NOTE: This disposition is nonprecedential.

# United States Court of Appeals for the Federal Circuit

---

**SOPHOS LIMITED,**
*Appellant*

**v.**

**ANDREI IANCU, UNDER SECRETARY OF COMMERCE FOR INTELLECTUAL PROPERTY AND DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE,**
*Intervenor*

---

2017-1567

---

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in No. IPR2015-01405.

---

Decided: March 28, 2018

---

STANLEY JOSEPH PANIKOWSKI, III, DLA Piper LLP (US), San Diego, CA, argued for appellant. Also represented by SEAN C. CUNNINGHAM, KATHRYN RILEY GRASSO.

MOLLY R. SILFEN, Office of the Solicitor, United States Patent and Trademark Office, Alexandria, VA, argued for intervenor. Also represented by NATHAN K. KELLEY,

SARAH E. CRAVEN, THOMAS W. KRAUSE, WILLIAM LAMARCA.

---

Before PROST, *Chief Judge,* O'MALLEY, and TARANTO, *Circuit Judges.*

TARANTO, *Circuit Judge*.

In this inter partes review, Finjan Holdings, Inc. challenged various claims of Sophos Limited's U.S. Patent No. 8,776,218, which describes and claims computer programs that perform runtime behavior-based detection of malicious software. The Patent Trial and Appeal Board of the Patent and Trademark Office (PTO) determined that certain claims are unpatentable for obviousness. Sophos appeals from the Board's decision. With Finjan no longer participating, the PTO's Director has intervened. Because the Board's claim construction, as the Board understood its scope, is incorrect, we vacate the Board's decision and remand for further proceedings.

## I

### A

The '218 patent relates to a computer program that monitors "an executing computer process" for "indication[s] of malicious behavior," takes "[a] plurality of malicious behavior indications observed" in the executing computer process and compares that observed collection to one or more "predetermined collection[s] of malicious behaviors" in a database of such collections, and, if there is a "match[]," conducts further analysis and causes action to be taken. '218 patent, Abstract. The particular claim phrase at issue here involves assigning a "rank" to a predetermined collection of malicious behaviors, relative to other collections. Doing so can help determine the threat level when the observed set of malicious behaviors in the executing computer process is found to match a

particular predetermined collection of malicious behaviors. *See* '218 patent, col. 18, lines 26–30, col. 24, lines 10–14.

Malicious software (malware) can take various forms such as "virus, worm, spam, phishing exploration, spyware, [and] adware." *Id.*, col. 3, lines 19–23. The patent describes using two kinds of databases for malware detection. Each element in one database is a predetermined malicious behavior referred to as a "gene," which may be identified in an executing computer process being monitored. *Id.*, col. 1, lines 46–50. The patent gives examples of genes (malicious behaviors), such as disabling operating system tools, disabling a firewall, adding itself to firewall lists, copying itself to a system folder, and opening a hidden file. *Id.*, col. 2, lines 16–24. Each element in the other database is a predetermined *collection* of such genes, each such collection referred to as a "phenotype." *Id.*, col. 1, lines 52–56. A phenotype may be any combination of such behaviors—in particular, "a predetermined collection of malicious behaviors which may include a grouping of specific genes that are typically present in a type or family of malicious code." *Id.*, col. 18, lines 18–21; col. 1, lines 54–56.

The patent describes the process of testing an executing or other program—a "runtime object" in the case of an executing program—by gathering observed indications of malicious behavior (genes) in the program, comparing a plurality of such indications to the phenotypes in the phenotype database, and "causing an action based on a prediction that the executing computer process is the type of malicious code as indicated by the phenotype." *Id.*, col. 1, lines 56–58; *see id.*, col. 18, lines 22–25 (stating that a monitoring component "may be able to identify a phenotype of behaviors in an executing code by comparing a collection of observed behaviors with the predetermined collections of known malicious behaviors stored as phenotypes in a phenotype database"). What is sought in the

comparison is a "match." *Id.*, Abstract; col. 17, lines 41–48, 61–65. The patent explains the benefits: "Matching this runtime genotype data with known combinations stored in the phenotype database, with or without additional content analysis, may enable the identification and interruption of malware while it is executing." *Id.*, col. 17, lines 41–45 (figure numbers omitted). "By matching combinations of behaviors in this way, detection of malware may be improved over solutions where only singular behaviors and a static content analysis is utilized." *Id.*, col. 17, lines 45–48.

The patent specification contains one mention of "rank[ing]." It says: "Phenotypes may capture a combination or a series of behaviors that may be ranked to create increasing levels of confidence that the runtime object being monitored is executing a behavior pattern comparable to a known family of malware." *Id.*, col. 18, lines 26–30.

During prosecution of the patent, in response to a rejection, Sophos amended its claims to add language specifically about ranking, not previously recited in the claims. J.A. 116, 120. Both in the language of the independent claims, *see infra* p. 5 (quoting claim 1) and in its explanation accompanying the amendment, Sophos made clear that it is each phenotype (each one a "combination or a series of behaviors," '218 patent, col. 18, line 27) that is "ranked," so that matching one phenotype rather than another can provide more information about the likely malware threat of the runtime object being tested. Sophos explained:

> [P]henotypes are created and ranked to provide increasing levels of confidence that a runtime object is executing a behavior pattern comparable to a known family of malware. A content analysis is then performed only after detected malicious behavior indications correspond to a phenotype hav-

> ing a predetermined level of confidence that the computer process contains a known family of malware. In this manner, the applicant's technique includes a progression from phenotype detection to content analysis based on a likelihood of malware. Claim 1 has been amended to clarify this inventive concept.

J.A. 120.

The Board and the parties treat claim 1 as representative. It reads:

> A computer program product embodied in a non-transitory computer readable medium that, when executing on one or more computers, performs the steps of:
>
> monitoring an executing computer process for an indication of malicious behavior, wherein the indication of the malicious behavior is a result of comparing an operation with a predetermined behavior, referred to as a gene, where the gene is stored for reference in a database and wherein the gene relates to at least one of API calls, registry access, process manipulation, and file system access;
>
> performing the monitoring step a number of times to collect a plurality of malicious behavior indications;
>
> comparing the plurality of malicious behavior indications to a predetermined collection of malicious behaviors, referred to as a phenotype, which comprises a grouping of specific genes that are typically present in a type of malicious code, and *wherein the phenotype is one of a number of phenotypes that are ranked to create increasing levels of confidence that a*

> *runtime object is executing a behavior pattern comparable to a known family of malware*;
>
> triggering a content analysis of the executing computer process when the plurality of malicious behavior indications for the executing computer process corresponds to one of the number of phenotypes having a predetermined level of confidence that the executing computer process contains a known family of malware, thereby providing a prediction that the executing computer process is the type of malicious code; and
>
> causing an action based on the prediction.

'218 patent, col. 23, line 60 through col. 24, line 24 (emphasis added). Claim 11 depends on claim 1, and claim 12 contains an identical "wherein . . . are ranked" clause in its comparing step. *Id.*, col. 24, lines 65–67; col. 25, lines 1–23.

B

Finjan petitioned for an inter partes review of claims 1 through 20 under 35 U.S.C. §§ 311–19. The Board, acting as the delegate of the PTO's Director under 37 C.F.R. § 42.4(a), instituted a review of claims 1, 11, and 12 on multiple grounds, all under 35 U.S.C. § 103. *Finjan Holdings, Inc. v. Sophos Ltd.*, IPR2015-01405, Paper No. 9, at 27 (P.T.A.B. Dec. 15, 2015) (*Institution Decision*).[1] The Board decided to review claims 1 and 12 for obviousness over U.S. Patent No. 7,809,670 (Lee) and U.S. Patent

---

[1] The '218 patent, which issued from a 2009 application, is governed by the version of § 103 that was in effect before the provision's amendment by the Leahy-Smith America Invents Act, Pub. L. No. 112-29, § 3(n)(1), 125 Stat. 284, 293 (2011).

No. 8,171,545 (Cooley), and also over U.S. Patent No. 7,089,428 (Farley) and Cooley. *Id.* The Board decided to review claim 11 for obviousness over Lee, Cooley, and U.S. Application No. 2007/0240217 (Tuvell) and also over Farley, Cooley, and Tuvell. *Id.*

In its Final Written Decision, the Board construed the claim phrase requiring that phenotypes "are ranked." *Finjan Holdings, Inc. v. Sophos Ltd.*, IPR2015-01405, 2016 WL 7987957, at *4–6 (P.T.A.B. Nov. 30, 2016) (*Final Written Decision*). The Board first construed the term "ranked" to mean simply "ordered," *id.* at *4, meaning that the phenotypes must be ordered vis-à-vis each other. The Board then concluded that, in the phrase "are ranked," ranking "*may* occur as part of the comparing step such that phenotypes are not 'already ranked'" before the comparing step begins. *Id.* at *6 (emphasis added).

The "may" in that conclusion, however, ultimately does not accurately reflect the Board's understanding of "are ranked." As the key substantive basis for its claim construction, the Board explained its understanding of the claimed ranking in a way that actually precludes pre-comparison ranking. Specifically, the Board said that "[a]s *a result of* the comparison, the phenotypes 'are ranked'"; "[i]t is *only* in the context of the comparison that the ranking occurs"; and "[t]he reason for the comparison between the 'malicious behavior indications' and the 'phenotypes' is to identify the most problematic phenotype, *which is 'ranked' according to how similar it is to the 'executing computer program*.'" *Id.* at *5 (emphases added). In short, the Board's understanding is that the invention ranks phenotypes based on their similarity to a particular runtime object being examined. The Director confirms that this is the Board's construction and that the

construction necessarily precludes pre-comparison ranking. Director's Br. 1–2.[2]

The Board then applied that understanding. Using that similarity-based understanding, it found that both Lee and Farley disclosed the "are ranked" limitation. *Final Written Decision*, 2016 WL 7987957, at *14, *18–19. And, as a result, it held that claims 1, 11, and 12 are unpatentable for obviousness. *Id.* at *20.

Sophos timely appealed the Board's decision under 35 U.S.C. §§ 141(c) and 319. Finjan declined to participate in this appeal, and the PTO's Director intervened, pursuant to 35 U.S.C. § 143, to defend the Board's decision. Appellee's Notice of Non-Participation, ECF No. 12 (Apr. 4, 2017); Notice of Intervention by the United States Patent and Trademark Office, ECF No. 18 (May 17, 2017). We have jurisdiction under 28 U.S.C. § 1295(a)(4)(A).

## II

Sophos argues that the Board, in construing the ranking limitation, misunderstood what "are ranked" means in the context of the claims. More specifically, Sophos contends that the Board was wrong in its fundamental view that the predetermined phenotypes, which are stored in the database, are ranked based on how similar they are to the set of malicious behavior indications observed in a particular monitored runtime object (program). The only

---

[2] The Director states that "[t]he Board construed the term 'are ranked' to *mean* ranking while the comparison is happening" and that the issue presented is: "Did the Board reasonably construe 'are ranked,' where the known collections of behaviors do not have a natural order, or ranking, except with respect to how similar they are to the unknown program, and that similarity cannot be known until the comparison is occurring?" Director's Br. 1–2 (emphasis added).

reasonable understanding of the claim phrase, Sophos says, is quite different: a phenotype is ranked relative to others based in some way on its indicating known malware; the runtime object is scrutinized to see if its set of observed behaviors matches one of the phenotypes in the phenotype database; and it is the rank of a matched phenotype that determines the level of confidence that the runtime object is like a known family of malware (triggering content analysis and action). We agree with Sophos.

The Board reached its conclusion regarding the scope of its claim construction on the basis of its degree-of-similarity-to-runtime-object understanding of the "are ranked" limitation. *Final Written Decision*, 2016 WL 7987957, at *5. On appeal, the Director defends the Board's construction of the "are ranked" limitation on that basis, stating that "the ranking is done during the claimed process to determine which phenotype most closely corresponds to a particular unknown program." Director's Br. 15. At oral argument, the Director effectively agreed that we may address the correctness of this basis for the Board's adoption of the claim construction challenged by Sophos.[3]

In an inter partes review proceeding, the Board is to give a claim "its broadest reasonable construction in light of the specification of the patent in which it appears." 37 C.F.R. § 42.100(b); *see Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2142 (2016) (affirming the PTO's authority to prescribe such a standard). "We review the Board's constructions based on intrinsic evidence de novo." *HTC*

---

[3] *See* Oral Argument at 19:47–23:45, 24:21–25:10, *Sophos Ltd. v. Iancu*, No. 17-1567 (Fed. Cir. Mar. 9, 2018), http://oralarguments.cafc.uscourts.gov/default.aspx?fl=2017-1567.mp3 (agreeing that the Board's construction was based on its understanding of ranking and that the Board's understanding may be reviewed in this appeal).

*Corp. v. Cellular Commc'ns Equip., LLC*, 877 F.3d 1361, 1367 (Fed. Cir. 2017). This includes "the Board's expression of its understanding of the scope of the claim term." *Id.*

The Board's view necessarily calls for ranking phenotypes vis-à-vis each other. That is inherent in the Board's construction of "ranked" to mean "ordered." *Final Written Decision*, 2016 WL 7987957, at *4. And the Director agrees, at least implicitly, when it defends the Board's understanding of ranking as supplying a phenotype-to-phenotype order where a "natural order, or ranking," does not exist for the phenotypes. Director's Br. 1–2.

But neither the Board's explanation nor the Director's defense of that explanation in this court indicates how the claim can reasonably be understood to call for that ranking to be based on how similar phenotypes in a database are to a particular runtime object being scrutinized. The "broadest reasonable interpretation . . . is an interpretation that corresponds with what and how the inventor describes his invention in the specification." *In re Smith Int'l, Inc.*, 871 F.3d 1375, 1382–83 (Fed. Cir. 2017); *see Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1298 (Fed. Cir. 2015) (prosecution history is relevant to this inquiry as well), *overruled in another respect by Aqua Prods., Inc. v. Matal*, 872 F.3d 1290 (Fed. Cir. 2017); *In re NTP, Inc.*, 654 F.3d 1279, 1288 (Fed. Cir. 2011) ("While the Board must give the terms their broadest reasonable construction, the construction cannot be divorced from the specification and the record evidence."); *In re Suitco Surface, Inc.*, 603 F.3d 1255, 1260 (Fed. Cir. 2010) ("The broadest-construction rubric . . . does not give the PTO an unfettered license to interpret claims to embrace anything remotely related to the claimed invention. Rather, claims should always be read in light of the specification and teachings in the underlying patent."). Here, the Board's central understanding is unreasonable in light of the

specification and, indeed, of the claim's own statement of its objective.

We have been pointed to nothing in the '218 patent that discloses ranking the predetermined phenotypes according to their degree of similarity to a particular set of malicious behaviors observed in a particular runtime object. To the contrary, the patent speaks consistently of seeking a "match" of a phenotype for the runtime object's set of malicious-behavior indications, never of examining degrees of similarity. '218 patent, Abstract; col. 17, lines 41–48, 64. In addition, the Board's notion would call for re-ranking the group of phenotypes with every new runtime object that is evaluated. The patent says nothing to that effect.

More fundamentally, the Board's notion of ranking the phenotypes by how similar each is to a particular runtime object is detached from the essential function of the invention. As claim 1 itself makes clear, the function of the comparison of a runtime object to phenotypes is to develop information about the threat presented by a runtime object, whose risk of being any type of malware is not known before the comparison. That risk information comes from matching behavior indications observed in the runtime object with a phenotype *independently* assessed for *its* threat indication, *i.e.*, what a particular phenotype indicates about the presence of a certain kind of malware. *See*, *e.g.*, '218 patent, col. 18, lines 36–41 (one phenotype may indicate that the collection of observed behavior indications is "bad" while another may indicate, more specifically, that the "process is exhibiting the same behavior as [a known] family of malware"); J.A. 529 (Finjan's statement to the Board that "[t]he purpose of ranking the phenotypes is to assess the risk that the runtime object is malware"). It is the phenotype-to-phenotype ranking, independent of similarity to the runtime object, that is the source of the information used to evaluate the runtime object, and to trigger a content

analysis and action based on the evaluation, which is the claimed invention's stated function. '218 patent, col. 1, lines 43–58; col. 18, lines 26–30. Yet the Board's notion of similarity-based ranking eliminates the essential independent source of information for assessing the runtime object, and it leaves nothing in its place that the Board or the Director has explained would still allow the claimed invention to perform its function.

The Board fundamentally misread the patent when it said, in its crucial paragraph, that "[t]he reason *for the comparison* . . . is to identify the most problematic phenotype." *Final Written Decision*, 2016 WL 7987957, at *5 (emphasis added). That statement gets the direction of inference in the patented process backwards. The point of the comparison is not to start with a known danger presented by the runtime object and infer how problematic a phenotype is by the degree of similarity to the runtime object. The danger of the runtime object is not yet known. The point of the comparison is to infer something about precisely that danger, by using independent information (through ranking) about how problematic a particular matched phenotype is. Ranking of phenotypes independently of similarity to the runtime object is an essential component of that process.

In short, nothing in the claims, the specification, or the prosecution history supports the Board's understanding that the predetermined phenotypes are ranked based on their similarity to the observed malicious behavior indications. We conclude that the Board's understanding is "divorced from the specification" and is "legally incorrect." *Smith*, 871 F.3d at 1382 (quoting *Microsoft*, 789 F.3d at 1298).

The Board's incorrect understanding of why and how ranking is performed in the context of the '218 patent appears to be a central basis for its determination that Lee and Farley disclose the "are ranked" limitation. But

we do not decide the issue of whether the prior art discloses the "are ranked" limitation under a proper construction. We remand to the Board for further proceedings consistent with this opinion.

III

The Board's decision is vacated and the matter remanded for further proceedings.

No costs.

**VACATED AND REMANDED**