United States Court of Appeals for the Federal Circuit

00-1373, -1374

HILGRAEVE CORPORATION,

Plaintiff-Appellant,

v.

SYMANTEC CORPORATION,

Defendant-Cross Appellant.

Ernie L. Brooks, Brooks & Kushman P.C., of Southfield, Michigan, argued for plaintiff-appellant. With him on the brief were Thomas A. Lewry, Robert C.J.Tuttle, John E. Nemazi, and Frank A. Angileri.

Martin C. Fliesler, Fliesler Dubb Meyer & Lovejoy LLP, of San Francisco, California, argued for defendant-cross appellant. With him on the brief were Burt Magen, and Sarah Barone Schwartz. Of counsel was Dennis J. Levasseur, Bodman Longley & Dahling LLP, of Detroit, Michigan.

Appealed from: United States District Court for the Eastern District
                   of Michigan

Judge Paul V. Gadola

United States Court of Appeals for the Federal Circuit

00-1373, -1374

HILGRAEVE CORPORATION,

Plaintiff-Appellant,

v.

SYMANTEC CORPORATION,

Defendant-Cross Appellant.

_____

DECIDED: September 18, 2001
_____

Before RADER, Circuit Judge, PLAGER, Senior Circuit Judge, and DYK, Circuit Judge.

DYK, Circuit Judge.

Hilgraeve Corp. ("Hilgraeve") appeals from the decision of the United States District Court for the Eastern District of Michigan granting the motion of Symantec Corp. ("Symantec") for summary judgment of non-infringement for U.S. Patent No. 5,319,776 ("'776 patent"). Hilgraeve Corp. v. Symantec Corp., 90 F. Supp. 2d 850 (E.D. Mich. 2000). Symantec cross-appeals the district court's grant of summary judgment for Hilgraeve that Symantec is not licensed to use the invention claimed in the '776 patent. Hilgraeve Corp. v. Symantec Corp., Civ. Action No. 97-40370 (E.D. Mich. Jun. 28, 1999) ("License Defense Order").

We vacate the district court's grant of summary judgment of non-infringement of the '776 patent and generally affirm the district court's grant of summary judgment that Symantec did not license the '776 patent. We find that questions of material fact exist as

to whether the limitations of the '776 patent claims are found in the methods performed by the accused products, and that Hilgraeve did not transfer any rights to practice the '776 patent.

BACKGROUND

Hilgraeve filed suit against Symantec in the Eastern District of Michigan for infringement of the '776 patent on September 15, 1997. On the same day, Hilgraeve filed a separate suit against McAfee Associates, Inc. for infringement of the '776 patent, also in the Eastern District of Michigan. The cases were not consolidated. In the McAfee case, the district court's grant of summary judgment of non-infringement, Hilgraeve Corp. v. McAfee Associates, Inc., 70 F. Supp. 2d 738 (E.D. Mich. 1999) ("McAfee I"), was vacated and remanded by this court because, under the agreed claim construction, questions of material fact existed about the operation of the accused device, 224 F.3d 1349, 55 USPQ2d 1656 (Fed. Cir. 2000) ("McAfee II").

The '776 patent relates to computer virus detection software. The software scans a digital data file for viruses as the file is transferred to a storage medium. If the software detects a virus prior to storing the file, it automatically blocks storage of the file. The software may be used, for example, to scan a file for viruses as the file is transferred from a floppy disk to a hard disk of a computer system, or as the file is transferred over the Internet from one computer system to a storage medium of another computer system.

The '776 patent contains 20 claims. Independent claims 1 and 18, which are at issue on this appeal, read as follows:

> 1.   In a system for transferring digital data for storage in a computer storage medium, a method of screening the data as it is being transferred and automatically inhibiting the storage of screened data containing at least one predefined sequence, comprising the steps of:

causing a quantity of digital data resident on a source storage medium to be transferred to a computer system having a destination storage medium;

receiving and screening the transferred digital data <u>prior to storage on the destination storage medium</u> to determine if at least one of a plurality of predefined sequences are present in the digital data received; and

in response to said screening step:

(a)   automatically causing the screened digital data to be stored on said destination storage medium if none of the plurality of predefined sequences are present, and

(b)   automatically inhibiting the screened digital data from being stored on said destination storage medium if at least one predefined sequence is present.

18.   A method of preventing the spread of computer viruses to a computer having a storage medium, comprising the steps of:

<u>simultaneously searching</u> for a plurality of virus signatures, each of which comprising an identifiable digital sequence, <u>while said computer is receiving a stream of digital data for storage on said storage medium</u>;

providing an indication of the detection of a virus from said searching step; and

automatically inhibiting the storage of said digital stream on said storage medium if any of said virus signatures have been detected.

'776 patent, col. 17, ll. 9-29 and col. 18, ll. 45-57 (emphases added to pertinent terms).

Because these claims require the inhibition of "storage," the district court was required to construe the meaning of the word "storage" in the patent. The district court construed "storage" as occurring "when the incoming digital data is sufficiently present on the destination storage medium so that any viruses contained in the data can spread and infect the computer system." <u>Hilgraeve</u>, 90 F. Supp. 2d at 857.

Hilgraeve contended that several Symantec products, including pcANYWHERE™ and Norton Antivirus™ ("NAV"), infringe the '776 patent under this claim construction. In other words, Hilgraeve alleged that the accused products screen incoming digital data for viruses during transfer and before "storage" on the destination storage medium. In contrast, Symantec contended that its products do not infringe because they screen for viruses only after the data have been "stored" on the destination storage medium. Thus,

the critical issue was whether the accused products screen for viruses before or after the data become sufficiently present on the storage medium so that viruses contained in the data could spread and infect the computer system.

To resolve this issue on summary judgment the district court relied on testimony of Symantec's expert witness about how the accused products operate and on statements made by Hilgraeve and its expert that it agreed with the overview offered by Symantec's expert about how the accused products operate. Hilgraeve, 90 F. Supp. 2d at 858-59. Upon accepting Symantec's view of how the products operate, the district court found that the accused products "first allow the incoming digital data to be stored as a whole on the destination storage medium before it is scanned. Virus screening is performed only after the incoming digital data has been fully transferred and stored." Id. at 859. The district court held that "[b]ecause there is no dispute about how the accused products operate, there is no genuine issue as to any material fact concerning whether Defendant's accused products literally infringe the '776 Patent" and granted summary judgment for Symantec. Id.

Before the district court, Symantec also asserted the affirmative defense to Hilgraeve's infringement claim that it had acquired a license to use the patent under a complex series of transactions involving Delrina Corp. and its subsidiaries. On June 30, 1993, Delrina Corp., Delrina (Delaware) (a subsidiary of Delrina Corp.), and Hilgraeve executed a Technology Transfer Agreement under which Delrina Corp. paid Hilgraeve $1.45 million, and Hilgraeve transferred certain rights to its software, allegedly including the technology at issue in this suit, to Delrina (Delaware). The Technology Transfer Agreement states that it is governed by the laws of the Province of Ontario, Canada. On the same day, Delrina (Canada) (also a subsidiary of Delrina Corp.) and Delrina (Delaware) entered into a Software Development and Cost Sharing Agreement (the "SDCS Agreement") to govern the shared development of software by the parties. In July 1995, Symantec acquired

Delrina Corp. On March 30, 1996, Delrina (Canada) licensed its intellectual property to Symantec. On March 2, 1999, Delrina (Delaware) entered into an agreement with Symantec to directly transfer rights to the technology transferred by Hilgraeve to Delrina (Delaware) on June 30, 1993.

The district court granted Hilgraeve's motion for summary judgment that Symantec did not have a license to the '776 patent prior to March 2, 1999, because Symantec had failed to establish that Delrina (Delaware) transferred any rights to the '776 patent to Delrina (Canada) or Delrina Corp., and Symantec therefore failed to show that it acquired any rights to the '776 patent through the 1995 acquisition of Delrina Corp. License Defense Order, slip op. at *14. As to events after March 2, 1999, the district court denied both Hilgraeve's and Symantec's motions for summary judgment regarding Symantec's licensing defense, finding that the March 2, 1999, agreement raised a general issue of material fact as to whether Symantec had acquired a license to the '776 patent through the March 2, 1999 agreement. Id. After granting Symantec's motion for summary judgment of non-infringement, the district court denied all other pending motions in the case without prejudice, and dismissed the case. Hilgraeve, 90 F. Supp. 2d at 859.

DISCUSSION

I. Jurisdiction and Standard of Review

We have jurisdiction over this appeal pursuant to 28 U.S.C. § 1295(a)(1). Summary judgment is properly granted when "there is no genuine issue as to any material fact and . . . the moving party is entitled to a judgment as a matter of law." Fed. R. Civ. P. 56(c); Chiuminatta Concrete Concepts, Inc. v. Cardinal Indus., Inc., 145 F.3d 1303, 1307, 46 USPQ2d 1752, 1755 (Fed. Cir. 1998). We review a district court's grant of a motion for summary judgment without deference. Ethicon Endo-Surgery, Inc. v. United States Surgical Corp., 149 F.3d 1309, 1315, 47 USPQ2d 1272, 1275 (Fed. Cir. 1998).

A patent infringement analysis requires two steps. Gentry Gallery, Inc. v. Berkline Corp., 134 F.3d 1473, 1476, 45 USPQ2d 1498, 1500 (Fed. Cir. 1998). "First, the claim must be properly construed to determine its scope and meaning. Second, the claim as properly construed must be compared to the accused device or process." Id. (quoting Carroll Touch, Inc. v. Electro Mech. Sys., Inc., 15 F.3d 1573, 1576, 27 USPQ2d 1836, 1839 (Fed. Cir. 1993)). Claim construction is a matter of law that is reviewed without deference. Cybor Corp. v. FAS Techs., Inc., 138 F.3d 1448, 1456, 46 USPQ2d 1169, 1174 (Fed. Cir. 1998) (en banc). Determination of infringement, whether literal or under the doctrine of equivalents, is a question of fact. Bai v. L & L Wings, Inc., 160 F.3d 1350, 1353, 48 USPQ2d 1674, 1676 (Fed. Cir. 1998). "Thus, summary judgment of non-infringement can only be granted if, after viewing the alleged facts in the light most favorable to the non-movant, there is no genuine issue whether the accused device is encompassed by the claims." Pitney Bowes, Inc. v. Hewlett-Packard Co., 182 F.3d 1298, 1304, 51 USPQ2d 1161, 1165 (Fed. Cir. 1999).

We review the construction of a license agreement without deference and interpret the licensing agreement under the law governing the agreement, here Ontario law. See Studiengesellschaft Kohle, m.b.H. v. Hercules, Inc., 105 F.3d 629, 632, 41 USPQ2d 1518, 1521 (Fed. Cir. 1997) (citing Cyrix Corp. v. Intel Corp., 77 F.3d 1381, 1384, 37 USPQ2d 1884, 1887 (Fed. Cir. 1996)).

II. Claim Construction Issues

As noted above, this is our second case involving the '776 patent. In McAfee II, we accepted the claim construction of "storage" urged by both parties and adopted by the district court in McAfee I. That claim construction differs slightly from the claim construction adopted below in the district court in this case in that the McAfee II claim construction views "storage" as occurring "when the incoming digital data is sufficiently present on the

destination storage medium, <u>and accessible by the operating system or other programs</u>, so that any viruses contained in the data can spread and infect the computer system." <u>McAfee II</u>, 224 F.3d at 1351 (emphasis added to differing language).

Symantec argues that "storage" should not be construed to occur when data become "accessible by the operating system or other programs," <u>Hilgraeve</u>, 90 F. Supp. 2d at 857, or when "any viruses contained in the data can spread and infect the computer system," but that "storage" should be construed to occur when the data become physically present (i.e., magnetically recorded) on the storage medium.

We need not decide here whether our claim construction in <u>McAfee II</u> is binding on us in this case as a matter of <u>stare</u> <u>decisis</u>. Our decision in <u>McAfee II</u> was precedential, but it merely adopted the district court's claim construction in <u>McAfee I</u> based on the parties' agreement that the district court's claim construction was correct. We have independently considered the issues of claim construction and conclude that the construction of "storage" in <u>McAfee II</u> is indeed correct.

The '776 patent distinguishes prior art virus scanning programs because they "do not automatically prevent the virus from being stored on the medium in the first place, hence they cannot totally prevent the virus from attacking or spreading." '776 patent, col. 1, ll. 51-54. Thus, "storage" of the virus is identified with the virus's ability to spread and infect the computer system. A virus may not spread or infect the computer system, however, unless it is accessed by the operating system or other programs. Given this, we agree with the <u>McAfee II</u> court that "storage" occurs "when the incoming digital data [are] sufficiently present on the destination storage medium and accessible by the operating system or

other programs so that any viruses contained in the data can spread and infect the computer system."[1] McAfee II, 224 F.3d at 1351.

III. Infringement

Symantec contends that even under our claim construction it does not infringe. Hilgraeve argues that questions of material fact remain regarding the operation of the accused devices and hence infringement.[2] We conclude here that the conflicting affidavits of the parties' experts leave material fact questions unanswered, just as we held in a somewhat similar context in McAfee II.

The district court based its summary judgment of non-infringement on the testimony of Symantec's expert, Dr. Melvin, who opined on the operation of the accused products, and on statements made by Hilgraeve and its expert, Dr. Geske, agreeing with portions of Dr. Melvin's testimony. The experts, however, did not in fact agree.

The experts described the operation of the accused products in different ways. Symantec's expert, Dr. Melvin, described the operation of NAV as occurring in a sequence of steps. In this sequence, first (step one) a file is transferred for storage onto the destination storage medium. This transfer includes opening a new file on the storage medium and recording incoming data into the new file. Second (step two), the application

---

[1]   The parties also dispute whether "destination storage medium" as used in claim 1 and "storage medium" as used in claim 18 mean the ultimate destination of the digital data or whether the terms may be construed to include an intermediate storage medium. In accordance with the definition of "storage" we have adopted, we conclude that "storage medium" refers to any storage medium of the computer system, if the data, when stored on the medium, are accessible to the operating system or other programs, such that viruses in the data can spread and infect the computer system.

[2]   While the parties, and the district court's decision, speak of the accused devices as infringing, more properly the allegation is that the operation of the devices directly infringes the method claims at issue, or that the sale of the devices induces customers to infringe the method claims.

causing the transfer makes a request to the operating system to close the file containing the transferred data. Third (step three), the operating system closes the file. Fourth (step four), after the file is closed, the Symantec product invokes the NAV Scan Engine to test the file for the presence of a virus. Symantec's expert alleged that after the third step and before the fourth step, the file is recorded on the storage medium and accessible to the operating system and other programs – and therefore "stored," and that since this occurs before the file is scanned for viruses, Symantec's products do not infringe. Hilgraeve's expert, Dr. Geske, stated that although he agreed with Dr. Melvin's "overview" of how the accused products operate, in his opinion there were critical points in Dr. Melvin's analysis that did not correspond with the behavior of the NAV as it executes. Critically, Dr. Geske interpreted the testimony of Mr. Cohen, the Chief Architect of the Symantec accused products, to mean that the accused products impose a barrier in the computer system's file system which prevents all programs and the operating system from accessing the transferred file until it is processed and screened for viruses. Thus, Dr. Geske disputed that the file becomes accessible to the operating system and other programs between steps three and four.

Symantec's expert sought to prove that a file becomes accessible to the operating system or other programs before it is scanned for viruses by the NAV Scan Engine by running four tests. Hilgraeve's expert asserted that these tests do not prove that Symantec's products do not infringe, and that even if they showed that the products do not infringe under the test circumstances, they do not prove non-infringement under normal operating conditions.

We agree that tests of an accused device under unusual conditions are not necessarily relevant to an infringement analysis. For example, in determining whether a product claim is infringed, we have held that an accused device may be found to infringe if

it is reasonably capable of satisfying the claim limitations, even though it may also be capable of non-infringing modes of operation. See Intel Corp. v. United States Int'l Trade Comm'n, 946 F.2d 821, 832, 20 USPQ2d 1161, 1171 (Fed. Cir. 1991); Key Pharms., Inc. v. Hercon Labs. Corp., 981 F. Supp. 299, 310 (D. Del. 1997), aff'd, 161 F.3d 709, 48 USPQ2d 1911 (Fed. Cir. 1998); Huck Mfg. Co. v. Textron, Inc., 187 USPQ 388, 408 (E.D. Mich. 1975) ("The fact that a device may be used in a manner so as not to infringe the patent is not a defense to a claim of infringement against a manufacturer of the device if it is also reasonably capable of a use that infringes the patent."); cf. High Tech Med. Instrumentation, Inc. v. New Image Indus., Inc., 49 F.3d 1551, 1556, 33 USPQ2d 2005, 2009 (Fed. Cir. 1995) (finding that an accused device does not infringe if it does not infringe in its normal configuration, even if it may be altered into an infringing configuration under unusual circumstances). So too the sale of a device may induce infringement of a method claim, even if the accused device is capable of non-infringing modes of operation in unusual circumstances.

In the first test, Symantec's expert downloaded an infected file from a web page on the Internet to a storage disk of a computer running NAV and the Windows 95™ operating system. After the file arrived at the computer, but before the NAV was able to scan and delete the file, he shut off power to the computer. When he turned the computer on again he was able to access the file with a utility program of Windows 95. In the second test, Dr. Melvin also downloaded an infected file from a web page to a storage disk of a computer running NAV, but he restarted the computer instead of shutting off its power, prior to scanning by NAV. When the computer restarted, he was able to access the file. Symantec alleges that these two tests show that the file is stored on the computer's storage medium prior to scanning. Even if that is true as a factual matter under the circumstances of the

tests, the tests are not probative of infringement during normal operation of the accused products. Because the '776 patent claims require "automatically inhibiting" the storage of the virus, as we said in McAfee II when considering similar tests, "a test disabling the automatic capabilities of [the accused product] is not probative of whether [the accused product] may infringe in the automatic mode." McAfee II, 224 F.3d at 1354.

In Dr. Melvin's third test, he downloaded an infected file to a computer running both NAV and McAfee's anti-virus screening program, VirusScan™. VirusScan intercepted and examined the file before NAV screened it for viruses, which according to Dr. Melvin, showed that the file was accessible by other programs prior to screening by NAV. While this third test may demonstrate that the infected file is accessible to VirusScan before it is screened by NAV, it is not clear from this test that the virus can spread and infect the computer system before it is screened by NAV, especially since both NAV and VirusScan are intended to prevent the spread of viruses. Moreover, as with the first two tests, whether or not the accused products infringe when operated in conjunction with another anti-virus product – perhaps an unusually redundant mode of operation – does not answer the question whether they infringe while operating alone.

In his fourth test, Dr. Melvin loaded into memory NAV and a special program for intercepting a particular file while the file is being downloaded and redirecting the file to the computer's storage medium. When Dr. Melvin then downloaded the particular file, which contained a virus, it was intercepted and redirected to the storage medium by the special program before it could be screened by NAV for viruses. That this test may prove that the functionality of the accused products can be defeated to avoid infringement does not prove non-infringement of the products under normal operating conditions.

Thus, we find the tests inconclusive on the issue of infringement. Because the record shows the existence of genuine issues of material fact concerning the interaction of

the accused devices with the operation system and other programs, the district court erred in granting summary judgment of non-infringement.

IV.   Symantec's Licensing Defense

Symantec urges that even if we vacate the district court's grant of summary judgment of non-infringement, the judgment can be affirmed on an alternative ground, namely that Symantec was licensed to practice the patent. We cannot agree.

The district court held that Symantec had no license defense for the period prior to March 2, 1999, because the purported transfer of patent rights from Delrina (Delaware) to Delrina (Canada) under the June 30, 1993 SDCS agreement was ineffective. While the district court appears to have been correct, we believe that there is a more fundamental defect in Symantec's license defense argument – Delrina (Delaware) itself never acquired a transferable license to practice the '776 patent, and Delrina (Delaware) therefore could not sub-license the '776 patent either before March 2, 1999, or thereafter.

Unless the '776 patent was licensed under the June 30, 1993 Agreement, Symantec agrees that it could not acquire a license. Symantec also admits that there is no express language in the June 30, 1993 Technology Transfer Agreement licensing or transferring rights to the '776 patent or any other Hilgraeve patent. Instead, Symantec points to language in the paragraph 2.1 of the Agreement providing that "HILGRAEVE sells, conveys, assigns and transfers to DELRINA DELAWARE and to HILGRAEVE, as joint tenants and not as tenants in common, all copyright rights in the Software," and that Hilgraeve acknowledged in paragraph 9.1 that as part of the transfer "HILGRAEVE has also agreed to transfer the necessary know-how and technical expertise to DELRINA DELAWARE with respect to the Software." On the basis of this language, Symantec urges us to find that:

> 'Software' is more than source code and object code. . . . When read in conjunction with the . . . 'know-how' and 'technical expertise' transferred to Delrina (Delaware), Delrina (Delaware) essentially acquired Hilgraeve's entire knowledge base with respect to [Hilgraeve's] products. Since the Software included in-transit anti-virus features, Delrina acquired Hilgraeve's knowledge base with respect to those in-transit anti-virus features and could use that knowledge base as it pleased."

In summary, Symantec urges us to find that "the Technology Transfer Agreement covered the technology in this case, which is allegedly covered by the '776 Patent."

Whatever the definition of "knowledge base" proposed by Symantec, we cannot conclude that rights to the '776 patent were transferred by the Technology Transfer Agreement. Under Ontario law, "effect must first be given to the intention of the parties, to be gathered from the words they have used . . . ." Consol. Bathurst Exp. Ltd. v. Mut. Boiler & Mach. Ins. Co., 1 S.C.R 888, 888 (Can. 1980). When the language of a contract is clear and unambiguous, only the contract is considered for interpretation, not extrinsic evidence. Indian Molybdenum v. The King, 3 D.L.R. 497, 502 (Can. 1951). Here, the contract provided for Hilgraeve to transfer "all copyright rights in the Software," but failed to mention the transfer of patent rights. From the terms of the contract we cannot conclude that the parties intended to transfer any patent rights. Symantec relies on Allan v. Bushnell T.V. Co., Ltd., 1 D.L.R. (3d) 534, 539 (Ont. High Ct. 1968) for the proposition that "unexpressed term[s] [are implied] to implement [the] parties' presumed intention." Allan, however, stated that

> the presumption is against the adding to contracts of terms which the parties have not expressed. The general presumption is that the parties have expressed every material term . . . . But . . . there may be cases where obviously some term must be implied if the intention of the parties is not to be defeated, some term of which it can be predicated that 'it goes without saying', some term not expressed but necessary to give to the transaction such business efficacy as the parties must have intended.

Id. Allan was a case involving a contract between a broadcasting company and a news service in which the unexpressed term which was implied in the contract was that the news

to be supplied to the company by the service had to be "accurate." Here, we cannot say

(and it does not "go without saying") that where the contract provided for the transfer of

copyrights in the software, but failed to mention the transfer of patent rights, that we must

imply such a term to the contract. The contract has a business efficacy without adding this

unexpressed term to it.

Moreover, in the subparagraph immediately following the paragraph 2.1 pertaining

to the transfer of copyrights, the contract refers to other intellectual property rights. In

paragraph 2.2, the parties agreed that Hilgraeve "shall not assert against DELRINA

DELAWARE, any other intellectual property right, including patent rights, it has or may have

in the future, with respect to the production, copying, licensing of the Software, or the

exercise by DELRINA DELAWARE of any rights transferred hereunder." Since the

contract specifically mentions patent rights in paragraph 2.2, we cannot say that the

omission of mention of patent rights in paragraph 2.1, which transferred rights to copyrights

in the Software, was accidental or that the transfer of patent rights is implicit anywhere the

contract. Cf. State Contracting & Eng'g Corp. v. Florida, 258 F.3d 1329, 59 USPQ2d

1498 (Fed. Cir. 2001) (applying Florida law to construe an agreement).

Symantec also contends that the covenant not to sue for patent infringement in

paragraph 2.2 is equivalent to a freely transferable license to the patent. This court has

stated that "licenses are considered as nothing more than a promise by the licensor not to

sue the licensee." Jim Arnold Corp. v. Hydrotech Sys., Inc., 109 F.3d 1567, 1577, 42

USPQ2d 1119, 1127 (Fed. Cir. 1997). The covenant not to sue in paragraph 2.2 does not

grant a transferable license to the patent.

CONCLUSION

Therefore, we vacate the district court's grant of summary judgment of non-

infringement, generally affirm the district court's grant of summary judgment that Symantec

did not license the '776 patent prior (but without limiting our holding to the period before

March 2, 1999), and remand for further proceedings consistent with this opinion.

<u>AFFIRMED-IN-PART, VACATED-IN-PART, AND REMANDED.</u>

COSTS

No costs.