NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

MPH TECHNOLOGIES OY,
Plaintiff-Appellant

v.

APPLE INC.,
Defendant-Appellee

2025-1069

Appeal from the United States District Court for the Northern District of California in No. 3:18-cv-05935-TLT, Judge Trina L. Thompson.

Decided: August 3, 2026

DEREK L. SHAFFER, Quinn Emanuel Urquhart & Sullivan, LLP, Washington, DC, argued for plaintiff-appellant. Also represented by STEVEN CHERNY, PATRICK DANIEL CURRAN, Boston, MA; CHRISTOPHER SABBAGH, Houston, TX.; BRIAN ERIK HAAN, JAMES DANIEL MITCHELL, DAVID J. SHEIKH, Arnold & Porter Kaye Scholer LLP, Chicago, IL.

BRIAN ROBERT MATSUI, Morrison & Foerster LLP, Washington, DC, argued for defendant-appellee. Also represented by SETH W. LLOYD, Washington, DC; ALEXANDRA

M. AVVOCATO, New York, NY; RICHARD HUNG, San Francisco, CA; ROSE S. LEE, RYAN J. MALLOY, BITA RAHEBI, Los Angeles, CA.

Before LOURIE, HUGHES, and STOLL, *Circuit Judges*.

STOLL, *Circuit Judge*.

MPH Technologies Oy filed a patent infringement suit against Apple Inc. in the United States District Court for the Northern District of California, accusing Apple of infringing various claims of U.S. Patent Nos. 8,346,949; 9,762,397; 9,712,494; 9,712,502; and 9,838,362 (collectively, the "'949 patent family"); as well as U.S. Patent No. 7,937,581. At claim construction, the district court (1) construed the "secure" terms in the asserted claims of the '949 patent family as limited to the IPSec protocol and (2) construed the term "unique identity" of the '949 patent family as limited to SPI values, which are specific to the IPSec protocol. The district court also held claims 6, 7, and 8 in the '581 patent indefinite. Following claim construction, the parties stipulated to judgment of noninfringement of the '949 patent family and invalidity of the '581 patent.

First, MPH appeals the district court's constructions of the '949 patent family's "secure" terms as requiring the IPSec protocol and the '949 patent family's "unique identity" term as limited to SPI values specific to the IPSec protocol. We hold that the disputed terms are not limited to the IPSec protocol. Accordingly, we reject the district court's claim construction, vacate the stipulated judgment of noninfringement, and remand.

Second, MPH appeals the district court's determination that the last limitation relating to "the secure connection" in claim 1 of the '581 patent is indefinite. We hold that a skilled artisan would understand the scope of "establishing a secure connection" with reasonable certainty,

and we therefore reverse that determination, vacate the stipulated judgment of invalidity, and remand.

BACKGROUND

I

A

The '949 patent is entitled "Method and System for Sending a Message Through a Secure Connection." U.S. Patent No. 8,346,949 Title.[1] The specification notes the invention is "intended to secure connections in telecommunication networks." *Id.* at col. 1 ll. 7–8. The technical background identifies a problem with the known methods and systems for securing connections between devices: they were "designed for static connections." *Id.* at col. 4 l. 28. It notes that while "IP security protocols (IPSec) provide[] the capability to secure communications between arbitrary hosts," "[s]tandard IPSec does not work well" when one of the connected devices is a mobile terminal that "changes its network point of attachment frequently." *Id.* at col. 1 ll. 42–43, col. 4 ll. 37–50. Thus, "the object of the invention is to forward secure messages in a way that enables changes to be made in the secure connection." *Id.* at col. 6 ll. 21–23.

The summary of the invention explains that "[t]he method and system of the invention enable secure forwarding of a message from a first computer to a second computer," noting that "[p]referably, the first computer processes the formed message using a security protocol." *Id.* at col. 6 ll. 27–46. It then further specifies that "[p]referably, the secure message is formed by making use of the

---

[1] The '949 patent is representative of the issues on appeal that pertain to the '949 patent family, so this opinion will accordingly cite to the claims and specification of the '949 patent.

IPSec protocols, whereby the secure message is formed by using an IPsec connection between the first computer and the intermediate computer." *Id.* at col. 6 ll. 64–67. It goes on to explain that "[a]n essential idea of the invention is to use the standard protocol (IPSec) between the intermediate computer and the second computer and an 'enhanced IPSec protocol' between the first computer and the intermediate computer." *Id.* at col. 7 ll. 29–32. But it then highlights that "[t]here are, however, several other control protocols that could conceivably be used between the first and the intermediate computer," and "[t]he invention is not restricted to the details of the figures and accompanying text, or any existing protocols, such as the currently standardised IPSec." *Id.* at col. 9 ll. 26–33.

Claim 1 of the '949 patent, representative on appeal, recites:

> 1. A method for secure forwarding of a message from a first computer to a second computer using *a secure connection* via an intermediate computer in a telecommunication network, comprising:
>
> the first computer and the second computer negotiating and exchanging keys with one another, by the first and second computer, according to a key exchange protocol to establish the secure connection between the first computer and the second computer via the intermediate computer,
>
> the secure connection having a source address of the first computer as a first end point and a destination address of the second computer as a second end point of the secure connection,
>
> in the first computer, forming *a secure message*, in the first computer, by giving the secure message a first *unique identity* and a first destination address to the intermediate computer,

> sending the secure message, using the secure connection, containing the first unique identity and the first destination address from the first computer to the intermediate computer, the intermediate computer receiving the secure message and performing a translation by using the first unique identity to find a second destination address to the second computer, the intermediate computer substituting the first destination address with the second destination. [sic] address to the second computer,
>
> the intermediate computer substituting, at the intermediate computer, the first unique identity with a second unique identity of the secure connection, and
>
> the intermediate computer forwarding, at the intermediate computer, the secure message with the second destination address and the second unique identity to the second computer in the secure connection.

Id. at col. 22 ll. 6–39 (emphases added to "secure" and "unique identity" terms). Dependent claims 2 and 8, also relevant to the issues on appeal, recite:

> 2. The method of claim 1 wherein the method further comprises forming the secure message by using *an IPSec connection* between the first computer and the second computer.
>
> 8. The method of claim 1 wherein the method further comprises *the IPSec connection* being one or more security associations (SA) and the unique identity being one or more [Security Parameters Index (SPI)] values.

Id. at col. 22 ll. 40–43, col. 23 ll. 1–4 (emphases added to terms relevant to claim differentiation argument).

B

The '581 patent is entitled "Method and Network for Ensuring Secure Forwarding of Messages." U.S. Patent No. 7,937,581 Title. It is an invention "intended to secure mobile connections in telecommunication networks" using IPSec connections. *Id.* at col. 1 ll. 15–17. The technical background highlights that a "problem with standard IP-Sec tunnel end points are [sic] that they are fixed." *Id.* at col. 4 ll. 36–37. The invention purports to solve this problem by allowing "an existing IPSec tunnel endpoint [to] be moved . . . from one point of attachment to another." *Id.* at col. 7 ll. 28–30. **[J.A. 175]**

MPH asserted that Apple infringed claims 6, 7, and 8 of the '581 patent. Each of claims 6, 7, and 8 depend from claim 1 of the '581 patent, which recites:

> 1. A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween, the method comprising:
>
> [1.a] *establishing a secure connection having a first address of the mobile terminal as a first end-point and a gateway address of the security gateway as a second end-point*,
>
> [1.b] the mobile terminal changing from the first address to a second address,
>
> [1.c] while at the second address, the mobile terminal sending a request message to the gateway address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the gateway address of the security gateway,
>
> [1.d] in response to the request message from the mobile terminal, the security gateway changing an

> address definition of the secure connection from the first address to the second address, and
>
> [1.e] *the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway*.

Id. at col. 10 l. 50–col. 11 l. 3 (emphases added to limitations relating to indefiniteness).

II

MPH asserted the '949 patent family against Apple's secure messaging services, and it asserted the '581 patent against Apple's virtual private network offerings. Relevant to this appeal, at claim construction, the parties disputed "unique identity" and the "secure" terms of the '949 patent family and the "establishing a secure connection" term of the '581 patent.

As to the disputed "secure" terms of the '949 patent family, MPH proposed the district court construe the "secure" terms in claim 1 of the '949 patent to include any security protocol. *See MPH Techs. Oy v. Apple, Inc.*, No. 18-cv-05935-TLT, 2024 WL 4603055, at *2–3 (N.D. Cal. Jan. 3, 2024) ("*Claim Construction Order*"). For its part, Apple sought a narrower construction, asserting that the term "secure" required use of the IPSec protocol. *See id.* The district court agreed with Apple, construing "secure" to require use of the IPSec protocol. *Id.* at *2–4. In so ruling, the district court addressed MPH's argument that, under the doctrine of claim differentiation, IPSec should not be read into claim 1 since other asserted claims "expressly refer[red] to IPSec." *Id.* at *3. The district court explained that claim differentiation is not a "hard and fast rule" but rather "a presumption that will be overcome when the specification or prosecution history dictates a contrary construction." *Id.* (quoting *GPNE Corp. v. Apple Inc.*, 830 F.3d

1365, 1371 (Fed. Cir. 2016)). The district court also highlighted various statements in the specification that supported its construction, such as the fact that "the term [IPSec] appears nearly 200 times in the '949 patent[]," *id.*, and the statement that "[a]n essential idea of the invention is to use the standard protocol (IPSec)," *id.* (alteration in original) (quoting '949 patent col. 7 ll. 29–30). Then, relatedly, the district court construed "unique identity" as limited to SPI values, which are specific to the IPSec protocol. *Id.* at *4.

Turning to the '581 patent, the district court held limitation 1.e—"the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway"—indefinite. *Id.* at *9. The district court determined the term "secure connection" in limitation 1.e lacked antecedent basis because "[t]he first 'secure connection' [in limitation 1.a] is between 'a first address of the mobile terminal' and 'a gateway address[,]' [b]ut the second 'secure connection' [in limitation 1.e] is between 'the second address of the mobile terminal' and 'the other terminal.'" *Id.* (internal citation omitted) (quoting '581 patent col. 10 ll. 54–56, col. 11 ll. 1–3). The district court read the claim as lacking "internal consistency" and declined to "re-write claim language to make it internally consistent." *MPH Techs. Oy v. Apple, Inc.*, No. 18-cv-05935-TL, 2024 WL 4603053, at *2–3 (N.D. Cal. Aug. 16, 2024) ("*Amending Order*").

Based on the district court's constructions of "unique identity" and the "secure" terms in the '949 patent family, the parties stipulated to judgment of noninfringement of the asserted claims of the '949 patent family. And based on the district court's holding of indefiniteness of claim 1 of the '581 patent, the parties stipulated to judgment of invalidity of the asserted claims of the '581 patent.

MPH appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(1).

DISCUSSION

MPH challenges the district court's constructions of the "secure" terms (and relatedly the construction of "unique identity") in the '949 patent family. MPH also challenges the district court's determination that the term "establishing a secure connection" in claim 1 of the '581 patent is indefinite. We discuss each in turn.

I

We first turn to MPH's argument that the district court erred in construing the "secure" terms in the '949 patent family as limited to IPSec protocol, an issue we review de novo when the district court's claim construction reasoning involved only intrinsic evidence. *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 808 (Fed. Cir. 2021). In light of the '949 patent's specification, this is a very close issue. After a full review of the relevant intrinsic evidence, however, we are convinced that the construction that most comfortably aligns with the specification and other intrinsic evidence does not limit the "secure" terms to the IPSec protocol.

Starting with the claims themselves, independent claim 1 of the '949 patent merely recites "secure forwarding," "secure connection," and "secure message." *See* '949 patent col. 22 ll. 6–39. On their face, these "secure" terms in claim 1 are broad and not limited to IPSec. And turning to the dependent claims, they are more confirmatory of this broad understanding of the claim language than contradictory. For example, dependent claim 2 recites: "[t]he method of claim 1 wherein the method further comprises forming the secure message by using *an IPSec connection* between the first computer and the second computer." *Id.* at col. 22 ll. 40–43 (emphasis added). While it is true, as Apple points out, that dependent claim 8 of the '949 patent refers to "*the* IPSec connection" and therefore

might favor reading the IPSec protocol into independent claim 1, *id.* at col. 23 l. 2, we agree with MPH that the use of "*the* IPSec connection" in claim 8 is more likely the result of a scrivener error during prosecution, as claim 8 initially depended from claim 2. *See* MPH Techs. Oy's Reply Claim Construction Br., Dkt. Nos. 99-2 at 4–5, 99-3 at 3, 5, *MPH Techs. Oy v. Apple, Inc.*, No. 3:18-cv-05935-TLT (N.D. Cal. Nov. 16, 2023).

We next turn to the specification, which contains many touch points relating to the meaning of "secure." "The claims, of course, do not stand alone." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc). Thus, "[c]laims must be read in view of the specification, of which they are a part." *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc) (citation omitted), *aff'd*, 517 U.S. 370 (1996). Indeed, "the specification 'is always highly relevant to the claim construction analysis'" and "is the single best guide to the meaning of a disputed term." *Phillips*, 415 F.3d at 1315 (citation omitted). Because "the specification necessarily informs the proper construction of the claims," we have recognized that "the specification may reveal an intentional disclaimer, or disavowal, of claim scope by the inventor." *Id.* at 1316; *see also Thorner v. Sony Comput. Ent. Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012). In such circumstances, "the inventor has dictated the correct claim scope, and the inventor's intention, as expressed in the specification, is regarded as dispositive." *Phillips*, 415 F.3d at 1316 (citation omitted). While it is a close question, we ultimately conclude the '949 patent's specification does not compel narrowing "secure" to IPSec specifically.

The specification does not expressly define "secure" as requiring IPSec. It certainly comes close to doing so, but other statements render this possible definition unclear. In favor of a narrow definition, as the district court noted, the specification states that "[a]n essential idea of the invention is to use the standard protocol (IPSec)." *Claim*

Construction Order, 2024 WL 4603055, at *3 (alteration in original) (quoting '949 patent col. 7 ll. 29–30). The specification also explains that "[t]he system of the invention . . . is characterized in that the first and the second computers have means to perform IPSec processing." '949 patent col. 8 ll. 32–36. And the description of the invention states that "an IPSec connection is shared by the first computer and the second computer." *Id.* at col. 10 ll. 11–12.

But while these portions of the specification might in a vacuum suggest that the claimed "secure" terms require IPSec, other parts of the specification make clear that the inventors did not intend to so limit the meaning of "secure." For example, the end of the summary of the invention explains that "[t]he invention is not restricted to the details of the figures and accompanying text, or any existing protocols, *such as the currently standardised IPSec*." *Id.* at col. 9 ll. 31–33 (emphasis added). Similarly, when discussing the use of IPSec in the invention, the specification recognizes that "[t]here are, however, several other control protocols that could conceivably be used between the first and the intermediate computer." *Id.* at col. 9 ll. 26–28. Even further, the specification indicates that "*[p]referably*, the secure message is formed by making use of the IPSec protocols, whereby the secure message is formed by using an IPsec connection between the first computer and the immediate computer." *Id.* at col. 6 ll. 64–67 (emphasis added). And the title, abstract, technical field, and object of the invention make no mention of IPSec, further undermining the conclusion that IPSec is essential to the invention. *Id.* at Title; *id.* at Abstract ("The method and system enable secure forwarding of a message . . . ."); *id.* at col. 1 ll. 7–8 ("The method and system of the invention are intended to secure connections in telecommunication networks."); *id.* at col. 6 ll. 17–18 ("The object of the invention is to develop a method for forwarding secure messages between two computers . . . .").

The district court emphasized the sheer number of times that the specification talks about IPSec and how the invention is intended to work with IPSec protocols. *Claim Construction Order*, 2024 WL 4603055, at *3 ("As Apple noted in the *Markman* hearing, the term ['secure'] appears nearly 200 times in the '949 patent[]. These repeated references to IPSec strongly support Apple's construction." (citing *GPNE*, 830 F.3d at 1368, 1371). We do not dispute that these references support the district court's construction. But once the inventor expressly stated that "[t]he invention is not restricted to the details of the figures and accompanying text, or any existing protocols, such as the currently standardised IPSec," '949 patent col. 9 ll. 31–33, we cannot say that the sheer number of references to IPSec in the specification allows us to ignore the inventor's express language in column 9 and read an IPSec requirement into the broad claim term "secure." Similarly, the district court's reliance on *GPNE* here is misplaced. In *GPNE*, "the specification *repeatedly* and *exclusively* use[d] the[] words ['pager' and 'pager units'] to refer to the devices [(i.e., nodes)] in the patented system," thus leading the district court to construe the claimed "nodes" as "pagers." 830 F.3d at 1370–71 (emphases added). Here, however, the inventor emphasized that the invention was not restricted to IPSec, and that IPSec is "prefer[red]" only. *See, e.g.*, '949 patent col. 6 ll. 64–65; *id.* at col. 9 ll. 31–33.

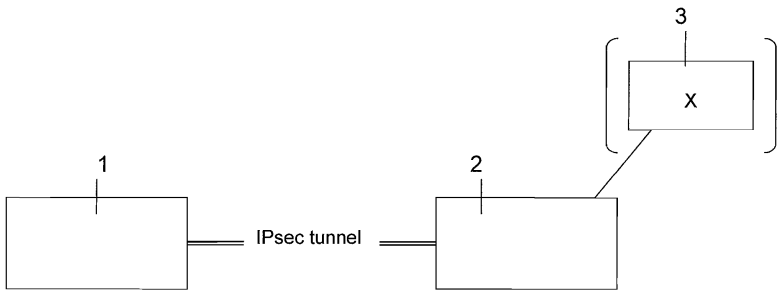
For these reasons, we reject the district court's construction of "secure" as limited to the IPSec protocol. And as we agree with MPH that the district court's construction of the '949 patent family's "unique identity" term as limited to SPI values specific to the IPSec protocol rises and falls with the district court's construction of "secure," we reject the district court's construction of "unique identity" as well. *See* Oral Arg. at 7:05–7:18, https://www.cafc.uscourts.gov/oral-arguments/25-1069_06012026.mp3. We accordingly vacate the judgment of noninfringement of the '949 patent

family and remand for further proceedings consistent with this opinion.

II

We now turn to the district court's determination that limitation 1.e in claim 1 of the '581 patent is indefinite. "[A] patent claim is indefinite if, when 'read in light of the specification delineating the patent, and the prosecution history, the claim fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.'" *BASF Corp. v. Johnson Matthey Inc.*, 875 F.3d 1360, 1365 (Fed. Cir. 2017) (cleaned up) (quoting *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014)). "'Reasonable certainty' does not require 'absolute or mathematical precision.'" *Id.* (citation omitted). "We review a determination of indefiniteness de novo. Determinations about governing legal standards and about intrinsic evidence are reviewed de novo, and any factual findings about extrinsic evidence relevant to the question, such as evidence about knowledge of those skilled in the art, are reviewed for clear error." *Id.* (citations omitted).

In order to assess whether a skilled artisan would understand with reasonable certainty the meaning of "the secure connection" in claim limitation 1.e, it is helpful to walk through the elements of the claim in tandem with the specification. Figure 1 of the '581 patent illustrates one embodiment of the invention:



'581 patent Fig. 1. Boxes 1, 2, and 3 represent computers, where "computer 1 may be a client computer" and "[c]omputer 2 might be a security gateway for a third computer 3." *Id.* at col. 8 ll. 51–56.

Claim 1 begins with its preamble identifying three devices in a telecommunication network: a mobile terminal, another terminal, and a security gateway between the two terminals. *Id.* at col. 10 ll. 50–53. Turning to Figure 1, computer 1 is a mobile terminal, computer 2 is a security gateway, and computer 3 is another terminal. Limitation 1.a recites "*establishing a secure connection* having a first address of the mobile terminal as a first end-point and a gateway address of the security gateway as a second endpoint," which is depicted in Figure 1 as the IPSec tunnel between computers 1 and 2. *Id.* at col. 10 ll. 54–56 (emphasis added). Then limitations 1.b–1.d recite "the mobile terminal changing from the first address to a second address," "the mobile terminal sending a request message to the . . . security gateway to request the security gateway to change the secure connection to be defined between the second address and the gateway address," and the security gateway accordingly changing an address definition. *Id.* at col. 10 ll. 57–67. At this point, computer 1 in Figure 1 has changed addresses, communicated that new address to the security gateway, and the security gateway has changed the secure connection to make computer 1's new address one of its endpoints.

Then, reaching limitation 1.e at issue, the limitation recites "the mobile terminal sending a secure message in *the secure connection* from the second address of the mobile terminal to the other terminal via the security gateway." *Id.* at col. 11 ll. 1–3 (emphasis added). Turning again to Figure 1, this last step is akin to computer 1, having now changed addresses, sending a secure message to computer 3 by sending the message through the IPSec tunnel

between computer 1 and computer 2, i.e., the mobile terminal and the secure gateway, and then the message going from computer 2 to computer 3.

Having walked through the claim step-by-step, we determine "the secure connection" term in limitation 1.e is not indefinite, as it refers to the "secure connection" as established between the mobile terminal and the security gateway. This plain claim language, read in light of the specification, informs a skilled artisan of its scope. The district court held the claim indefinite because it read the "secure connections" as different between limitations 1.a and 1.e. The district court understood "[t]he first 'secure connection' [to be] between 'a first address of the mobile terminal' and 'a gateway address[,]' [b]ut the second 'secure connection' [to be] between 'the second address of the mobile terminal' and 'the other terminal.'" *Claim Construction Order*, 2024 WL 4603055, at *9 (citations omitted). We disagree that a skilled artisan would read the claim in such a way because, as the district court later noted, "if it is not the same secure connection, then the solution that the new invention is supposed to solve is not really solved." *Amending Order*, 2024 WL 4603053, at *5. We similarly disagree with Apple's contention that reading the secure connection in limitation 1.e to be the same as established in limitation 1.a "would just result in a single 'secure connection' that has irreconcilably conflicting sets of endpoints." Appellee's Br. 44. When read in light of the specification, however, the claim informs a skilled artisan that the secure connection remains between the mobile terminal and the security gateway. We accordingly reverse the holding of indefiniteness, vacate the judgment of invalidity of the '581 patent, and remand for further proceedings consistent with this opinion.

CONCLUSION

We have considered Apple's remaining arguments but find them unpersuasive. For the foregoing reasons, we reverse, vacate, and remand.

REVERSED, VACATED, AND REMANDED

COSTS

Costs to Appellant.