in an outer IP header,” which is sent to an intermediate computer. *Id.* at 6:54–59. The intermediate computer “matches the outer IP header address fields together with a unique identifier used by the security protocol, and performs a translation of the outer addresses and the unique identity used by the security profile.” *Id.* at 6:59–63. The translated packet is then sent to a second computer, which processes it using a standard security protocol. This method does not use any “extra encapsulation overhead” typical of prior-art solutions. *Id.* at 6:65–67.

The claims of the ’494 and ’362 patents cover the intermediate computer. Claim 1 of the ’494 patent is a representative independent claim for those patents:

1. An intermediate computer for secure forwarding of messages in a telecommunication network, comprising:

an intermediate computer configured to connect to a telecommunication network;

the intermediate computer configured to be assigned with a first network address in the telecommunication network;

the intermediate computer configured to receive from a mobile computer a secure message sent to the first network address

having an encrypted data payload of a message and a unique identity, the data payload encrypted with a cryptographic key derived from a key exchange protocol;

the intermediate computer configured to read the unique identity from the secure message sent to the first network address; and

the intermediate computer configured to access a translation table, to find a destination address from the translation table using the unique identity, and

to securely forward the encrypted data payload to the destination address using a network address of the intermediate computer as a source address of a forwarded message containing the encrypted data payload wherein the intermediate computer does not have the cryptographic key to decrypt the encrypted data payload.

(emphasis added).

The '502 patent claims the mobile computer that sends the secure message to the intermediate computer. Claim 1 is a representative independent claim:

1. A computer for sending secure messages, and for enabling secure forwarding of messages in a telecommunication network by an intermediate computer to a recipient computer, comprising:

a computer configured to connect to a telecommunication network;

the computer configured to be assigned with a network address in the telecommunication network, wherein the computer is

a mobile computer in that the address of the mobile computer changes;

the computer configured to form a secure message by encrypting the data payload of a message and giving the message a unique identity and a destination address of an intermediate computer, wherein the unique identity and the destination address are capable of being used by the intermediate computer to find an address to a recipient computer;

the computer configured to send the secure message to the intermediate computer for forwarding of the encrypted data payload to the recipient computer; and

the computer configured to set up a secure connection using a key exchange protocol.

II

MPH asserted claims of the challenged patents against Apple in the Northern District of California. Apple petitioned for *inter partes* review of each claim of the three patents, relying primarily on a combination of Request for Comments 3104 (RFC3104)² and U.S. Patent No. 7,032,242 (Grabelsky) (collectively, the combination). The Board held that Apple failed to show that several dependent claims of each patent would have been obvious in view of the combination. Apple challenges each of these determinations. We have jurisdiction under 28 U.S.C. § 1295(a)(4)(A).

² G. Montenegro & M. Borella, *RSIP Support for End-to-end IPsec*, Request for Comments 3104, The Internet Society (Oct. 2001).

DISCUSSION

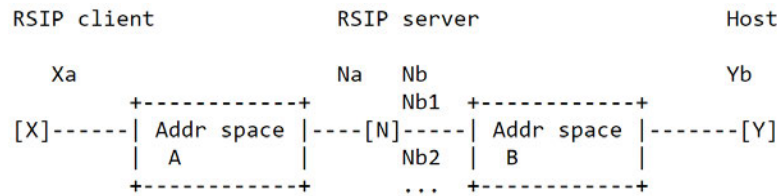
We review claim construction de novo and any subsidiary factual findings based on extrinsic evidence for substantial evidence. *Cisco Sys., Inc. v. Int'l Trade Comm'n*, 873 F.3d 1354, 1360 (Fed. Cir. 2017). Claim terms are generally given their plain and ordinary meaning, which is the meaning one of ordinary skill in the art would ascribe to a term when read in the context of the claim, specification, and prosecution history. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1313–14 (Fed. Cir. 2005) (en banc). “There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution.” *Thorner v. Sony Comput. Ent. Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

We also review the Board’s legal conclusions of obviousness de novo and factual findings for substantial evidence. *Personal Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 991 (Fed. Cir. 2017). “What a piece of prior art teaches presents a question of fact.” *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1364 (Fed. Cir. 2015).

I

Dependent claim 11 of the ’494 patent and dependent claim 12 of the ’362 patent require that “the source address of the forwarded message is the same as the first network address.” The Board was not persuaded that RFC3104 discloses this limitation.

RFC3104 discloses mechanisms for enabling IP security protocol communications using Realm Specific IP (RSIP). The document utilizes the following model topology:



J.A. 1187. In this model, an RSIP server examines a packet sent by Y destined for X. J.A. 1188. “X and Y belong to different address spaces A and B, respectively, and N is an [intermediate] RSIP server.” *Id.* N has two addresses: Na on address space A and Nb on address space B, which are different. *Id.* According to Apple, the message sent from Y to X is received by RSIP server N on the Nb interface and then must be sent to Na before being forwarded to X as shown in the diagram below:



J.A. 249–50. In Apple’s view, because the intermediate computer sends the message from Nb to Na before forwarding it to X, Na is both a first network address and the source address of the forwarded message. That the message was not sent directly to Na, Apple claims, is of no import given the claim language. The Board disagreed and found there was no record evidence that the mobile computer sent the message directly to Na. *Apple Inc. v. MPH*

Techs. Oy, No. IPR2019-00823, 2020 WL 6494243, at *22 (P.T.A.B. Nov. 4, 2020).³

Apple argues the Board misconstrued the claims to require that the mobile computer send the secure message *directly* to the intermediate computer. According to Apple, that construction is inconsistent with the phrase “intermediate computer configured to receive from a mobile computer a secure message sent to the first network address” in claim 1 of the ’494 patent, upon which claim 11 depends.⁴ Under this passive language, Apple claims, the mobile computer need not send the message to the first network address so long as the message is sent there eventually. Opening Br. 27–31; Oral Arg. at 2:27–3:16.⁵ We do not agree.

The plain meaning of “intermediate computer configured to receive from a mobile computer a secure message sent to the first network address” requires the mobile computer to send the message to the first network address. The phrase identifies the sender (i.e., the mobile computer) and the destination (i.e., the first network address). The proximity of the concepts links them together, such that a natural reading of the phrase conveys the mobile computer sends the secure message *to* the first network address. That the claims use passive voice is of no import. The plain language establishes direct sending.

³ The final written decision for the ’494 patent is nearly identical in several respects to that of the ’362 patent. For simplicity, we cite to the final written decision of the ’494 patent.

⁴ Claim 1 of the ’362 patent, upon which claim 12 depends, contains the same phrase, except it refers to a “second computer” instead of a “mobile computer.”

⁵ Available at https://oralarguments.cafc.uscourts.gov/default.aspx?fl=21-1532_01142022.mp3.

The written description confirms this plain meaning. It describes how the mobile computer forms the secure message with “the destination address . . . of the intermediate computer.” ’494 patent at 6:56–58 (emphasis added); *accord id.* at 11:32–33. The mobile computer then sends the message to that address. *Id.* at 6:58–63. There is no passthrough destination address in the intermediate computer that the secure message is sent to before the first destination address. Accordingly, like the claim language, the written description describes the secure message as sent from the mobile computer directly to the first destination address.

Apple’s claim construction argument therefore fails. And Apple does not challenge the Board’s finding that RFC3104 does not disclose the limitation of claim 11 of the ’494 patent and claim 12 of the ’362 patent under the Board’s construction. Accordingly, we affirm the Board’s holding that Apple failed to show those claims would have been obvious.

II

Dependent claim 4 of the ’494 patent is similar to claim 5 of the ’362 patent and recites:

4. The intermediate computer of claim 1, wherein the translation table includes two partitions, the first partition containing *information fields* related to the connection over which the secure message is sent to the first network address, the second partition containing information fields related to the connection over which the forwarded encrypted data payload is sent to the destination address.

(emphasis added).

The Board interpreted “information fields” in this claim to require “two or more fields.” *Apple*, 2020 WL 6494243, at *19. And because Apple’s obviousness argument relied on Figure 21 of Grabelsky, which disclosed a

partition with only a single field, the Board found Apple failed to show the combination taught this limitation. *Id.* at *19–20. Moreover, the Board found Apple failed to show a motivation to modify the combination to use multiple fields. *Id.* at *20–21. Apple challenges this finding as well as the Board’s construction of information fields.

A

On claim construction, Apple claims there is a presumption that a plural term covers one or more items. Opening Br. 33. It suggests that patentees can overcome that presumption by using a word, like plurality, that clearly requires more than one item. Oral Arg. at 9:44–10:20. Apple misstates the law.

In accordance with common English usage, we presume a plural term refers to two or more items. *See Leggett & Platt, Inc. v. Hickory Springs Mfg. Co.*, 285 F.3d 1353, 1357 (Fed. Cir. 2002) (“[T]he claim recites ‘support wires’ in the plural, thus requiring more than one welded ‘support wire.’”); *cf. Dayco Prods. v. Total Containment, Inc.*, 258 F.3d 1317, 1327–28 (Fed. Cir. 2001) (plurality “when used in a claim, refers to two or more items, absent some indication to the contrary”). That presumption can be overcome when the broader context shows a different meaning applies. *See Versa Corp. v. Ag-Bag Int’l. Ltd.*, 392 F.3d 1325, 1330 (Fed. Cir. 2004) (holding a plural term, in context, did not require more than one item). This is simply an application of the general rule that claim terms are usually given their plain and ordinary meaning. *See Thorner*, 669 F.3d at 1365 (discussing exceptions to plain-and-ordinary meaning rule).⁶

⁶ Apple’s reliance on the statutory canon that “in the absence of the contrary indication . . . the singular includes the plural (and vice versa)” is misplaced. Opening Br. 33 (quoting Antonin Scalia and Bryan A. Garner, *Reading*

Here, the term “information fields” is plural and, thus, presumably requires more than one field. Nothing in the phrase “partition containing information fields related to the connection” or surrounding claim language suggests otherwise. There is no indication, for example, that the use of the plural fields represents an effort to “achieve grammatical consistency” with another term. *In re Omneprazole Patent Lit.*, 84 F. App’x 76, 80 (Fed. Cir. 2003) (non-precedential). Nor is the term used to describe a function (e.g., means for creating fields). *See Versa Corp.*, 392 F.3d at 1330 (holding “means for creating air channels” did not require a supporting structure that made multiple channels).

The written description also does not persuade us to depart from the presumption that “information fields” refers to two or more fields. For example, we see no express language indicating the plural should include the singular or broadly describing the invention as containing one or more fields. To be sure, there is nothing in the written description providing any significance to using a plurality of information fields in a partition. However, absent any contrary intrinsic evidence, the Board correctly held that fields referred to more than one field.

B

On motivation to modify the combination to use more than one field, Apple faults the Board for rejecting its expert’s testimony. Apple argues the Board abused its discretion by applying the teaching, suggestion, or motivation

Law: The Interpretation of Legal Texts 129 (2012)). The United States Code expressly states that “[i]n determining the meaning of any Act of Congress, unless the context indicates otherwise . . . words importing the plural include the singular . . .” 1 U.S.C. § 1. In short, Congress made clear through statute that plural includes singular. There is no similar definition in this patent.

test rejected in *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398 (2007). We see no such error in the Board's analysis.

The Board examined both the initial and the supplemental declarations of Apple's expert. It found that testimony was conclusory and was, as a whole, improperly guided by hindsight. *Apple*, 2020 WL 6494243, at *21. The Board emphasized how Apple's expert used the phrases "would naturally have included"; "it would be logical"; and "could be, and most logically would be." *Id.* It also found that there was no factual support underlying the expert testimony. *Id.* The Board determined that the testimony amounted to an argument about "what *could* be combined" and a conclusory statement that the combination would have been obvious. *Apple*, 2020 WL 6494243, at *21.

The Board was free to reject Apple's expert's testimony based on a lack of factual support. *See TQ Delta, LLC v. CISCO Sys., Inc.*, 942 F.3d 1352, 1362 (Fed. Cir. 2019) (reversing obviousness determination when expert's testimony was "[u]ntethered to any supporting evidence" and, thus, could not support the Board's findings). Likewise, it was free to disregard the testimony for failure to provide "any meaningful explanation for why [a skilled artisan] would be motivated to combine these references at the time of this invention." *InTouch Techs., Inc. v. VGO Commc'ns, Inc.*, 751 F.3d 1327, 1352 (Fed. Cir. 2014). We see no use or endorsement of an erroneous obviousness standard in the Board's analysis. Nor can we reweigh evidence on appeal. *See In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1334 (Fed. Cir. 2016). Accordingly, we decline to disturb the Board's findings, which are supported by substantial evidence.

III

Claim 2 of the '494 patent and claim 3 of the '362 patent recite:

The intermediate computer of claim 1, wherein the intermediate computer is further configured to *substitute* the unique identity read from the secure message with another unique identity prior to forwarding the encrypted data payload.

(emphasis added).

The Board construed the word substitute to require “changing or modifying, not merely adding to.” *Apple*, 2020 WL 6494243, at *10. Because it determined that RFC3104—which Apple relied on for this limitation—merely involved “adding to” the unique identity, the Board found Apple had failed to show RFC3104 taught this limitation. *Id.* at *18. It also found that Apple failed to show a skilled artisan would have been motivated to modify the combination to arrive at the claimed invention. *Id.* at *19.

Apple argues the undisputed evidence shows the combination taught an intermediate computer “configured to substitute the unique identity” as required by claim 2 of the ’494 patent and claim 3 of the ’362 patent. Opening Br. 43–46. The parties agree RFC3104 taught tunneling, which involves adding a new outer IP header to an encapsulated data packet. To Apple, this means RFC3104 “substitute[s] the unique identity,” so the Board’s contrary finding is unsupported by substantial evidence.

The Board’s uncontested claim construction of substitute disposes of Apple’s challenge. The Board expressly addressed Apple’s nearly identical argument from the hearing that “adding the header is the same as replacing the header because at the end of the day you have a different header than what you had before, a completely different header.” J.A. 640. The Board disagreed with Apple and construed substitute to mean “changing, replacing, or modifying, not merely adding,” and observed that this construction disposed of Apple’s position. *Apple*, 2020 WL 6494243, at *10. Apple did not appeal that construction, and we also have no reason to doubt it, as the written

description disparages prior art solutions utilizing tunneling. See '494 patent at 5:15–50; 6:21–34. In view of the unchallenged construction, substantial evidence supports the Board's finding that RFC3104's disclosure of adding a new header does not satisfy the substitution required by the claims.

Moreover, substantial evidence supports the Board's finding that Apple failed to show a motivation to modify the prior art combination to include substitution. *Apple*, 2020 WL 6494243, at *19. Apple relied solely on its expert's contrary testimony, which the Board properly disregarded as conclusory. *Id.*

IV

Claim 9 of the '494 patent is similar to claim 10 of the '362 patent and recites:

9. The intermediate computer of claim 1, wherein the intermediate computer is configured to *modify the translation table entry address fields* in response to a signaling message sent from the mobile computer when the mobile computer changes its address such that the intermediate computer can know that the address of the mobile computer is changed.

(emphasis added).

Apple argued that establishing a secure authorization in RFC3104 includes creating a new table entry address field as required by the claim. *Apple*, 2020 WL 6494243, at *21. The Board disagreed, reasoning that “modify[ing] the translation table entry address fields” requires having existing address fields when the mobile computer changes its address. J.A. 51. Accordingly, it found Apple failed to show the combination taught this limitation.

Apple now argues the “configured to modify the translation table entry address fields” limitation is purely

functional and, thus, covers any embodiment that results in a table with different address fields, including new address fields. We do not agree.

As the Board held, the plain meaning of “modify[ing] the translation table entry address fields” requires having existing address fields in the translation table to modify. The surrounding language showing the modification occurs “when the mobile computer changes its address such that the intermediate computer can know that the address of the mobile computer is changed” further supports the existence of an address field prior to modification. Accordingly, the limitation does not merely claim a result; it recites an operation of the intermediate computer that requires an existing address field.⁷

V

Claim 13 of the ’362 patent, on which claims 14–16 depend, recites:

13. The intermediate computer of claim 1, wherein the intermediate computer is configured to receive a request to update the mapping with a new address of the first computer.

Apple relied on its reasoning as to claim 10 of the ’362 patent to show that the proposed combination taught this limitation. The Board likewise relied on the deficiencies it identified for claim 10 of the ’362 patent to find Apple failed to show the combination taught this claim without any additional analysis. *Apple v. MPH Techs. Oy*, No. IPR2019-00826, 2020 WL 6494252, at *13 (P.T.A.B. Nov. 4, 2020). Apple argues this explanation is inadequate because the Board’s claim-10 analysis focuses on a different limitation:

⁷ Because we reject Apple’s claim construction, we need not address its substantial evidence challenge that depends on that construction.

the requirement to “modify the translation table entry address fields.”

The Board’s analysis adequately disposed of Apple’s challenge. Certainly, the Board’s analysis focused on the plain meaning of “modify” and its implicit requirement that the objects of modification (i.e., address fields) already exist. But the Board placed the same requirement on the term update in its analysis: “the plain meaning of ‘updates,’ requires an existing entry and existing address fields.” J.A. 129. Accordingly, the Board’s reliance on its analysis of claim 10 explains its disposition of claim 13 and associated dependent claims; Apple failed to show the combination taught an intermediate computer that updates an existing mapping. We, therefore, see no error in the Board’s analysis.

VI

Claim 7 of the ’502 patent, on which claims 8 and 9 depend, recites:

7. The computer of claim 1, wherein the computer is configured to send a signaling message to the intermediate computer when the computer changes its address such that the intermediate computer can know that the address of the computer is changed.

RFC3104 disclosed an ASSIGN_REQUEST_RSIPSEC message that requests an IP address assignment. Apple argued that, when a computer moves to a new address, the computer uses this message as part of establishing a secure connection and, in the process, the intermediate computer knows the address has been changed. J.A. 5034–36. The Board found that the message was not used to signal address changes. *Apple Inc. v. MPH Techs. Oy*, No. IPR2019-00824, 2020 WL 6494246, at *16 (P.T.A.B. Nov. 4, 2020). Accordingly, it found Apple failed to show that the

intermediate computer knows that the address is changed, as required by the claim language.

Apple reprises its arguments, which the Board rejected. Claims 7–9 of the '502 patent require a computer to send a message to the intermediate computer “such that the intermediate computer can know that the address of the computer is changed.” Apple claims that RFC3104’s use of an ASSIGN_REQUEST_RSIPSEC message in establishing a secure authorization necessarily satisfies this limitation because the mobile computer must communicate the new address. However, the Board’s contrary finding is supported by substantial evidence, including MPH’s expert testimony and RFC3104 itself.⁸

MPH’s expert testified that a skilled artisan would not have understood the relevant disclosure in RFC3104 to teach any signal address changes. J.A. 8400. Indeed, as the Board found, the relevant disclosure in RFC3104 relates to establishing an RSIP-IPSec session, not to signal address changes. *Apple*, 2020 WL 6494246, at *16–17. And we see no reason why the Board was required to equate communicating a new address and signaling an address change. Accordingly, substantial evidence supports the Board’s finding.

CONCLUSION

For the foregoing reasons, we affirm the Board’s final written decisions holding that claims 2, 4, 9, and 11 of the '494 patent; claims 7–9 of the '502 patent; and claims 3, 5,

⁸ Though framed as a claim construction issue, Apple does not dispute that the limitation requires the intermediate computer to know the address is changed, and we see no error in that construction. The Board found RFC3104 failed to meet this requirement. Accordingly, we treat Apple’s argument as a substantial evidence challenge.

18

APPLE INC. v. MPH TECHNOLOGIES OY

10, and 12–16 of the '362 patent would not have been obvious.

AFFIRMED

COSTS

Costs to MPH.