United States District Court,
E.D. Michigan, Southern Division.

HILGRAEVE CORPORATION,
Plaintiff.
v.
McAFEE ASSOCIATES, INC,
Defendant.

June 10, 1999.

Owner of patent for computer virus detection program sued competitor for infringement. On defendant's motion for summary judgment, the District Court, Edmunds, J., held that: (1) patent was not literally infringed, and (2) plaintiff was estopped from asserting that patent was infringed under doctrine of equivalents.

Motion granted.

5,319,776. Construed and Ruled Not infringed.

Ernie L. Brooks, Robert C.J. Tuttle, John E. Nemazi, Thomas A. Lewry, Brooks & Kushman P.C., Southfield, MI, for plaintiff.

Michael Barclay, David L. Larson, Colleen Bal, Behrooz Shariati, Craig Gordon, Wilson Sonsini Goodrich & Rosati, Palo Alto, CA, R. Terrance Rader, Eric Dobrusin, Rader, Fishman & Grauer PLLC, Bloomfield Hills, MI, for defendant.

MEMORANDUM OPINION AND ORDER GRANTING DEFENDANT'S MOTION FOR SUMMARY JUDGMENT OF NON-INFRINGEMENT

EDMUNDS**, District Judge.**

This is a patent infringement action brought by Plaintiff Hilgraeve Corporation ("Hilgraeve") against Defendant Network Associates, Inc. ("Network"), formerly known as McAfee Associates, Inc. FN1 Now before the Court is Defendant's motion seeking summary judgment of non-infringement of U.S. Patent No. 5,319,776 ("the '776 patent") owned by Hilgraeve which describes an improvement to a personal computer data transfer program that scans for computer viruses during the data transfer and prior to storage on a destination storage medium so as to prevent computer viruses from infecting the computer in the first instance. Hilgraeve accuses Network of infringing Claims 1, 2, 6, and 18 of the '776 patent both literally and under the doctrine of equivalents by using, marketing, and selling the accused product, VirusScan. FN2

FN1. Defendant has also filed a counterclaim against Hilgraeve seeking a declaratory judgment declaring

that the patent is invalid and that there is no infringement.

FN2. The DOS, Windows 95, Windows 98 and Windows NT versions of VirusScan are at issue. For purposes of infringement, the parties' experts agree that all of these versions of VirusScan work the same way. *See* Geske Dep. at 56; Belgard Decl. at para. 11.

As with all patent infringement claims, the Court must apply a two-step analysis. First, the Court must construe the meaning and scope of the disputed claim language in the '776 patent. Next, the Court must compare the properly construed claims of the '776 patent with the accused product and determine whether infringement has occurred either literally or under the doctrine of equivalents. The first step involves a question of law for the Court and thus is particularly well-suited for summary judgment. The second step presents a question of fact, however, summary judgment is appropriate here as well if the Court finds there are no triable issues of fact on the question whether the Defendant's accused product, VirusScan, infringed the '776 patent either literally or under the doctrine of equivalents.

This Court, after construing the relevant claim language in the '776 patent, concludes that Defendant Network's motion for summary judgment of non-infringement should be GRANTED. Hilgraeve has not met its burden by establishing that there are triable issues of material fact concerning whether Network infringed the '776 patent either literally or under the doctrine of equivalents.

I. Facts

The '776 Patent issued on June 7, 1994 and is entitled "In Transit Detection of Computer Virus with Safeguard". The '776 patent acknowledges that it is not the first invention to address the spread of computer viruses and refers to prior art; i.e., virus detection and scanning devices by IBM and John Rex. *See* '776 Patent at Col. 1, Lines 37-44; Col. 4, Lines 48-58. The '776 specification explains that the invention was developed to address a "major shortcoming" of the prior art; i.e., the failure to automatically prevent a virus from attacking or spreading in the first place rather than merely detecting and then curing a virus. Thus, to distinguish it from the prior art, the '776 patent screens incoming digital data for viruses "on the fly" while the data is being transferred and before it is stored on the destination storage medium, and then automatically inhibits virus-infected data from being stored. Id. at Col. 1, Lines 55-62.

This matter is before the Court on Defendant Network's motion for summary judgment of non-infringement. Hilgraeve contends that Defendant's accused product, VirusScan, infringes independent Claims 1 and 18, as well as dependent Claims 2 and 6, of the '776 patent because it similarly screens incoming digital data for viruses during transfer and *before* "storage" on the destination storage medium. Defendant, on the other hand, asserts that the accused product screens only after all the incoming digital data has been transferred and "stored" on the destination storage medium. Thus, the critical issues presented here are: (1) what order the sequential steps in Claims 1 and 18 are to be performed; (2) how "storage", as used in Claims 1 and 18, is to be construed; and (3) when the accused product screens for viruses.

II. Summary Judgment Standard

Summary judgment is appropriate only when there is no genuine issue as to any material fact and the moving party is entitled to judgment as a matter of law. Fed.R. Civ. P. 56(c). The central inquiry is "whether the evidence presents a sufficient disagreement to require submission to a jury or whether it is so one-sided

that one party must prevail as a matter of law." Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 251-52, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). After adequate time for discovery and upon motion, Rule 56(c) mandates summary judgment against a party who fails to establish the existence of an element essential to that party's case and on which that party bears the burden of proof at trial. Celotex Corp. v. Catrett, 477 U.S. 317, 322, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986).

The movant has an initial burden of showing "the absence of a genuine issue of material fact." Celotex, 477 U.S. 317, 323, 106 S.Ct. 2548, 91 L.Ed.2d 265. Once the movant meets this burden, the non-movant must come forward with specific facts showing that there is a genuine issue for trial. Matsushita Electric Industrial Co., Ltd. v. Zenith Radio Corp., 475 U.S. 574, 587, 106 S.Ct. 1348, 89 L.Ed.2d 538 (1986).

To demonstrate a genuine issue, the non-movant must present sufficient evidence upon which a jury could reasonably find for the non-movant; a "scintilla of evidence" is insufficient. Liberty Lobby, 477 U.S. at 252, 106 S.Ct. 2505. The inquiry is whether the evidence presented is such that a jury applying the relevant evidentiary standard could "reasonably find for either the plaintiff or the defendant." Liberty Lobby, 477 U.S. at 255, 106 S.Ct. 2505.

III. Analysis

[1] This patent infringement case requires a two-step analysis: (1) construction of the meaning and scope of the '776 patent; and (2) comparison of the properly construed claims of the '776 patent with the Defendant's accused product and a determination whether infringement has occurred.

[2] Summary judgment is appropriate in this patent case. Claim construction, being the first step in a patent infringement case, is a matter of law to be decided exclusively by the court. Markman v. Westview Instruments, Inc., 517 U.S. 370, 383, 116 S.Ct. 1384, 1393, 134 L.Ed.2d 577 (1996). Accordingly, matters of claim construction are particularly well-suited for summary judgment. Markman v. Westview Instruments, Inc., 52 F.3d 967, 970-71 (Fed.Cir.1995) (en banc).

The second step in this patent case presents a question of fact. Summary judgment is also appropriate here if the court finds there are no triable issues of fact on the question whether Defendant's accused product, VirusScan, infringes the '776 patent either literally or under the doctrine of equivalents. Wolverine World Wide, Inc. v. Nike, Inc., 38 F.3d 1192, 1200 (Fed.Cir.1994); Johnston v. IVAC Corp., 885 F.2d 1574, 1576-77 (Fed.Cir.1989).

A. Claim Construction

1. General Principles

[3] The Supreme Court has recently clarified that "[t]he construction of a patent, including terms of art within its claims is exclusively within the province of the court." Markman v. Westview Instruments, Inc., 517 U.S. 370, 372, 116 S.Ct. 1384, 1387, 134 L.Ed.2d 577 (1996). When construing disputed claim language, the court must first consider three sources of intrinsic evidence; the patent's claims, the specification, and, if in evidence, the prosecution history. Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed.Cir.1996) (citing Markman, 52 F.3d at 979).

[4] [5] First, the court considers the language in the challenged claim. The words "are generally given their ordinary and customary meaning," however, "a patentee may choose to be his own lexicographer and use

terms in a manner other than their ordinary meaning, as long as the special definition of the term is clearly stated in the patent specification or file history." Vitronics Corp., 90 F.3d at 1582. The court may also look to other claims in the patent for guidance, but is not permitted to read narrow claim limitations into broad claims. SRI Int'l v. Matsushita Elec. Corp. of Am., 775 F.2d 1107, 1122 (Fed.Cir.1985) (en banc).

[6] Next, the court examines the patent's specification. This contains a written description of the invention which must be clear and complete enough to enable those of ordinary skill in the art to make and use it. "For claim construction purposes, the description may act as a sort of dictionary, which explains the invention and may define terms used in the claims." Markman, 52 F.3d at 979. The specification is always highly relevant to the claim construction analysis, and "[c]laims must be read in view of the specification, of which they are a part." *Id*. Usually, the patent's specification is the single best guide to the meaning of a disputed term. Vitronics, 90 F.3d at 1582. The Federal Circuit Court of Appeals has observed that although the examples set forth in the specification do not necessarily limit the scope of a claim, Transmatic, Inc. v. Gulton Indus., Inc., 53 F.3d 1270, 1277 (Fed.Cir.1995), a claim construction that excludes the preferred embodiment set out in the specification is not likely to be correct, Hoechst Celanese Corp. v. BP Chemicals Ltd., 78 F.3d 1575, 1581 (Fed.Cir.1996), *cert. denied,* 519 U.S. 911, 117 S.Ct. 275, 136 L.Ed.2d 198 (1996).

[7] [8] [9] Finally, the court considers the patent's prosecution history, if it is placed in evidence, and looks for representations by the patentee as to the meaning of words used in the patent claim. Markman, 52 F.3d at 980. "The prosecution history limits the interpretation of claim terms so as to exclude any interpretation that was disclaimed during prosecution." Southwall Technologies, Inc. v. Cardinal IG Co., 54 F.3d 1570, 1576 (Fed.Cir.1995), *cert. denied,* 516 U.S. 987, 116 S.Ct. 515, 133 L.Ed.2d 424 (1995) (citations omitted). The court may also consider the prior art cited in the history for clues as to what the disputed claim does not cover. Vitronics, 90 F.3d at 1583 (citations omitted). The prosecution history, however, cannot be used to "enlarge, diminish, or vary the limitations in the claim." Markman, 52 F.3d at 980 (internal quotes and citations omitted).

If the meaning of a claim is clear after considering these three sources of intrinsic evidence, the court does not consider any extrinsic evidence. Vitronics, 90 F.3d at 1583. The patent's claims, specification and prosecution history are given priority because they "constitute the public record of the patentee's claim, a record on which the public is entitled to rely." *Id*. As the *Vitronics* court explained:

In most situations, an analysis of the intrinsic evidence alone will resolve any ambiguity in a disputed claim term. In such circumstances, it is improper to rely on extrinsic evidence. In those cases where the public record unambiguously describes the scope of the patented invention, reliance on any extrinsic evidence is improper. The claims, specification, and file history, rather than extrinsic evidence, constitute the public record of the patentee's claim, a record on which the public is entitled to rely. In other words, competitors are entitled to review the public record, apply the established rules of claim construction, ascertain the scope of the patentee's claimed invention and, thus, design around the claimed invention. Allowing the public record to be altered or changed by extrinsic evidence introduced at trial, such as expert testimony, would make this right meaningless. The same holds true whether it is the patentee or the alleged infringer who seeks to alter the scope of the claims.

Id. (internal citations and quotes omitted).

[10] Nonetheless, the court may consider extrinsic evidence if it determines this evidence would assist it in ascertaining the meaning and scope of a disputed claim. *Id*. As the *Markman* court explained:

Extrinsic evidence consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises. This evidence may be helpful to explain scientific principles, the meaning of technical terms, and terms of art that appear in the patent and prosecution history. Extrinsic evidence may demonstrate the state of the prior art at the time of the invention. It is useful to show what was then old, to distinguish what was new, and to aid the court in the construction of the patent.

52 F.3d at 980 (internal quotes and citations omitted).

The *Markman* court emphasized that, although the court may consider conflicting evidence, claim construction remains a question of law for the court.

Through this process of construing claims by, among other things, using certain extrinsic evidence that the court finds helpful and rejecting other evidence as unhelpful, and resolving disputes *en route* to pronouncing the meaning of claim language as a matter of law based on the patent documents themselves, the court is *not* crediting certain evidence over other evidence or making factual evidentiary findings. Rather, the court is looking to the extrinsic evidence to assist in its construction of the written document, a task it is required to perform. The district court's claim construction, enlightened by such extrinsicevidence as may be helpful, is still based upon the patent and prosecution history. It is therefore still construction, and is a matter of law.... (Emphasis in original).

Id. at 981. The court further observed that testimony of the patentee and his attorney "on the proper construction of the claims" was entitled to "no deference" because it "amounts to no more than legal opinion-[and] it is precisely the process of construction that the court must undertake." *Id*. In sum, "the court has complete discretion to adopt the expert legal opinions as its own, to find guidance from it, or to ignore it entirely, or even to exclude it", but it cannot rely on extrinsic evidence "to change the meaning of the claims." *Id*.

Here, the court finds it unnecessary to consult extrinsic evidence to accomplish its task of claim construction. Consideration of the '776 patent's claims, specification, drawings, and that portion of its prosecution history in evidence suffices to allow the Court to properly construe the disputed claim language.

2. Construction of Disputed Claim Language

The '776 patent discloses an improvement to a personal computer data transfer program. The claimed advance over the prior art is the invention's ability to prevent computer viruses from entering and infecting a computer system in the first instance by transferring digital data virus-free to a destination storage medium. FN3 The '776 patent discloses a method for scanning for computer viruses *during* the transfer of incoming digital data and *before* storage on the destination storage medium, and, in response to the screening step, for automatically inhibiting virus-infected data from being stored and automatically storing virus-free data. FN4 At issue here are Claims 1, 2, 6, and 18 of the '776 patent. Claims 1 and 18 are independent claims, whereas Claims 2 and 6 are dependent claims. FN5 Accordingly, a finding that Network's accused product does not infringe either of the independent claims will dispose of Plaintiff's case. *See* Desper Products, Inc. v. QSound Labs, Inc., 157 F.3d 1325, 1338 n. 5 (Fed.Cir.1998); London v. Carson Pirie Scott & Co., 946 F.2d 1534, 1539 (Fed.Cir.1991).

FN3. The '776 patent specification asserts that the claimed invention solves the problems of the prior art "by performing an in transit detection of computer viruses ... which allows multiple virus signatures to be simultaneously tested for.... 'on the fly' " and by inhibiting "the virus from entering the computer in the first place." '776 patent, Col. 1, Lines 45-62.

FN4. The '776 patent specification discloses that "[i]f any one or more of the [virus] signatures are detected, the file into which the incoming bitstream *would have been stored* is closed or aborted so the virus does not take up residency on the storage medium." Id. at Col. 1, Lines 65-69, Col. 2, Line 1 (emphasis added). Thus, the inventive advance of the '776 patent is its capability to scan for viruses during the transfer and before the incoming digital data is stored on the destination storage medium thus preventing viruses from infecting this computer system in the first instance.

FN5. Hilgraeve does not dispute Defendant's contention that Claims 2 and 6 are dependent upon Claim 1.

The parties' dispute focuses on the meaning and scope of language contained in Claims 1 and 18. FN6 To resolve their dispute, the Court must construe these claims, ascertain the specific order in which the disclosed sequential steps are to be performed, and define the "storage" and "prior to storage" terms as used in Claims 1 and 18.

FN6. This dispute centers around the meaning and scope of the language highlighted below.

Claim 1 reads 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 *prior to storage on the destination storage medium* 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*.

'776 patent, Col. 17, Lines 9-29 (Emphasis added).

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

simultaneously searching for a plurality of virus signatures, each of which comprising an identifiable digital sequence, *while said computer is receiving a stream of digital data for storage* on said storage medium; 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. 28, Lines 45-57 (Emphasis added).
The parties agree that these are method claims which disclose sequential steps of operation and that the steps must be performed in a particular order. *See* Plf.'s Resp. at 4, n. 5. The disclosed order is as follows: (1) incoming digital data is first screened for viruses *while* the digital data is being received or is "in transit" and *before* storage on the destination storage medium, and (2) in response to the screening step, virus-infected digital data is automatically inhibited from being stored whereas virus-free data is automatically stored.

[11] Because Claims 1 and 18 require that virus screening be completed during transfer and *before* storage on the destination medium, the Court must construe the meaning of the word "storage" as used in those claims. The parties' essentially agree on the meaning of storage. FN7 This Court construes "storage" as follows: storage occurs when the incoming digital data is 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. The intrinsic evidence; i.e., the '776 patent claim language, specification, drawings, and prosecution history, supports the Court's construction of Claims 1 and 18. To the extent Hilgraeve argues "prior to storage" must be construed from the ordinary user's perspective, there is nothing in the intrinsic evidence to support this construction. There is no support for an argument that "prior to storage" is to be construed from the subjective point of view of the user. To construe the language in such a fashion would improperly broaden the scope of Claims 1 and 18, would effectively eliminate each of the sequential steps which Hilgraeve admits are present and must be performed in a particular order, and would effectively remove from the '776 invention an important prophylactic and distinguishing feature; i.e., the screening for viruses while digital data is in transit and "prior to storage on the destination storage medium."

FN7. Hilgraeve urges the Court to recognize that storage occurs "when the incoming file or data is sufficiently present on the destination disk medium so any viruses can spread and infect the system." Plf.'s Resp. at (i), 4, 7. Defendant, similarly urges the Court to recognize that storage occurs "when the digital data is written to, and present on, the destination medium, and accessible by the operating system or other programs, so any viruses contained in the data can spread elsewhere in the computer system." Def.'s Reply at 2.

As taught in Claim 1, the incoming digital data is first screened for viruses while the digital data is being received and "prior to storage on the destination storage medium," '776 patent, Col. 17, Lines 17-18; and

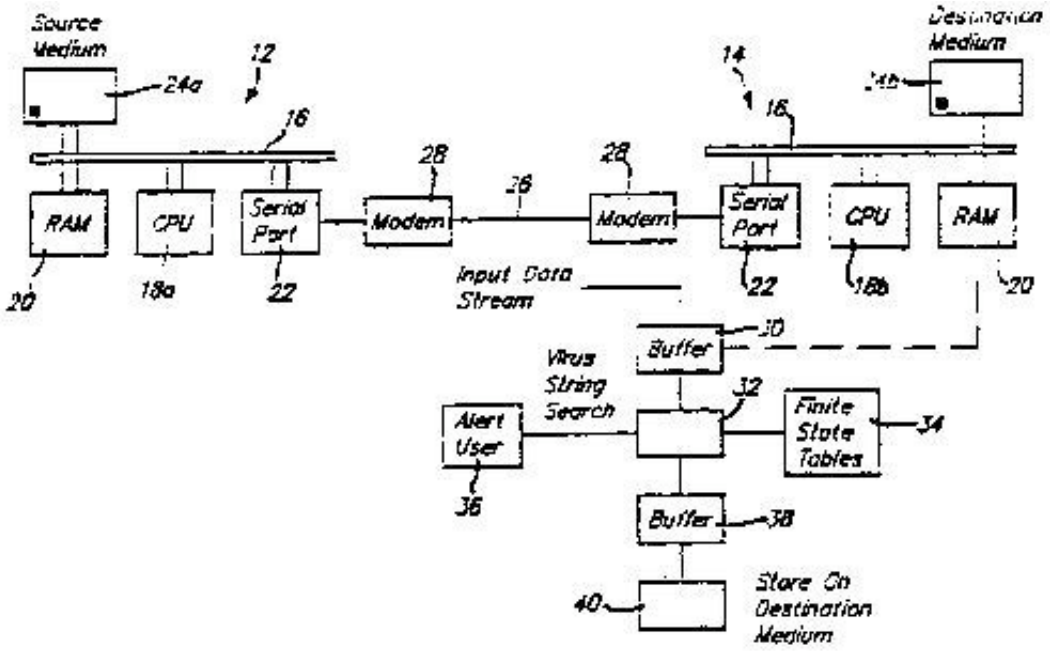
then, "in response to said screening step", the "screened digital data" is either automatically "stored on the destination storage medium" if a virus is not detected or automatically inhibited from "being stored on said destination storage medium" if one is detected during the screening step. Id. at Col. 17, Lines 22-29.

Claim 18 likewise discloses a method claim with similar sequential steps. Specifically, the '776 invention first "simultaneously" searches for "a plurality of virus signatures" "while said computer is receiving a stream of digital data for storage". Id. at Col. 18, Lines 48-52. Second, if a virus is detected "from said searching step", an indicator is provided showing that a virus has been detected. Id. at Col. 18, Lines 53-54. Finally, if any viruses have been detected, the '776 invention "automatically inhibit[s] the storage of said digital stream on said storage medium." Id. at Col. 18, Lines 55-57. Accordingly, both Claims 1 and 18 teach that the virus screening or searching is done while the digital data is being received or transferred and before it is stored on the destination storage medium.

The '776 patent specification, including the embodiments described and illustrated therein, corroborate this claim construction. They disclose that Claims 1 and 18's sequential steps are to be performed as follows. First is the transmission step. Here, digital data is caused to be transmitted from one computer storage medium to another. Second is the processing or screening step. Here, incoming digital data is received and screened "in transit" for computer viruses and before storage on the destination storage medium. Third is the inhibiting step. Here, in response to the screening performed in step (2), virus-free digital data is automatically stored on the destination storage medium and virus-infected digital data is automatically inhibited from being stored on the destination storage medium. Id. at Col. 2, Lines 17-34.

The processing or screening step (step 2) is pivotal here and best understood when examined along with the embodiments illustrated in Figures 1 and 2 of the '776 patent. These illustrations provide diagrams of "a data communications system in which data transmitted over a telecommunications link between two computer systems is tested in transit using the invention," Id. at Col. 2, Lines 59-64, "an overall flow diagram of the in transit detection process", Id., and "a file copying mechanism using the invention to test the data transmission in transit". Id. at Col. 2, Lines 65-66. Below is a drawing from the '776 patent diagraming the invention using a telecommunications link between two computer systems.

***747**



As explained in the specification, the incoming data stream "is placed by CPU [central processing unit] **18b** into an input buffer **30** comprising a portion of RAM **20**." Id. at Col. 3, Lines 64-67. Unlike the prior art, the invention's error and virus screening process is performed at step **32**. Thus, in the '776 patent, incoming data is screened before it reaches buffer **38** which is the place "[m]ost computer operating systems buffer data being written to the storage medium." Id. at Col. 4, Lines 46-47; Col. 4, Lines 24-26. The '776 specification discloses that:

Typically, the input buffer **30** is configured to hold one or more blocks of data which have been transmitted over communication line **26** by the computer system **12**. A cyclic redundancy check (CRC) or other error checks are performed on the data in input buffer **30**. If a transmission error is detected, many communications protocols cause the block containing the error to be resent.

When the incoming data stream has been error checked and the input buffer becomes filled, in a conventional data communications system, the data in buffer 30 would be stored on the destination medium **24b**. *The present invention intervenes at this point by subjecting the buffered data to a character by character virus signature string search analysis* depicted at **32**.

Id. at Col. 3, Lines 67-68; Col. 4, Lines 1-13 (emphasis added).

In the preferred embodiment, the " 'string search routine' disclosed in the '776 patent is performed at step **32** and is implemented using a finite state machine based on preloaded finite state tables **34**", Id. at Col. 4, Line 1, which tests each character as it enters looking for a match to a virus signature. Id. at Col. 5, Lines 2-21. Blocks of data are transmitted, screened for viruses, and stored in the designed receive file if virus-free, and then the next block of data is transferred and the process is repeated. Id. at Col. 6, Lines 22-68; Col. 7, Lines 1-14. If, in response to the "in transit" screening step, a virus is detected in a block of data being transmitted, "the transfer will of course be cancelled prematurely." Id. at Col. 6, Lines 14-16. Also, "[i]f a virus was detected *during the transfer,* " the data in the file can be purged or deleted by overwriting. Id. at

Col. 6, Lines 24-31 (emphasis added). "For added safety, any portion of the file already written can be overwritten with 1's or 0's to ensure that none of the virus remains." Id. at Col.2, Lines 1-3.

The patent specification further teaches that, if "a virus signature is detected" during the incoming virus screening step at **32**, "the user is alerted at step **36**, typically by an appropriate warning message displayed on the computer system monitor," Id. at Col. 4, Lines 16-19, and "any storage of the data onto the destination medium **24b** is terminated, with the receiving file being deallocated or marked to be overwritten", Id. at Col. 4, Lines 19-22. However, "[i]f no virus signature is detected, the data is stored on destination medium **24b** as depicted at **38** and **40**." Id. at Col. 4, Lines 23-24.

Accordingly, only virus-free digital data passes through to buffer **38** on the way to storage on the destination storage medium **40**. Virus-infected digital data is automatically inhibited from storage. Virus-infected data will cause the transfer to be interrupted midstream, will trigger a flag which notifies the user that a virus signature has been detected in a block of incoming data, and will notify the user that it must decide whether the transfer should be prematurely terminated. If the transfer is terminated, then virus-infected data is stopped before it reaches buffer **38** and is never stored on the destination storage medium **40**. Moreover, blocks of virus-free data which have passed through and have been stored on the destination storage medium can be purged or deleted by overwriting as an added anti-virus safety.

In sum, the '776 patent-in-suit operates as follows: The invention receives a quantity of data in buffer **30** during the transfer of digital data from a source medium to a destination medium. The invention scans the data in buffer **30** for the presence of a predefined digital sequence, such as a virus signature, before storing the data on the destination medium **40**. If a predefined sequence is found in the digital data, the data in buffer **30** is inhibited from being stored on the destination storage medium. If a predefined sequence is not found in the digital data, the virus-free data is transferred from buffer **30** to a file on the destination storage medium where it is then stored. If a predefined sequence is subsequently detected in an incoming block of digital data, the previously stored, virus-free block of digital data can be purged or overwritten as an added anti-virus safety.

The patent's prosecution history likewise supports the Court's construction of the order within which the sequential steps of Claims 1 and 18 are to be performed as well as the Court's construction of "storage." The Court is mindful that "[t]he prosecution history limits the interpretation of claim terms so as to exclude any interpretation that was disclaimed during prosecution." Southwall Technologies, 54 F.3d at 1576. The Court is also mindful that it may consider the prior art cited in the prosecution history for clues as to what the disputed claim does not cover. *See* Vitronics, 90 F.3d at 1583. The Court cannot, however, use the prosecution history to "enlarge, diminish, or vary the limitations in the claim." Markman, 52 F.3d at 980 (internal quotes and citations omitted). The prosecution history below reveals that, in the screening step, the "prior to storage on the destination storage medium" requirement was added to distinguish the '776 invention from the prior art.

As originally filed, Claim 1 disclosed a method for identifying and inhibiting the storage of data containing at least one predefined sequence or virus signature. Unlike the final amended version of the screening step of Claim 1, there was no sequential limitation that virus screening be performed before storage on the destination storage medium. *See* Def's Ex. 11, 4/19/90 Patent Application at 25.

In the first Office Action, dated October 24, 1991, the examiner rejected all the claims as unpatentable under 35 U.S.C. s. 103 for obviousness in view of an existing patent to Nagata et al. (No. 4,979,210). *See* Def's

Ex. 12, 10/24/91 Patent and Trademark Office Correspondence at 3. All claims were likewise rejected under 35 U.S.C. s. 112, second paragraph, "as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention." *Id*. at 8.

The applicants responded by submitting the following November 7, 1991 amendment: FN8

FN8. Consistent with Patent Office practice, deletions are shown in brackets and additions are underlined. *See* 37 C.F.R. s. 1.121.

1. (Amended) In a [data transfer] system for [receiving a transmission of] *transferring* digital data for storage in a computer storage medium, a method of [identifying and] inhibiting the storage of data containing at least one predefined sequence, comprising *the steps of:*
causing a [transmission] *quantity* of digital data resident on a source storage medium to be transmitted to a computer system having a destination storage medium;

receiving and processing the [transmission] *transmitted digital data* to determine if at least one *of a plurality of* predefined [sequence is] *sequences are* present in the [transmission] *digital data received;* and

in response to said processing *step:*

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

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

Def.'s Ex. 13, 11/7/91 Amendment at 2, 4-5. Claim 18 was also added as a new claim. *Id*. at 4. Applicants also argued that the examiner's rejection for obviousness under s. 103 was inappropriate because, unlike the prior art, the '776 invention scanned for viruses in transit and thus prevented viruses from infecting the computer system in the first instance:

While virus scanning programs exist, they do not provide an effective answer to the problem, as they scan files which have already been stored. In other words, a computer virus has the opportunity to attack, mutate and otherwise spread before the file containing the virus is scanned. In contrast, the present invention provides a real and complete solution to this problem by providing a way to check for virus signatures while a *digital* data file is *in transit,* so that the receiving computer is protected in the first instance from ever being infected.

Importantly, the present invention has the capability to *simultaneously* test for a *multitude* of virus signatures *while* the digital data is being received.... The present invention also has the capability to respond to the detection of a virus by not only preventing the copying of the complete file, but also to mark the file for erasure, and even write over any portion of the file that was copied at the option of the operator.

Id. at 6-7 (emphasis in original).

The examiner did not agree with the applicants' arguments, and, in the next Office Action, dated February

13, 1992, continued the prior rejection and made it final. *See* Def.'s Ex. 14, 2/13/92 Patent and Trademark Office Corresp. at 4. It was explained that the rejection of all claims under s. 103 was in view of prior art; i.e., IBM's Virus Scanning Program and John Rex's "Simultaneous Searching for Multiple Strings", and was based on the fact that the combination of these prior art references disclosed all the features of claims 1 and 18 and others in the '776 patent application. As to the only missing feature; i.e., causing or inhibiting the storage of data on the destination medium, the examiner considered it obvious to inhibit a detected computer virus from being stored on the computer system. *Id*. at 5-6.

An interview was conducted on June 19, 1992 without any agreement being reached as to patentability. *See* Def.'s Ex. 15, 6/19/92 Patent and Trademark Office Memo. Thereafter, in August 1992, applicants submitted a proposed amendment, together with a declaration of one of the inventors, Matthew Gray. The proposed amendment was not entered because the examiner found that it raised new issues. *See* Def.'s Ex. 16, 8/13/92 Amendment; Ex. 17, 8/12/92 Decl. of Matthew H. Gray. Subsequently, applicants filed a continuation application, refiled the amendment, and the claims were allowed. By this action, Claims 1 and 18 were amended to read as follows: FN9

FN9. Added language is underlined.

1. (Twice Amended) 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 [transmitted] *transferred* to a computer system having a destination storage medium;

receiving and [processing] *screening* the [transmitted] *transferred* digital data *prior to storage on the destination storage medium* to determine if at least one of a plurality of predefined sequences are present in the digital data received; and

in response to said [processing] *screening* step:

(a) *automatically* causing the *screened* digital data [of said transmission] 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 [of said transmission] from being stored on said destination storage medium if at least one predefined sequence is present.

* * * * * *

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

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

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.

Def.'s Ex. 16, 8/13/92 Amendment at 1-2, 4.

Important here is the addition of the requirement in the screening step that the screening be performed "prior to storage on the destination storage medium."

The Gray Declaration emphasized that the unique feature of the '776 invention was its ability to screen for a multitude of virus signatures while digital data was being transferred and its ability to stop the transfer midstream when a virus was detected and "before the virus was copied into the system." *See* Def.'s Ex. 17, Gray Decl. of 8/12/92 at para. 4. Because it would preclude the copying and storage of virus-infected data on the computer system in the first instance, the '776 invention was "the best method of protecting against computer viruses". *Id*. It was this prophylactic feature which distinguished the '776 invention from the prior art which scanned, detected and then removed "infected files from a computer's storage media such as a hard disk drive." *Id*. at para. 3. It is also the key feature that distinguishes the '776 invention from Defendant's accused product, VirusScan.

Having properly construed the language in Claims 1 and 18, the Court now addresses the question whether Defendant's accused product infringes Hilgraeve's '776 patent by practicing the same method steps.

B. Infringement

[12] [13] [14] Unlike claim construction, the question of infringement is a question of fact for the jury, and "[t]he patentee bears the burden of proving infringement by a preponderance of the evidence." *Laitram,* 939 F.2d at 1535. Nonetheless, summary judgment of non-infringement is properly granted if the court determines the patentee has failed to raise a genuine issue of material fact on the issue of infringement and the accused infringer is entitled to judgment as a matter of law. Wolverine, 38 F.3d at 1196; Johnston, 885 F.2d at 1576-77. Hilgraeve alleges that Defendant has infringed its '776 patent both literally and under the doctrine of equivalents because it screens for viruses before storage on the destination storage medium. The court analyzes each of these claims separately.

1. Literal Infringement

[15] As observed by the Federal Circuit Court of Appeals, "a literal infringement issue is properly decided upon summary judgment when no genuine issue of material fact exists, in particular, when no reasonable jury could find that every limitation recited in the properly construed claim either is or is not found in the accused device." Bai v. L & L Wings, Inc., 160 F.3d 1350, 1353 (Fed.Cir.1998). Here, Defendant's accused product, VirusScan, FN10 does not literally meet all of the claim limitations. Accordingly, as a matter of law, there is no literal infringement and Defendant is entitled to summary judgment as to this claim.

FN10. The DOS, Windows 95, Windows 98 and Windows NT versions of VirusScan are at issue. For purposes of infringement, the parties' experts agree that all of these versions of VirusScan work the same way. *See* Geske Dep. at 56; Belgard Decl. at para. 11.

[16] To determine whether infringement has occurred, the Court compares the properly construed claims of the '776 patent with the Defendant's accused product. Hilgraeve contends that Defendant's accused product,

VirusScan, infringes Claims 1 and 18 of the '776 patent because it similarly screens incoming digital data for viruses during transfer and *before* "storage" on the destination storage medium. Defendant, on the other hand, asserts that the accused product screens only after all the incoming digital data has been transferred and "stored" on the destination storage medium. Thus, the critical issue presented here is **when** not **if** the accused product performs the virus screening.

Defendant asserts that its accused product, VirusScan, does not perform the claimed steps of "screening the data as it is being transferred" or "receiving and screening the transferred digital data *prior to storage on the destination storage medium* " (Claim 1), and does not perform the step of "searching for a plurality of virus signatures ... *while said computer is receiving a stream of digital data for storage* " (Claim 18). Rather, Defendant urges, the accused VirusScan product performs its virus screening step *after* all the digital data has been transferred, received and "stored" on the destination storage medium. This Court agrees.

Defendant proffers the testimony of its expert, Mr. Richard Belgard, who opines, based upon his examination of the '776 patent-in-suit, the accused VirusScan product's source code and testing with VirusScan, that VirusScan first stores digital data and then screens for viruses. Accordingly, he opines, VirusScan does not practice Claims 1 and 18 of the '776 patent. To illustrate this point, Mr. Belgard developed a flow chart showing VirusScan's sequential steps of operation and explaining how VirusScan operates in conjunction with an application program invoking the Windows95 operating system to delete a transferred file that VirusScan determines is infected with a virus. Below is a description of the VirusScan operation which demonstrates that "storage" as construed by the Court occurs at step 5 and virus screening is performed thereafter at steps 6 and 7.

First, the application program transfers all the data for storage in a file on the destination storage medium. Second, the application program makes a request for the operating system to close the file containing the transferred data. Third, VirusScan intercepts the program's request to the operating system to close that file. When the "close file" command is intercepted, all the requested data has been transferred and stored in a designated file on the destination storage medium and is ready to be made available to the computer system. Fourth, VirusScan makes a call to the operating system to close the file on behalf of the application program.

Fifth, the operating system closes the file, releases the transferred digital data that it has maintained on behalf of the application program, and returns control back to VirusScan. As demonstrated by Mr. Belgard's testing, at this point, the operating system has made all the data transferred to the file available to the computer system, and the file has been completely stored on the destination storage medium; e.g., the hard disk drive. As far as the operating system, and all other application programs are concerned, the file is available for copying and executing even if it contains a virus.

At the sixth step, VirusScan scans the file for viruses. If no viruses are found, control is returned back to the application program, as shown in step seven. If a virus is detected, VirusScan calls the operating system to delete the file or take whatever option was chosen. This is shown in step eight. At step nine, the operating system responds to the VirusScan call and deletes the file (or performs the other chosen options). VirusScan then returns to the calling application as shown in step 10. *See* Belgard 2/4/99 Decl. para.para. 41-51 and Ex. E.

Unlike the '776 patent's disclosed method, the accused product first allows the incoming digital data (file), including virus-infected data, to pass through buffer (38) to be stored on the destination storage medium

(40) by the operating system. Although digital data does not remain at step 5, during this vulnerable post-storage, pre-scan period, the potential exists for virus-infected data to spread and infect a computer system. At step 5, all the data is transferred, stored on the destination storage medium, and accessible to the operating system and other programs. Thus, Virus screening by VirusScan is performed only after the incoming digital data has been fully transferred and after "storage." The virus screening performed at steps 6 and 7 takes place after the "storage" at step 5. Therefore, the accused VirusScreen product cannot perform the "receiving and screening... prior to storage" limitation of Claim 1. *See* Belgard 2/4/99 Decl. at para.para. 45-51, 52-62; Belgard 3/23/99 Supp. Decl. at para.para. 10-12; Geske Report at 7. Accordingly, there is no literal infringement of the screening "prior to storage" limitation of Claim 1 of the '776 patent. Similarly, because the accused product scans for viruses after digital data has been transferred and stored, there is no literal infringement of Claim 18's limitation that simultaneous searching for a plurality of viruses be performed "while said computer is receiving a stream of digital data for storage on said storage medium." The accused product does not search or screen for viruses *while* the digital data is being transferred or *while* digital data is being received *for storage*. As construed above, consistent with Claim 1, Claim 18 of the '776 patent requires that the virus screening is to be performed during the transfer of digital data and "prior to storage on the destination storage medium." FN11

FN11. Hilgraeve does not dispute that this clause of Claim 18 requires that virus screening be performed before storage. *See* Plf.'s Resp. at 11.

Contrary to Hilgraeve's assertions, it has not presented competent evidence disputing that VirusScan first stores incoming digital data (at step 5) before it screens for viruses (at steps 6 and 7). Hilgraeve relies on three forms of evidence: expert testimony by Dr. Geske, purported lay testimony by a co-inventor of the '776 patent-in-suit, John Hile, and marketing materials allegedly used in connection with the accused VirusScan product. Each category of evidence and its flaws are discussed in turn.

First, testimony of Hilgraeve's expert, John Geske, does nothing to advance Hilgraeve's claim that Defendant's accused product screens for viruses *before* storage. Rather, Dr. Geske admits in his expert report that "[a]fter the digital data has been transferred to the destination storage medium, *VirusScan* receives and screens the transferred data to determine if a predefined sequence (virus signature) is present in the digital data received." Plf.'s Ex. 20, Geske 12/9/98 Expert Report at 7. *See also* Def.'s Ex. 3, Geske 1/19/99 Dep. at 151, 155-157, Geske 3/19/99 Decl. at para. 20. Hilgraeve's expert likewise fails to raise a genuine dispute concerning: (1) the sequence of VirusScan's operating steps as detailed in Mr. Belgard's flow chart; and (2) Belgard's conclusion that, because "storage" occurs at step 5 and virus screening occurs at steps 6 and 7, VirusScan does not practice the limitations of Claims 1 and 18 of the '776 patent, and thus there is no infringement. Dr. Geske simply ignores step five where Mr. Belgard opines that "storage" occurs and concludes there is infringement because screening is done at steps 6 and 7. Without providing factual support for his decision to ignore step 5, Dr. Geske summarily concludes that the "receiving and screening... prior to storage" step of Claim 1 is practiced by the accused VirusScan product at steps 6 and 7 of Mr. Belgard's flow chart. This factually unsupported conclusion is insufficient to create a triable issue of fact. *See* Johnston, 885 F.2d at 1578.

Similarly, Hilgraeve's expert's criticism of Belgard's VirusScan testing and proof of the above facts misses the point and is thus unavailing. Contrary to Hilgraeve's assertions, the testing is probative of a material fact. Defendant's expert, Richard Belgard, did not set out to evaluate VirusScan's methodology from the perspective of an ordinary user. Rather, using his expertise in the subject matter, Mr. Belgard's atypical use

was designed to test and confirm his analysis of the accused product's source code and his conclusion that VirusScan first stores and then scans transferred digital data for viruses. Dr. Geske's factually unsupported conclusion that Mr. Belgard could not duplicate any of his tests and his criticism that Mr. Belgard did not configure VirusScan in a manner most favorable to Hilgraeve are insufficient to create a triable issue of fact. *See* Geske 3/19/99 Decl. at para.para. 4, 10.

Likewise unavailing is Dr. Geske's reference to a subsequent transfer to a floppy disk, after initially transferring the data to a computer's hard drive, and calling that floppy disk a "destination storage medium" in an attempt to refute Mr. Belgard's conclusions. This subsequent transfer to a floppy dist merely demonstrates an additional copying sequence after the file has already been stored on the computer's hard drive. Dr. Geske admits as much in his Declaration at para. 14: "For a download operation with the floppy disk being the destination, the data is transferred to a buffer on the hard drive where it is screened for viruses." This testimony does nothing to dispute Mr. Belgard's proffered opinion that VirusScan first stores and then screens for viruses and thus does not practice the "receiving and screening ... prior to storage" limitation of Claim 1 or the "searching for a plurality of virus signatures... while ... receiving a stream of digital data for storage" limitation of Claim 18. Accordingly, Hilgraeve's criticism of Defendant's expert's tests on the accused product is not enough to survive summary judgment.

Hilgraeve's infringement arguments, similar to its expert's opinions, improperly gloss over the "prior to storage" limitation contained in the screening step and instead focus on the "automatically inhibit" language of the inhibiting step. *See* Geske 12/9/98 Expert Report at 7; Geske 3/19/99 Decl. at para.para. 5, 6, 11, and 14. Doing so, they improperly ignore the sequential order of the steps of Claims 1 and 18 which Hilgraeve admits are required "to be performed in a particular order". Plf.'s Resp. at 4. Infringement cannot be established by broadly arguing that both the '776 patent and the accused product "transfer data to the system and buffer it, screen the buffered data for viruses, store the screened data for retrieval if virus-free, and inhibit storage of the screened data if a virus is found." *See* Plf.'s Resp. at 32. Rather, to prove infringement, Hilgraeve must establish that every limitation recited in the properly construed claims can be found in the accused device. *See* Bai, 160 F.3d at 1353. Likewise, at the summary judgment stage, Hilgraeve must show that there are triable issues of material fact concerning whether Defendant's accused VirusScan product practices every limitation in Claims 1 and 18. Hilgraeve has not met its burden here with Dr. Geske's proffered testimony. It likewise fails to satisfy its burden with the proffered testimony of John Hile.

In an effort to defeat summary judgment, Hilgraeve presents the Court with the Declaration of one of the co-inventors of the '776 patent-in-suit, John Hile. In his Declaration, Mr. Hile describes tests he performed using the accused VirusScan product and proffers an opinion that VirusScan "performs each of the steps of method claims 1, 2, 6, and 18 of the '776 patent." Hile 3/17/99 Decl. at para. 2. Mr. Hile's Declaration, the testing it describes, and the opinions it expresses are claimed to be that of a lay witness, based on personal knowledge, and thus admissible under Fed.R.Evid. 701.FN12 This Court disagrees. The Hile Declaration and supporting exhibits are hereby stricken because they are a thinly-veiled effort to introduce expert testimony in an improper manner.

FN12. Fed.R.Evid. 701 provides that:

If the witness is not testifying as an expert, the witness' testimony in the form of opinions or inferences is limited to those opinions or inferences which are (a) rationally based on the perception of the witness and (b) helpful to a clear understanding of the witness' testimony or the determination of a fact in issue. Despite Hilgraeve's assertion that he is merely a lay witness providing a lay opinion of how VirusScan

operates "from the user's perspective", Hilgraeve attempts to use Hile's testimony to establish that Defendant's accused product literally infringes claims 1, 2, 6, and 18 of the '776 patent. *See* Hile 3/17/99 Decl. at para. 16 (where he avers "I believe that the error was due to the fact that buffered data was deleted from the temporary Internet files so it could not be stored on the destination floppy disk") and para.para. 20, 22, and 24 (which contain similar "I believe" opinion language related to infringement issues).

Lay opinion evidence concerning how VirusScan operates "from a user's perspective" is not helpful in resolving the infringement issues raised here and thus is not admissible under Rule 701. This Court is not convinced that an ordinary user, using VirusScan and viewing the computer screen as Mr. Hile did, would be able to draw the same inferences Mr. Hile does and conclude that VirusScan performs the same steps in the same order as those in Claims 1 and 18 of the '776 patent. On the contrary, Mr. Hile's opinions and conclusions require specialized knowledge and are drawn from his technical or specialized knowledge in the area of computer science. This testimony "is precisely the type of 'specialized knowledge' governed by Rule 702" concerning expert opinion testimony.FN13 United States v. Figueroa-Lopez, 125 F.3d 1241, 1246 (9th Cir.1997), *cert. denied,* 523 U.S. 1131, 118 S.Ct. 1823, 140 L.Ed.2d 959 (1998).

FN13. Fed.R.Evid. 702 provides that:
If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise.
[17] The federal courts have consistently observed that where opinion testimony is based on a witness's specialized knowledge, it is to be admitted under Rule 702 rather than 701. *See* Doddy v. Oxy USA, Inc., 101 F.3d 448, 460 (5th Cir.1996) (where the court observed that "a person may testify as a lay witness only if his opinions or inferences do not require any specialized knowledge and could be reached by any ordinary person"); Randolph v. Collectramatic, Inc., 590 F.2d 844, 846 (10th Cir.1979) (where the court observed that Rule 701 generally "does not permit a lay witness to express an opinion as to matters which are beyond a realm of common experience and which require the special skill and knowledge of an expert witness"). "A holding to the contrary would encourage [a party] to offer all kinds of specialized opinions without pausing first properly to establish the required qualifications of their witnesses." Figueroa-Lopez, 125 F.3d at 1246. Moreover, if "[t]he mere percipience of a witness to the facts on which he wishes to tender an opinion" were allowed to "trump Rule 702", then "a layperson witnessing the removal of a bullet from a heart during an autopsy could opine as to the cause of the decedent's death." *Id.*

Experts typically do as Mr. Hile has done here, tie observations to conclusions through the use of specialized knowledge or experience. When they do so, admission of such testimony is governed by Rule 702 and is subject to the relevancy and reliability factors discussed in Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993). *See* Kumho Tire Co., Ltd. v. Carmichael, 526 U.S. 137, ----, 119 S.Ct. 1167, 1174, 143 L.Ed.2d 238 (1999) (where the Court held that *Daubert* factors apply to the testimony of engineers and other experts who are not scientists). Hilgraeve cannot use Rule 701 as a back door attempt to admit testimony of an expert nature under the guise of lay opinion and thus strip the Court of its *Daubert* gatekeeping functions. *See* United States v. Thomas, 11 F.3d 1392 (7th Cir.1993) (where the court observed that "it would be highly prejudicial" to allow a party to bring "expert testimony through the back door under the guise of lay opinion testimony"). Because Mr. Hile's conclusions are based on his technical or specialized knowledge, to be admitted and considered as evidence, he should have been disclosed as an expert. This was not done, and the Court will not permit Hilgraeve to use Rule 701 as a back door to admit evidence that it should have sought to have admitted under Rule 702.

Finally, the Court addresses Hilgraeve's evidence concerning *the user's perspective* of the accused product; i.e., Defendant's promotional materials, and Hilgraeve's argument that infringement can be determined by considering the *user's perspective* or *market expectations* of the accused product. Hilgraeve presents evidence of Defendant's marketing materials which compare its VirusScan product with other competing virus scanning products. There is no comparison with the '776 patented invention. *See* Plf.'s Resp. at 16-17. Assuming, without deciding, that this evidence is admissible, the Court concludes that this evidence is insufficient to raise a triable issue of fact concerning infringement of the '776 patent.

The material facts presented here are those concerning how the accused product actually operates; i.e., does its source code or some other credible evidence show that it screens incoming digital data for viruses before "storage"; not how a typical user perceives that the accused product operates. The marketing and promotional documents Hilgraeve proffers here do not disclose the accused product's source code. They do not provide technical details about the accused product's operating steps; i.e., revealing when virus screening and "storage" occur. Accordingly, they do not give rise to the inference that the accused product infringes Claims 1 and 18 of the '776 patent. Likewise, general statements that VirusScan is designed to prevent the spread of computer viruses, without more, do not give rise to the inference that VirusScan infringes Claims 1 and 18.

The essence of Hilgraeve's infringement argument is that any comparison of Claims 1 and 18 of the '776 patent with Defendant's accused product must be considered from the user's perspective; i.e., regardless of proof that the accused product does not practice each element of the patent-in-issue, if a typical user of the accused product, during its normal operation, *perceives* that the accused product performs like the '776 invention, then this is evidence that the accused product does in fact infringe Claims 1 and 18 of the '776 patent. *See* Plf.'s Resp. at 31-32. This Court is not persuaded by Hilgraeve's "user-perspective" argument.

How an ordinary user perceives that an accused product works is not the test applied in a patent infringement action. Rather, the Court examines evidence concerning how the product *actually* operates. For example, with a computer product, the court examines its source code and related technical materials. With a mechanical device, the court examines the engineering drawings and specifications; not how an ordinary user "perceives" or speculates that the accused device operates. The Court then compares the accused product with the patented claims, as construed by the Court, and determines whether the accused product practices the claims of the patent-in-issue.

Hilgraeve's reliance on Laitram Corp. v. Cambridge Wire Cloth Co., 863 F.2d 855, 859 n. 11 (Fed.Cir.1988), is misplaced. Hilgraeve vastly overstates the significance of the dicta found in the referenced footnote. The *Laitram* court merely observed that the defendant's position during litigation was contrary to its promotional materials which claimed that the accused product was superior to the plaintiff's patented invention. The court, however, did not premise its decision on that observation. Accordingly, this decision does nothing to advance Hilgraeve's arguments here. More on point, is the Federal Circuit Court of Appeals' decision in SmithKline Diagnostics, Inc. v. Helena Laboratories Corp., 859 F.2d 878, 890-91 (Fed.Cir.1988). There, the Court rejected an "infringement by estoppel" argument similar to the one Hilgraeve raises here.

In *SmithKline,* the plaintiff argued that, because defendant had incorrectly identified a patented element as part of the accused product, it should not benefit from sales and should be estopped from denying that its product infringes plaintiff's patented product. The *SmithKline* court rejected the plaintiff's "infringement by estoppel" theory, observed that the defendant's product was not the patented invention and refused to adopt a theory that would allow marketing materials to convert a non-infringing product into an infringing product.

The same rationale and result apply with even greater force under the facts presented here. This Court refuses to adopt a theory that would allow marketing materials to covert a non-infringing product into an infringing product.

Comparison of the embodiments taught in the '776 patent with Defendant's accused product and consideration of the evidence presented by Hilgraeve in opposition to Defendant's motion compels the conclusion that no genuine issue of materialfact exists for trial on the question whether Defendant's accused product, VirusScan, literally infringes Hilgraeve's '776 patent.

2. Infringement Under the Doctrine of Equivalents and Prosecution History Estoppel

[18] Under the doctrine of equivalents, "a product or process that does not literally infringe upon the express terms of a patent claim may nonetheless be found to infringe if there is 'equivalence' between the elements of the accused product or process and the claimed elements of the patented invention." Warner-Jenkinson Co. v. Hilton Davis Chemical, 520 U.S. 17, 19, 117 S.Ct. 1040, 1045, 137 L.Ed.2d 146 (1997). The Supreme Court recently voiced its concern that the doctrine of equivalents had "taken on a life of its own, unbounded by the patent claims", and thus undertook to clarify the proper scope of the doctrine. Id. 117 S.Ct. at 1048-49. It held that "the doctrine of equivalents must be applied to individual elements of the claim, not to the invention as a whole" and "application of the doctrine, even as to an individual element, is not allowed such broad play as to effectively eliminate that element in its entirety." Id. at 1049.

[19] Moreover, because "the question under the doctrine of equivalents is whether an accused element is equivalent to a claimed element, the proper time for evaluating equivalency-and thus knowledge of the interchangeability between elements-is at the time of infringement." Id. at 1053. The Court further emphasized that "intent plays no role in the application of the doctrine of equivalents." Id. at 1052. Rather, "the determination of equivalence should be applied as an objective inquiry on an element-by-element basis." Id. at 1054. Moreover, the Court concluded that whatever approach for determining "equivalency" is used; i.e., either the triple identity or the insubstantial differences approach, it must be "probative of the essential inquiry: Does the accused product or process contain elements identical or equivalent to each claimed element of the patented invention?" *Id*. Under either approach, the critical focus should be on individual elements with "a special vigilance against allowing the concept of equivalence to eliminate completely any elements." *Id*. "An analysis of the role played by each element in the context of the specific patent claim will thus inform the inquiry as to whether a substitute element matches the function, way, and result of the claimed element, or whether the substitute element plays a role substantially different from the claimed element." *Id*.

[20] [21] Defendant argues that prosecution history estoppel precludes Hilgraeve from asserting a claim of infringement under the doctrine of equivalents. "Prosecution history estoppel provides a legal limitation on the application of the doctrine of equivalents by excluding from the range of equivalents subject matter surrendered during prosecution of the application of the patent. The estoppel may arise from matter surrendered as a result of amendments to overcome patentability rejections, or as a result of arguments to secure allowance of a claim." Sextant Avionique v. Analog Devices, Inc., 172 F.3d 817, 826 (Fed.Cir.1999) (internal quotes and citations omitted). The question is whether prosecution history estoppel is available here presents a question of law for the Court. Bai, 160 F.3d at 1356. The essence of this estoppel theory is that "a patentee should not be able to obtain, through litigation, coverage of subject matter relinquished during prosecution." Haynes Int'l, Inc. v. Jessop Steel Co., 8 F.3d 1573, 1577-78 (Fed.Cir.1993), *modified on rehearing,* 15 F.3d 1076 (Fed.Cir.1994) (affirming summary judgment of non-infringement).

The test for prosecution history estoppel is "an objective one, measured from the vantage point of what a competitor was reasonably entitled to conclude, from the prosecution history, that the applicant gave up to procure issuance of the patent." *Id.* As observed in *Bai,* "[a]n applicant who responds to an examiner's prior art rejection by narrowing his claim cannot later assert that the surrendered subject matter is an equivalent of the amended limitation." 160 F.3d at 1356. Thus, if "a patent applicant has made a substantive change to his claim that clearly responds to an examiner's rejection of that claim as unpatentable over prior art, prosecution history estoppel applies to that claim; only the question of the scope of the estoppel remains." Sextant, 172 F.3d at 826 (internal quotes and citations omitted).

"The scope of the estoppel in such cases includes features that the applicant amended his claim to avoid or trivial variations of such prior art features. Moreover, prosecution history estoppel cannot be avoided by filing a continuing application with narrowed claims rather than responding directly to an outstanding rejection." Desper Products, 157 F.3d at 1338 (internal quotes and citations omitted). The scope of the estoppel is ascertained by considering the subject matter surrendered during the prosecution history, and "is determined with reference to the prior art and any amendments and/or arguments made in an attempt to distinguish such art". Sextant, 172 F.3d 817, 826 (citations omitted).

[22] Prosecution history estoppel applies here. *See* prosecution history *supra* at 748-751. As originally submitted, there was no Claim 18 and Claim 1 of the '776 patent application contained no limitation that virus screening was to be performed "prior to storage." In an effort to overcome rejection based on prior art, the applicants amended the patent claims and argued that the claims were patentable because they required that virus screening be performed during the transfer of incoming digital data and before storage. It is evident from the prosecution history that the '776 patent applicants: (1) narrowed the scope of their claims so as to avoid the prior art; (2) added the limitation that virus screening was to be performed "prior to storage on the destination storage medium"; and (3) surrendered the subject matter at issue here; i.e., computer virus screening methods that screen for viruses after storage. Accordingly, Hilgraeve is estopped from arguing here that the accused product, which screens for viruses *after* "storage", infringes any claim of the '776 patent under the doctrine of equivalents.

IV. Conclusion

For the foregoing reasons, Defendant's motion for summary judgment of non-infringement is GRANTED, and the claims asserted in Plaintiff Hilgraeve's complaint are hereby DISMISSED.

E.D.Mich.,1999.
Hilgraeve Corp. v. McAfee Associates, Inc.

Produced by Sans Paper, LLC.