United States Court of Appeals for the Federal Circuit

TVIIM, LLC,
Plaintiff-Appellant

v.

MCAFEE, INC.,
Defendant-Appellee

2016-1562

Appeal from the United States District Court for the Northern District of California in No. 3:13-cv-04545-HSG, Judge Haywood S. Gilliam Jr.

Decided: March 21, 2017

JOHN J. SHAEFFER, Fox Rothschild, LLP, Los Angeles, CA, argued for plaintiff-appellant. Also represented by JEFFREY H. GRANT; WILLIAM A. RUDY, Denver, CO.

JOSEPH J. MUELLER, Wilmer Cutler Pickering Hale and Dorr LLP, Boston, MA, argued for defendant-appellee. Also represented by RICHARD WELLS O'NEILL, SARAH B. PETTY; NINA S. TALLON, MICHAEL WOLIN, Washington, DC.

Before PROST, *Chief Judge,* CLEVENGER and REYNA, *Circuit Judges.*

REYNA, *Circuit Judge.*

TVIIM, LLC ("TVIIM") sued McAfee, Inc. ("McAfee") in the United States District Court for the Northern District of California for infringement of U.S. Patent No. 6,889,168 ("'168 patent"). A jury determined that McAfee did not infringe the '168 patent and that the '168 patent was invalid. After the jury verdict, TVIIM filed motions for judgment as a matter of law ("JMOL") and for a new trial. The district court denied both motions, and TVIIM filed this appeal challenging the jury verdict and the district court's denial of its post-verdict motions. We affirm because substantial evidence supports the jury's findings of non-infringement and invalidity under a uniform construction of the relevant claim terms, and the district court did not abuse its discretion in denying a new trial.

BACKGROUND

1. The '168 Patent

The '168 patent is entitled "Method and Apparatus for Assessing the Security of a Computer." It describes "a security system which identifies security vulnerabilities and discrepancies for a computing system." '168 patent, col. 1, ll. 65–67. The '168 patent both identifies potential security threats to a computer and, under certain conditions, recommends action to a user to stop the threat.

Four claims of the '168 patent are relevant to this appeal. Independent claim 1 recites:

> A security system for a computer apparatus, wherein said computer apparatus includes a processor and system memory, said security system comprising:

> at least one security module which under direction from the processor accesses and analyzes selected portions of the computer apparatus to identify vulnerabilities;
>
> at least one utility module which under the direction from the processor, performs *various utility functions* with regards to the computer apparatus *in response to* the identified vulnerabilities; and
>
> a security system memory which contains security information for performing the analysis of the computer apparatus.

'168 patent, col. 10, l. 65 to col. 11, l. 10 (disputed terms emphasized).

Dependent claim 7 recites:

> The security system of claim 1 wherein the security modules include at least one of . . . an integrity checking module which analyzes files in the system memory to identify system vulnerabilities;
>
> a network checking module which analyzes the computer apparatus to identify vulnerabilities created *as a result of* the computer apparatus connecting with a data network; and
>
> a password checking module which analyzes passwords for users of the computer apparatus to identify vulnerabilities.

Id. col. 11, ll. 25–46 (disputed term emphasized).

Dependent claim 9 recites: "The security system of claim 7 wherein the system memory comprises a list of known vulnerabilities which may be employed by the integrity checking module." *Id.* col. 11, ll. 62–64.

Finally, independent claim 11 recites:

> A method of providing a security assessment for a computer system which includes a system memory, comprising the steps of:
>
> providing a security subsystem in the computer system such that functionality of the security subsystem is directed through a processor for the computer system, wherein the security performs steps comprising:
>
> identifying a configuration of the system;
>
> accessing the system memory and performing at least one procedure to provide a security assessment for at least one aspect of the computer system;
>
> *as a result of* any vulnerabilities discovered in the assessment, identifying corrective measures to be taken with regards to the computer system;
>
> *reporting the discovered vulnerability* and the identified corrective measures; and
>
> upon receiving an appropriate command, initiating the corrective measures.

Id. col. 12, ll. 1–18 (disputed terms emphasized).

2. McAfee

McAfee developed "Program Updates" for Microsoft Windows users to protect software programs against new security threats. Program Updates detects and installs updates for numerous non-Windows programs such as Apple iTunes and Adobe Acrobat. To do so, it scans a user's computer to determine whether any of the non-Windows programs are installed. If it detects such a program, Program Updates makes two determinations: (1) whether the National Vulnerability Database ("NVD") lists any vulnerabilities in the currently installed version

of that program; and (2) whether an update is available. If an update is available, Program Updates will install the update.

Prior to installing an update, Program Updates does not provide users with a detailed report of security threats; rather, it tells the user whether an update is "Critical" or merely "Recommended." J.A. 2044–46, 3338. If an update is available, Program Updates will install the available update whether or not the NVD lists any known vulnerabilities. By contrast, if no software update is available, Program Updates will not take action even if it detects a vulnerability. Without an available update, Program Updates will not provide users with any information about a detected vulnerability. J.A. 2047–48. To summarize, the presence of a known vulnerability is irrelevant to whether Program Updates installs an update.

3. Prior Art

At trial, McAfee argued that two prior art references anticipated the '168 patent and, in the alternative, that their combination would have rendered the '168 patent obvious.

The first reference, HostGUARD, is a software program developed by several named inventors of the '168 patent. HostGUARD first detects computer security threats and then reports them to the user. J.A. 1090, 3796–97. These detailed reports include file names and locations, the particular nature of the vulnerability, and steps the user can take to combat the threat. HostGUARD requires the user to decide whether to take corrective action. Thus, the user (not HostGUARD itself) takes any desired corrective action. J.A. 3796.

The second reference, System Security Scanner ("S3"), is a "security assessment tool" that "evaluates system vulnerabilities from the inside." J.A. 3799. S3 allows a

user to select which specific vulnerabilities to assess and then provides a "detailed description" of detected vulnerabilities to the user. J.A. 3816, 3801, 3836. For example, it offers a "long description" report that identifies "bugs" that create exploitable weaknesses in the system. J.A. 2610–11; *see also* J.A. 2293 (testimony that S3 provides users with reports on "specific vulnerabilities found on specific computers"). S3 does not fix vulnerabilities itself; rather, it requires a user to open a new window and take corrective action.

4. District Court Proceedings

TVIIM sued McAfee in 2013, alleging that Program Updates infringed the '168 patent. McAfee counterclaimed for declarations of non-infringement, invalidity, and inequitable conduct.

McAfee moved for summary judgment that HostGUARD anticipated the asserted claims of the '168 patent. In its motion, McAfee argued that all claim terms should be given their plain and ordinary meaning. In its opposition, TVIIM asked the district court to construe only one term: "vulnerability." The district court denied McAfee's motion on anticipation because material issues of fact remained for trial. The district court also ruled that "vulnerability" should "have its plain and ordinary meaning and is not limited in scope to 'pre-existing' security problems or vulnerabilities." J.A. 567. The court then asked for supplemental briefing on the plain and ordinary meaning of "vulnerability." The parties agreed that a "vulnerability" is an "exploitable weakness in a computer system." J.A. 633. The court adopted that construction and asked if it needed to construe any other terms. Both parties said no further construction was necessary.

The case went to trial, and the jury returned a verdict that: (1) McAfee did not infringe the '168 patent; (2) the '168 patent was invalid; and (3) TVIIM did not obtain the

'168 patent through inequitable conduct. The jury's general verdict of invalidity did not distinguish between obviousness and anticipation. The inequitable conduct issue is not subject to this appeal.

TVIIM filed motions for JMOL and a new trial, arguing that the jury had rendered an inconsistent verdict. According to TVIIM, the jury could not have arrived at both a non-infringement and invalidity determination using a single construction of three claim terms: "as a result of/in response to"; "various utility functions"; and "reporting the discovered vulnerabilities." TVIIM concedes that it did not seek construction of any of these terms before or during trial. Opening Br. at 70.

The district court denied TVIIM's motions. It found that the jury's verdict was not inconsistent because substantial evidence supported both a non-infringement and invalidity verdict under a single construction of all three claim terms. J.A. 6–8.

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

STANDARD OF REVIEW

We review denials of motions for JMOL and motions for new trial under the law of the regional circuit—here, the Ninth Circuit. *InTouch Techs., Inc. v. VGO Commc'ns, Inc.*, 751 F.3d 1327, 1338 (Fed. Cir. 2014). The Ninth Circuit reviews denials of JMOL *de novo*. *Harper v. City of Los Angeles*, 533 F.3d 1010, 1021 (9th Cir. 2008). In the Ninth Circuit, the district court grants JMOL when "the evidence, construed in the light most favorable to the nonmoving party, permits only one reasonable conclusion, and that conclusion is contrary to the jury's verdict." *Id.* (quotation marks and citation omitted). A district court must uphold a jury's verdict "if it is supported by substantial evidence, which is evidence adequate to support the jury's conclusion, even if it is also possible to draw a

contrary conclusion." *Id.* (quotation marks and citation omitted). Substantial evidence is "such relevant evidence as a reasonable mind might accept as adequate to support a conclusion." *Theme Promotions, Inc. v. News Am. Mktg. FSI*, 546 F.3d 991, 1000 (9th Cir. 2008) (quotation marks and citation omitted). Whether a claim is anticipated is a question of fact, *MPHJ Tech. Invs., LLC v. Ricoh Ams. Corp.*, 847 F.3d 1363, 1378 (Fed. Cir. 2017), as is the question of infringement, *Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 448 F.3d 1324, 1332 (Fed. Cir. 2006).

The Ninth Circuit reviews the denial of a motion for new trial for abuse of discretion. *Incalza v. Fendi N. Am., Inc.*, 479 F.3d 1005, 1013 (9th Cir. 2007). It reverses the denial only if the record lacks any evidence supporting the verdict or if the district court makes a mistake of law. *Molski v. M.J. Cable, Inc.*, 481 F.3d 724, 729 (9th Cir. 2007).

DISCUSSION

1. Non-Infringement And Invalidity

Claim terms must be construed the same way for the purpose of determining invalidity and infringement. *Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1330 (Fed. Cir. 2003). A district court's determination that a claim term has a "'plain and ordinary meaning' may be inadequate when [the claim] term has more than one 'ordinary meaning.'" *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1361 (Fed. Cir. 2008).

We first address TVIIM's argument that the jury rendered an inconsistent verdict of infringement and invalidity because the claim terms "as a result of/in response to," "various utility functions," and "reporting the discovered vulnerabilities" have more than one ordinary meaning. We note that TVIIM did not seek construction of any of the three terms at trial. It never presented multiple

ordinary meanings of the three terms or showed that they are open to varying interpretations. We are not persuaded that any of the three terms has multiple ordinary meanings, and we discern no error in the district court submitting them to the jury without specific instruction. TVIIM argues that it is not seeking a new claim construction of any terms on appeal. To be sure, it has waived any new construction. "[A] party may not introduce new claim construction arguments on appeal or alter the scope of the claim construction positions it took below. Moreover, litigants waive their right to present new claim construction disputes if they are raised for the first time after trial." *Conoco, Inc. v. Energy & Envtl. Int'l, L.C.*, 460 F.3d 1349, 1358–59 (Fed. Cir. 2006) (citations omitted). Thus, TVIIM "cannot be allowed to create a new claim construction dispute following the close of the jury trial." *Broadcom Corp. v. Qualcomm Inc.*, 543 F.3d 683, 694 (Fed. Cir. 2008).

We next address whether substantial evidence supports the jury's verdict of non-infringement based on using the same construction it used for its invalidity verdict. *See Harper*, 533 F.3d at 1021. We conclude that the jury verdict is supported by substantial evidence.

A. "As A Result Of/In Response To"

There was no dispute at trial that the term "as a result of/in response to" requires a causal relationship between corrective action and the discovered vulnerability. McAfee's expert Dr. Rubin testified that Program Updates installs software updates regardless of whether a vulnerability exists and that the only requirement for update installation is the availability of an update. J.A. 2444 ("The only determining factor whether Program Updates will update software is if there's an update available."). In other words, the presence of a vulnerability is irrelevant to whether Program Updates installs a software update. As a result, with Program Updates

there is no causal relationship between corrective action and the discovered vulnerability. We find Dr. Rubin's testimony on this point to be substantial evidence supporting the jury's non-infringement verdict.

We also find that substantial evidence supports the jury verdict of invalidity based on anticipation. Dr. Rubin testified that the prior art anticipated the '168 patent by initiating corrective action in response to a detected vulnerability. *See, e.g.*, J.A. 2476 (explaining how HostGUARD discloses the "as a result of any vulnerabilities" limitation of claim 11); J.A. 2494 (concluding that S3 anticipates claim 1). TVIIM insists that the jury failed to distinguish "all" vulnerabilities from "potential" vulnerabilities. But TVIIM failed to clarify its position during claim construction. Moreover, the jury was free to credit Dr. Rubin's testimony that HostGUARD and S3 anticipate claims 1 and 11, even in the face of opposing arguments from TVIIM. We thus find Dr. Rubin's testimony to be substantial evidence supporting the jury's invalidity determination.

B. "Various Utility Functions"

TVIIM and McAfee presented competing expert testimony on infringement. TVIIM's expert Dr. Garuba testified that Program Updates satisfies the "various utility functions" term by performing four functions: identifying the threat, accessing the update, downloading the update, and installing the update. J.A. 2123–24. McAfee's expert Dr. Rubin disagreed and testified that Program Updates performs only one function—downloading software updates via multiple steps. J.A. 2445 ("[T]he only thing that [Program Updates] does is it updates the programs."); *see also* J.A. 2454–55. Given the conflicting expert testimony, we find that a reasonable mind might accept Dr. Rubin's testimony over Dr. Garuba's. Thus, substantial evidence supports the jury's verdict of non-infringement. *See Versata Software,*

Inc. v. SAP Am., Inc., 717 F.3d 1255, 1263 (Fed. Cir. 2013) (affirming jury award as supported by substantial evidence despite competing expert testimony).

Dr. Rubin's testimony also supports the jury's invalidity verdict for anticipation. He explained how S3 performs "different utility functions." J.A. 2493. TVIIM expert Eric Knight also testified that HostGUARD "corrected, at a minimum, ownership and permission," *i.e.*, different functions. J.A. 2620. Thus, the testimony that the prior art and '168 patent both perform multiple functions constitutes substantial evidence in support of the jury's verdict of invalidity.

Given the testimony at trial, we find that a uniform construction of "various utility functions" would allow the jury to arrive at verdicts of non-infringement and invalidity, as both are supported by substantial evidence.

C. "Reporting The Discovered Vulnerabilities"

At trial, TVIIM argued that Program Updates infringes "reporting the discovered vulnerabilities" by providing a "risk rating" to users prior to installation, *i.e.*, whether a particular update is "critical" or simply "recommended." When pressed about what vulnerability information is provided to users by Program Updates, TVIIM's expert Dr. Yu responded, "[n]othing more than just a risk rating." J.A. 2046. In other words, although Program Updates reports the risk level to the user, it does not report any specific information on vulnerabilities. Dr. Rubin testified that such a risk rating does not constitute "reporting the discovered vulnerabilities," because Program Updates does not report "something like a [Common Vulnerabilities and Exposures] number or a specific description of the vulnerability." J.A. 2455. Program Updates will not report any detected vulnerability to a user if no update is available. We find this testimony to be substantial evidence supporting the jury's non-infringement verdict.

Regarding invalidity for anticipation, the record demonstrates that unlike Program Updates, HostGUARD and S3 provide users with specific reports on detected vulnerabilities. *See, e.g.*, J.A. 2478 (Dr. Rubin) ("So here we see the actual vulnerability is described" [in S3]); J.A. 3796 (HostGUARD brochure describing "reports [that] are written in plain English and are formatted to effectively communicate the results of the security assessment"); J.A. 3841–78 (examples of "Vulnerability Descriptions" in S3).[1] Program Updates, by contrast, does not provide any detailed vulnerability descriptions. J.A. 2002, 2046, 2455. Given this evidence presented, we find that the jury verdict of invalidity is supported by substantial evidence.

As with the other two terms, TVIIM has not persuaded us that a jury could not arrive at a non-infringement and invalidity verdict based on a single construction of "reporting the discovered vulnerabilities." Because substantial evidence supports the jury's verdicts, the district court did not abuse its discretion by denying TVIIM's motion for a new trial.

2. Any Potential Error In Claim Construction Was Harmless

On appeal, TVIIM concedes that substantial evidence supports the jury's finding for *either* non-infringement or invalidity but argues it does not support *both*. Opening Br. at 73 ("[A]ny single ordinary meaning construction could support either infringement or invalidity.") (emphasis omitted); *see also* J.A. 2638 (TVIIM's counsel stating at

---

[1] TVIIM asserts that the jury and district court improperly construed "vulnerabilities" to include "discrepancies." But the district court specifically found that "the intrinsic evidence does not clearly exclude 'discrepancies' from the scope of the claim term 'vulnerability.'" J.A. 634. TVIIM did not appeal that construction.

trial, "I think there's questions of fact with respect to infringement.").

Thus, by TVIIM's own admission, the jury's invalidity determination could be proper under "any single ordinary meaning construction." Opening Br. 73. This concession is determinative, because even if we were to find an inconsistent verdict, substantial evidence under "any" construction supports the jury's verdict of invalidity. Consequently, any potential error by the jury regarding non-infringement was harmless. *Cf. Senju Pharm. Co. v. Lupin Ltd.*, 780 F.3d 1337, 1353 (Fed. Cir. 2015) (affirming the district court's invalidity finding and therefore not reaching non-infringement arguments); *MobileMedia Ideas LLC v. Apple Inc.*, 780 F.3d 1159, 1173 (Fed. Cir. 2015) (holding that because the patent was invalid, the court "need not reach Apple's argument that its accused iPhones do not infringe").

CONCLUSION

The jury's findings of non-infringement and invalidity under a single construction of all three disputed claim terms are supported by substantial evidence. Even if error occurred in the jury's verdict of infringement, we agree with McAfee that substantial evidence supports the jury's invalidity finding. This renders any error harmless. In light of these findings, we hold that the district court's denial of TVIIM's motion for JMOL is supported by substantial evidence, and that the district court did not abuse its discretion in denying TVIIM's motion for a new trial. We therefore *affirm*.

AFFIRMED

COSTS

No costs.