Trials@uspto.gov
571-272-7822

Paper 9
Date: September 12, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.
Petitioner,

v.

OPEN TEXT INC.,
Patent Owner

IPR2023-00556
Patent 8,726,389 B2

Before GARTH D. BAER. AARON W. MOORE, and SCOTT RAEVSKY, *Administrative Patent Judges.*

BAER, *Administrative Patent Judge.*

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

CrowdStrike, Inc. ("Petitioner") filed a Petition requesting an *inter partes* review of claims 1–30 (the "challenged claims") of U.S. Patent No. 8,726,389 B2 (Ex. 1001, "the '389 patent"). Paper 1, 1 ("Pet."). Open Text Inc. ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

Under 35 U.S.C. § 314, an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Upon consideration of the Petition in view of the present record and for the reasons explained below, we determine that Petitioner has shown a reasonable likelihood of prevailing with respect to at least one of the challenged claims. Accordingly, we institute an *inter partes* review on all grounds set forth in the Petition.

B. Related Proceedings

The parties identify the following related matters: *Webroot, Inc. v. Trend Micro Inc.*, No. 6:22-cv-00239 (W.D. Tex.); *Webroot, Inc. v. Sophos Ltd.*, No. 6:22-cv-00240 (W.D. Tex.); *Webroot, Inc. v. CrowdStrike, Inc.*, No. 6:22-cv-00241 (W.D. Tex.); and *Webroot, Inc. v. AO Kaspersky Lab*, No. 6:22-cv-00243 (W.D. Tex.). Pet. 68; Paper 4, 1.

C. The '389 Patent (Ex. 1001)

The '389 patent "relates generally to methods and apparatus for dealing with malware." Ex. 1001, 1:9–10. Figure 2 of the '389 patent is reproduced below.

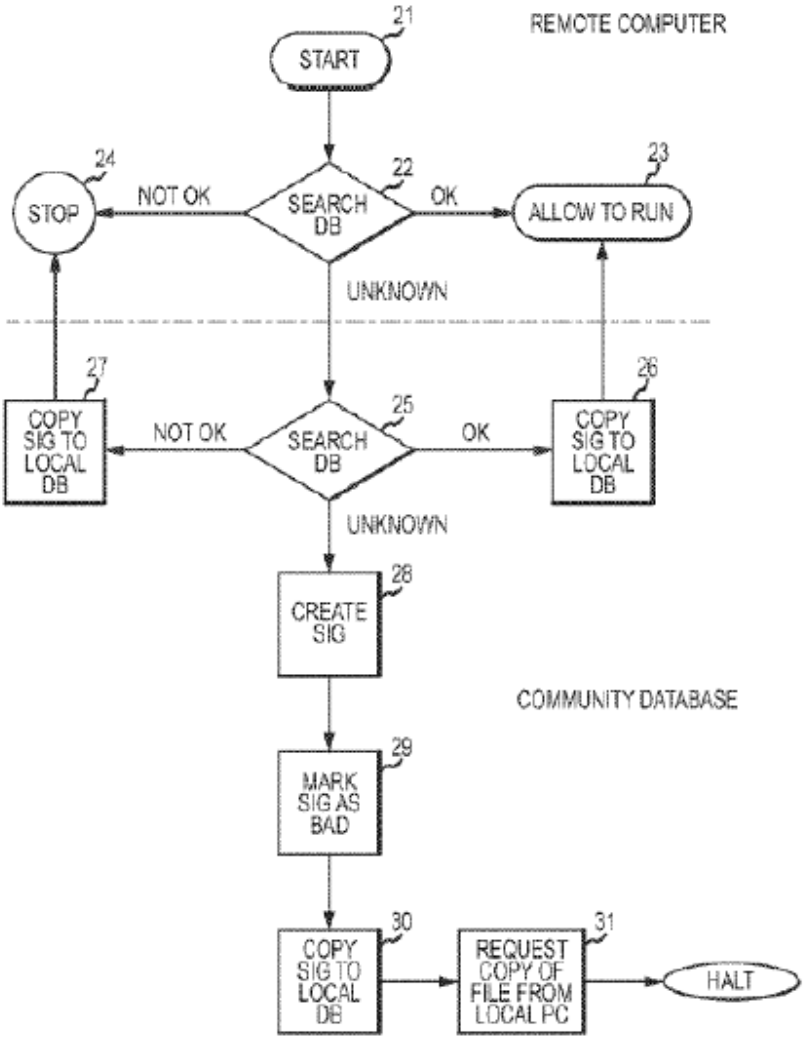

FIG.2

Figure 2 is a flowchart illustrating a method that starts at step 21 by running an object, such as a process, at a remote computer. *Id.* at 7:51–53, 8:21–22. At step 22, operation of such a process is hooked using local software running on the remote computer to search a local database for a signature or key representing that process and related objects. *Id.* at 8:22–28. If the signature indicates that the process is safe, it is allowed to run at step 23; if the signature indicates that the process is not safe, it is stopped at step 24. *Id.* at 8:33–37.

If the object is unknown locally, details of the object are passed over a network to the base computer for storing in the community database and for further analysis at the base computer. *Id.* at 8:47–50. The community database is then searched at step 25 for a signature for that object. *Id.* at 8:51–52. If found and identified as safe, then "a copy of the signature or at least a message that the object is safe" is sent to the remote computer at step 26; similarly, if found and identified as unsafe, a copy is provided to the remote computer with such a designation at step 27. *Id.* at 8:63–9:13. If the object is unknown to the community database, a signature is created at step 28 and marked as unsafe at step 29. *Id.* at 9:14–20. Such an unsafe designation may be changed as experience with the object is collected. *See id.* at 9:29–42.

D. Illustrative Claim

Challenged claims 1 and 15 are independent. Claim 1 is illustrative and is reproduced below.

> 1. A method of classifying a computer object as malware, the method comprising:
>
> at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;
>
> at the base computer, receiving data about the computer object from a second remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured,

> or runs on the second remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;
>
> storing, at the base computer, said data received from the first and second remote computers;
>
> correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;
>
> comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and
>
> classifying, by the base computer, the computer object as malware on the basis of said comparison.

Ex. 1001, 20:27–62.

E. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability. Pet. 7.

Claims Challenged	35 U.S.C. §	References/Basis
1–13, 15–27, 29, 30	103(a)[1]	Kester[2], Kennedy[3]

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), included revisions to 35 U.S.C. § 103 that became effective after the filing of the application that led to the challenged patent. Therefore, we apply the pre-AIA version of 35 U.S.C. § 103.
[2] US 2005/0210035 A1, Pub. Sept. 22, 2005 (Ex. 1004).
[3] US 7,594,272 B1, Sept. 22, 2009 (Ex. 1005).

Claims Challenged	35 U.S.C. §	References/Basis
14, 28	103(a)	Kester, Kennedy, Honig[4]

II. DISCUSSION

A. Discretion under 35 U.S.C. § 314(a) Based on Parallel Litigation

As noted above, the '389 patent is the subject of parallel district-court litigation. Patent Owner asks that we exercise our discretion to deny the Petition based on the related litigation. *See* Prelim. Resp. 4–22. For the reasons that follow, we decline to deny the Petition under § 314(a).

Institution of an *inter partes* review is discretionary. *See* 35 U.S.C. § 314(a) (2018) (stating "[t]he Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition") (emphasis added); *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) ("[T]he PTO is permitted, but never compelled, to institute an IPR proceeding."). The advanced state of a parallel district court action may warrant exercising discretion on behalf of the Director to deny a petition for inter partes review. *See NHK Spring Co. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 at 20 (PTAB Sept. 12, 2018) (precedential); *Apple Inc. v. Fintiv Inc.*, IPR2020-00019, Paper 11 at 5–6, 8 (PTAB March 20, 2020) (precedential) ("*Fintiv*"); Patent Trial and Appeal Board Consolidated Trial Practice Guide (Nov. 2019), 58 & n.2, available at https://www.uspto.gov/TrialPracticeGuide Consolidated.

[4] US 7,225,343 B1, May 29, 2007 (Ex. 1006).

Whether to exercise such discretion is informed by the Director's Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation ("Interim Procedure").[5]

We consider the following factors in assessing "whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding":

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
2. proximity of the court's trial date to the Board's projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the petition and in the parallel proceeding;
5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
6. other circumstances that impact the Board's exercise of discretion, including the merits.

Fintiv at 5–6. In evaluating these factors, we "take[] a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review." *Id*. at 6.

1. Possibility of Stay

A stay of a related proceeding pending resolution of the PTAB trial "allays concerns about inefficiency and duplication of efforts." *Fintiv* at 6. At this time, no stay has been requested or ordered in the related litigation. Pet. 64; *see also* Prelim. Resp. 6–11. Although Patent Owner asserts that a

[5] Available at https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf.

stay is unlikely even if Petitioner does seek one, *see* Prelim. Resp. 7–11, there has been no actual denial of a stay to weigh this factor against exercising discretion to deny institution. *See Fintiv* at 6–7. We thus treat this factor as neutral.

2. Schedules

According to *Fintiv*, "[i]f the court's trial date is earlier than the projected statutory deadline, the Board generally has weighed this fact in favor of exercising authority to deny institution." *Fintiv* at 9. The current scheduled trial date is August 19, 2024. *See* Ex. 1009, 6; Prelim. Resp. 8. A final written decision in this case will issue no later than mid-September, 2024. Thus, the district court's trial date is a few weeks earlier than the projected statutory deadline. However, as Petitioner notes, there is some chance the district-court trial will not proceed before our final written decision given the related litigation's complexity and because the trial date is the same for each defendant in five separate lawsuits that have been consolidated, but only for pretrial issues. Pet. 64. In these circumstances, we treat this factor as neutral.

3. Investment in Parallel Proceeding

"[I]f, at the time of the institution decision, the district court has issued substantive orders related to the patent at issue in the petition, this fact favors denial" of the Petition. *Fintiv* at 9–10. Patent Owner argues this factor favors denial because the district court issued a claim construction order, and the parties have already engaged in extensive discovery. Prelim. Resp. 15. Despite the parties' investment in the parallel proceeding, fact discovery remains open, expert reports have not yet been served, and dispositive motions are not due until May 7, 2024. Ex. 1009, 5–6. In these

circumstances, we treat this factor as weighing slightly in favor of denying institution.

4. Overlap of Issues

"[I]f the petition includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel proceeding, this fact has favored denial." *Fintiv* at 12. Petitioner stipulates that, "if the Board institutes IPR, Petitioner will not seek resolution in the District Court of any instituted ground of invalidity for the '389 Patent." Pet. 65. This is consistent with a *Sand Revolution* stipulation but less restrictive than a *Sotera* stipulation. *See Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24, 11–12 (PTAB June 16, 2020) (informative); *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12, 13–14 (PTAB Dec. 1, 2020) (precedential). While not rising to the level of a stipulation that the Interim Procedure indicates would preclude discretionary denial, Petitioner's stipulation does mitigate concerns about overlapping issues with the related litigation. *See* Interim Procedure 7–8. In addition, as Petitioner notes, the Petition addresses claims 15–29, which are not asserted in the related litigation. Pet. 65. In these circumstances, we find this factor weighs against exercising discretion to deny institution.

5. Overlap of Parties

The parties are the same as in the related litigation. *See* Pet. 66; Prelim. Resp. 19. Accordingly, this factor does not weigh against discretionary denial. *See Fintiv* at 13–14 (if the petitioner is unrelated to the defendant in the parallel proceeding, that might weigh against denial).

6. Other Circumstances

The final factor takes into account any other relevant circumstances, including the merits. "For example, if the merits of a ground raised in the petition seem particularly strong on the preliminary record, this fact has favored institution." *Fintiv* at 14–15. "[C]ompelling, meritorious challenges will be allowed to proceed at the PTAB even where district court litigation is proceeding in parallel." Interim Procedure 3–5.

Petitioner asserts that the strength of its proposed grounds weighs strongly in favor of institution. Pet. 66. Patent Owner asserts that the Petition's merits fail to show even the reasonable likelihood of success. Prelim. Resp. 20–22. We address the merits of Petitioner's challenges below. For the reasons we explain, Petitioner's challenges meet the "reasonable likelihood" standard that we apply in determining whether to institute. We decline to further characterize the Petition's merits. We accordingly treat this factor as neutral.

7. Summary

As discussed above, the third factor—investment in the parallel proceeding—weighs slightly in favor of denying institution, whereas the fourth factor—overlap of issues—weighs against exercising our discretion to deny institution. In these circumstances, we decline to exercise discretion under 35 U.S.C. § 314(a) to deny the Petition.

B. Discretion under 35 U.S.C. § 325(d)

Patent Owner contends we should deny institution under 35 U.S.C. § 325(d) because "the same or substantially the same prior art or arguments previously were presented to the Office." Prelim. Resp. 30. Specifically, Patent Owner explains, Kester was advanced in an office action and "applied

by [an] examiner against a limitation found in dependent claims 14 and 28." *Id*. at 31–32. "Despite considering Kester during prosecution of the '389 patent," Patent Owner notes, "the examiner did not identify Kester as disclosing or teaching any limitation of independent claims 1 and 15." *Id*. at 32.

In evaluating arguments under § 325(d), we use a two-part framework: (1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and (2) if either condition of the first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims. *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 8 (PTAB Feb. 13, 2020) (precedential).

Patent Owner has not demonstrated that this case satisfies the first part of the *Advanced Bionics* framework. It is undisputed that Petitioner's combination of references was not of record during the '389 patent's prosecution because two of the three references are new and Patent Owner does not assert those new references are cumulative to any that were already before the Office. *See* Prelim. Resp. 31–33. Thus, the same art was not previously before the Office. Nor has Patent Owner shown that the same or substantially the same arguments were previously presented to the office. Even if Patent Owner is correct that the examiner did not identify Kester as disclosing any particular limitation of the independent claims, it does follow that the examiner actually considered that issue. To the contrary, because the examiner concluded that other references taught the independent claims'

elements, there was no need to consider whether Kester did as well. *See* Ex. 1002, 158–59. In these circumstances, we decline to exercise our discretion to deny institution under § 325(d).

C. Claim Construction

Neither party proposes an express construction for any claim terms. Pet. 6; Prelim. Resp. 28–29. We agree that no claim terms require express construction to determine whether to institute *inter partes* review. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'" (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. Level of Ordinary Skill in the Art

Petitioner contends a skilled artisan would have had "a bachelor's degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience and would have had a working knowledge of host monitoring systems, software security analysis, and dynamic malware analysis." Pet. 6–7. Further, according to Petitioner, "[a]dditional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education." *Id.* Patent Owner's formulation for a skilled artisan is substantively similar. *See* Prelim. Resp. 29–30. Specifically, according to Patent Owner, a person of ordinary skill in the art "would have had a Bachelor's degree in an accredited program of Electrical Engineering, Computer Engineering, or Computer Science or in a similar discipline, and have 2-3 years of practical work or research experience in the general fields of electrical engineering, computer science, networking, communications,

and device and network security." *Id.* Patent Owner adds that "[m]ore advanced degrees and/or training in a related discipline can compensate for shorter work experience." *Id.* at 30.

For purposes of this Decision, we adopt Petitioner's proposal, which we find consistent with the level of skill reflected by the prior art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (the prior art may reflect an appropriate level of skill in the art). But, we note that we would have reached the same ultimate conclusion to institute review if we had adopted Patent Owner's proposal.

E. Description of Prior Art References

1. Kester (Ex. 1004)

Kester describes "monitoring and controlling application files" operating on computing devices. Ex. 1004 ¶¶ 3, 5. Figure 1 of Kester is reproduced below.

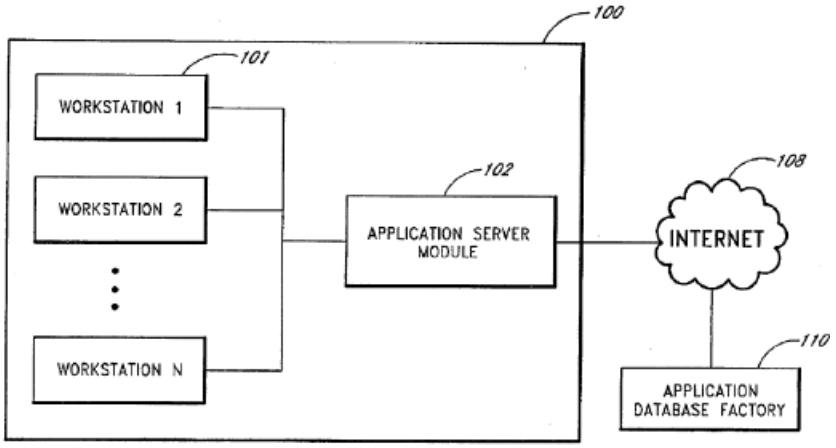

FIG. 1

Figure 1 "is a block diagram of a site collection system for controlling application files on a workstation." *Id.* ¶ 12. Multiple workstations 101, each of which includes a "workstation management module," are coupled to

application server module 102, which communicates via Internet 108 to upload and download applications with application database factory 110. *Id.* ¶¶ 35–39.

Each workstation management module maintains a "hash/policy table" that stores "the expected network activity" associated with various applications. *Id.* ¶¶ 39, 45. When an application that accesses the network is launched, the workstation management module calculates a hash for comparison with the hash/policy table. *Id.* ¶¶ 51–53. "If the hash and collection data correspond to a hash stored in the hash/policy table [] and the collection data associated with the hash in the hash/policy table [], . . . the policy associated with the hash is applied in response to the network access request." *Id.* ¶ 143. "For example, an access privilege can include allowing the launched application to run on the workstation." *Id.* ¶ 40.

"To determine the access privilege for the workstation 101 and/or user, the workstation management module 101 can utilize a predetermined association between the application and an expected network behavior or activity for the application." *Id.* ¶ 43. Such predetermined associations are made by a network administrator who "interfaces with the application server module 102 via [a] classification user interface" and "can classify uncategorized applications and/or recategorize previously categorized applications." *Id.* ¶ 71. In particular, the network administrator receives data from an application inventory database via the classification user interface and "select[s] or create[s] access privileges/policies/rules for users, workstation, and/or groups of users/workstations." *Id.* ¶ 72.

2. Kennedy (Ex. 1005)

Kennedy "pertains in general to computer security and in particular to detection [of] a computer worm and/or other type of malicious software." Ex. 1005, 1:7–9. Figure 4 of Kennedy is reproduced below.

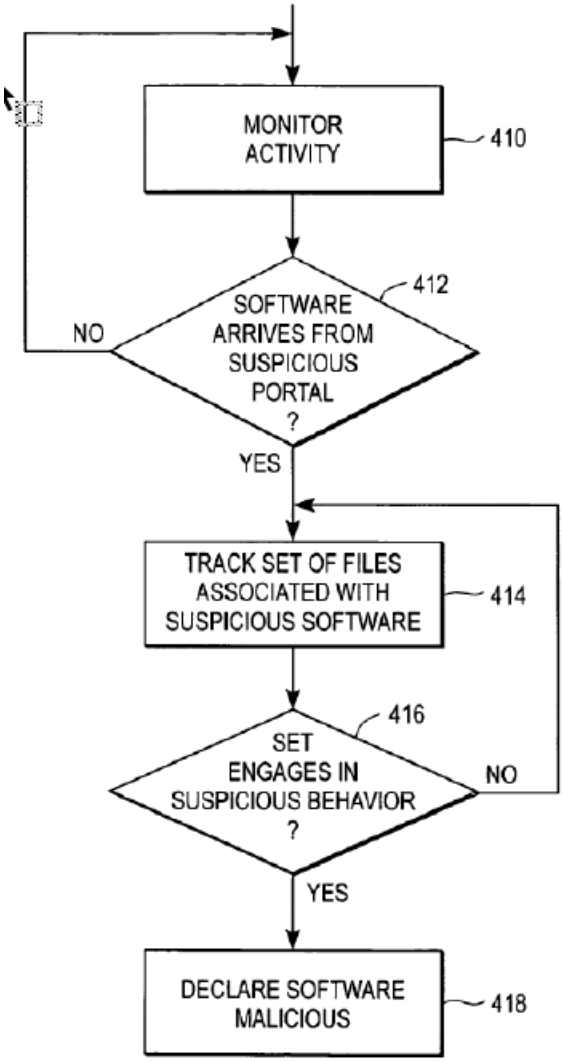

FIG. 4

Figure 4 is a flowchart illustrating steps of a "malicious software detection module (MSDM) [that] monitors a storage device of the computer system for the arrival of software from a suspicious portal." *Id.* at 1:41–47, 1:63–65.

While monitoring activity on a local storage device at step 410, the MSDM detects the arrival of new software and the portal through which the software arrived. *Id.* at 5:51–54. As checked at step 412, if the software arrived from a portal designated as suspicious, the MSDM designates the software itself as suspicious. *Id.* at 5:54–56. At step 414, the MSDM tracks files associated with the suspicious software and may create a logical set of files associated with the suspicious software. *Id.* at 5:57–61. As checked at step 416, if the files in the set (individually or collectively) engage in suspicious behavior, the MSDM declares the software as malicious at step 418 and takes corrective action. *Id.* at 5:64–6:2.

3. Honig (Ex. 1006)

Honig "relates to systems and methods for detecting anomalies in a computer system, and more particularly to an architecture and data format for using a central data warehouse and heterogeneous data sources." Ex. 1006, 1:44–47. Figure 1 of Honig is reproduced below.

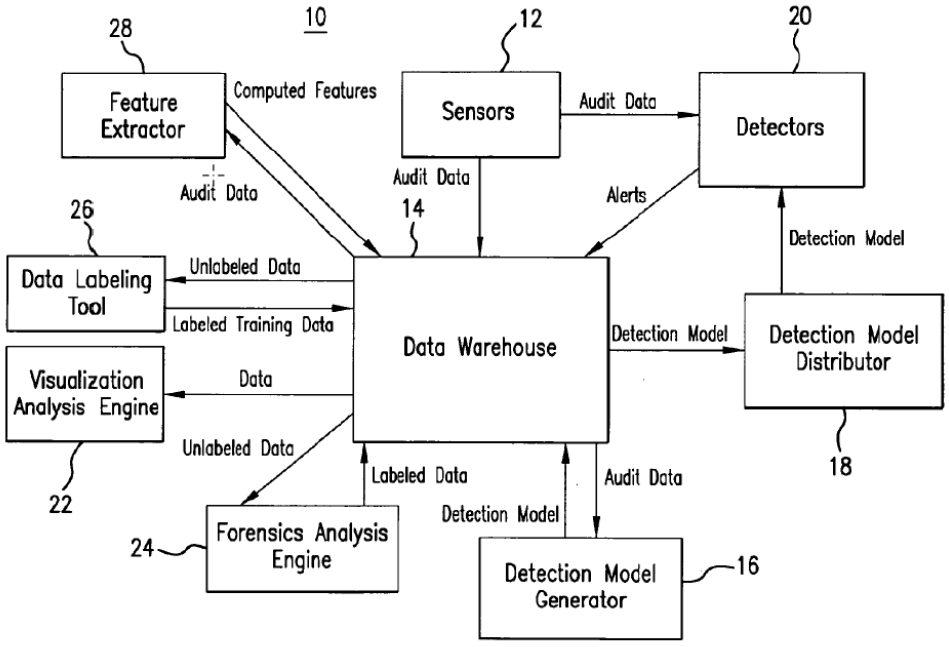

FIG. 1

Figure 1 illustrates an "adaptive model generation" system that "provides and automates many of the critical processes in the deployment and operation of real time data mining-based intrusion detection systems." *Id.* at 6:50–54, 7:53–54. The system "abstract[s] the processes of data collection, data aggregation, detection model evaluation, detection model generation, and model distribution," and "uses a general XML-based data and model representation scheme that facilitates the translation of data from what is collected at the audit stream to the form necessary for generation of detection models." *Id.* at 6:54–63.

Sensors 12 gather information from an environment and send the data to data warehouse 14, which is accessed by detection model generators 16 to "generate models that classify activity as either malicious or normal." *Id.* at 8:14–18. Model distributor 18 deploys the model to real-time detector 20, which uses the model to evaluate audit data received from sensors 12 to detect intrusions. *Id.* at 8:19–24. Data analysis engines 22, 24, 26, 28 retrieve data from data warehouse 14, allowing for "implement[ation of] many systems that are helpful in the deployment of an intrusion detection system." *Id.* at 8:25–33. Honig describes at least three general types of model-detection algorithms that its architecture may support: "misuse detection," which trains on labeled normal and attack data; "supervised (traditional) anomaly detection," which trains on normal data; and "unsupervised anomaly detection," which trains on unlabeled data. *Id.* at 20:33–38.

F. Obviousness Analysis

1. Ground 1: Obviousness based on Kester and Kennedy

In its first unpatentability ground, Petitioner contends that claims 1–13, 15–27, 29, and 30 would have been obvious over Kester and Kennedy. Pet. 13–48. Based on the present record and for the reasons explained below, we determine that Petitioner has demonstrated a reasonable likelihood of success in proving that claims 1–13, 15–27, 29, and 30 would have been obvious over Kester and Kennedy.

a) Petitioner's Proposed Combination of Kester and Kennedy

Petitioner relies primarily on Kester for teaching receiving and storing information about events, as well as an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed, as the challenged claims require. Pet. 13–21. Kester also teaches, Petitioner explains, the claimed correlation and comparison between different objects received from two computers. *Id.* at 21–26. According to Petitioner, "Kester does not detail that identifying an application's relationship to another application is part of the process of determining whether received collection data indicates that an application is malware." *Id.* at 27. "However," Petitioner explains, "*Kennedy* teaches this concept" and one skilled in the art would have been motivated to include Kennedy's monitoring in Kester because it "would have made *Kester's* method/system more desirable and more effective in identifying malicious/rogue programs (malware), thereby improving similar malware detection method/systems in the same way." *Id.* at 27, 30.

Patent Owner challenges several aspects of Petitioner's asserted combination. *See* Prelim. Resp. 43–63. We address those issues below.

b) Whether Kester is Analogous Art

Patent Owner argues that Kester is not analogous to the '389 patent because the '389 patent relates to "rapid determination of whether an object is safe or malware" whereas Kester relates more broadly to "monitoring and controlling application files" on computers. Prelim. Resp. 44–45. On this record, we disagree that Kester is not analogous. As Petitioner notes, Kester is in the same field of endeavor as the '389 patent's claimed invention because both relate to classifying computer objects as malware. *See* Pet. 9–10 (citing Ex. 1001, 1:10–12, claims 1, 15; Ex. 1004 ¶¶ 98, 79 82, 134, Fig. 4A). That is true even though, as Patent Owner argues, Kester also includes additional classifications beyond just malware. *See* Prelim. Resp. 44–45. In addition, we agree with Petitioner that "Kester is also reasonably pertinent to certain problems addressed by the '389 Patent such as the need to initially classify an object as not malware, generate a mask for the object that defines acceptable behavior for the object, and reclassify the object if the actual monitored behavior extends beyond the mask." Pet. 10 (citing Ex. 1001, 4:25–36, 14:61–15:10, claims 14 and 28; Ex. 1004 ¶¶ 76, 179–181, claims 1, 2). Although, as Patent Owner contends, Kester's solution (a human reviewer), is different from the '389 patent's solution (automated detection), *see* Prelim. Resp. 49–51, that does not distinguish the common problem that both address—i.e., classifying objects as malware. Because Kester is in the same field of endeavor as the '389 patent and is reasonably pertinent to problems addressed in the '389 patent, we agree with Petitioner that Kester is analogous prior art. *See In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004).

c) Comparing Data to Identify Relationships and Petitioner's Rationale for Combining References

Independent claim 1 recites "comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and classifying, by the base computer, the computer object as malware on the basis of said comparison." Ex. 1001, 20:56–62. Independent claim 15 recites similar comparing and classifying steps. *See id*. at 22:34–41. According to Petitioner, the combined Kester-Kennedy system teaches this feature because "[i]n *Kester*, the application server module 102 and/or application database factory 110 receives collection data from each workstation, merges that data, and uses that merged collection data (i.e., *correlated data about the computer object received from the first and second remote computers*) to determine a group/category for the application." Pet. 24. Further, Petitioner explains, Kennedy teaches "identifying an application's relationship to another application is part of the process of determining whether received collection data indicates that an application is malware." *Id*. at 27. Petitioner goes on to explain that one skilled in the art would have been motivated to include Kennedy's monitoring in Kester because it "would have made *Kester's* method/system more desirable and more effective in identifying malicious/rogue programs (malware), thereby improving similar malware detection method/systems in the same way." *Id*. at 30.

Patent Owner argues that Petitioner's obviousness challenge fails because in Kester, a network administrator performs the claimed comparison, rather than a base computer as claimed. Prelim. Resp. 53, 54. Further, Patent Owner asserts, Kennedy is deficient because it lacks the

claimed base computer. *See id*. at 53. We disagree with Patent Owner's argument at this stage because it attacks the references individually rather than addressing the asserted combination, as set forth in the Petition. Specifically, Petitioner relies on Kester for teaching the claimed base computer and on Kennedy for teaching the claimed comparison. *See* Pet. 19, 27–28. Thus, it does not matter that neither reference alone teaches the claimed comparison by a base computer. On this record, we agree with Petitioner that the combined system teaches a base computer that performs the claimed comparison and classification steps.

Patent Owner next challenges Petitioner's rationale for combining references. According to Patent Owner, a skilled artisan would not have combined Kester with Kennedy because Kester's human administrator is incompatible with Kennedy's automated process. Prelim. Resp. 55–56. Patent Owner asserts that Petitioner's proposed combination disregards Kester's improved accuracy, a benefit that results from Kennedy's human reviewer performing manual analysis. *Id*. at 56–59.

We disagree with Patent Owner's arguments. First, these arguments do not undermine the efficiency benefits that would come with Kennedy's automation, even if that efficiency might come with a tradeoff—i.e., losing a human reviewer's accuracy and flexibility. *See Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000) ("The fact that the motivating benefit comes at the expense of another benefit, however, should not nullify its use as a basis to modify the disclosure of one reference with the teachings of another."). Second, Petitioner does not need to show that replacing Kester's human administrator with Kennedy's automated process "was an improvement in a categorical sense." *See Intel Corp. v. PACT XPP*

Schweiz AG, 61 F.4th 1373, 1381 (Fed. Cir. 2023) (internal quotation omitted). Rather, there is a motivation to combine when, as here, "a known technique 'has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way.'" *Id*. at 1380 (quoting *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007)).

Last, Patent Owner contends that one skilled in the art would not have had a reasonable expectation of success in combining the references as Petitioner proposes because Kennedy teaches performing heuristics on multiple remote user computers, whereas Kester implements its classification process on a single centralized computer. Prelim. Resp. 61–63. Patent Owner asserts that "Petitioner fails to . . . contend with the practical challenges associated with combining two very different approaches." *Id*. at 61. On this record, we disagree. Although Patent Owner identifies differences between the two systems, Patent Owner does not identify any actual incompatibilities or difficulties that might result from running Kennedy's comparison algorithm Kester's single base computer, as Petitioner proposes. *See id*. at 61–63. On the other side, Petitioner presents evidence from Dr. Lee that one skilled in the art would have had a reasonable expectation of success in combining the references as Petitioner proposes, and that the combination "would have been accomplished using known methods and with no change to their respective functions." Ex. 1004 ¶ 118. On this record, we agree with Petitioner that "since file set tracking and behavior monitoring was a well-known way to detect the presence of malware, there would have been a reasonable expectation of

success configuring *Kester's* application file monitoring system/method to perform *Kennedy's* file set tracking and behavior monitoring." Pet. 31.

d) Ground 1 Summary

Other than as outlined above, Patent Owner does not additionally challenge Petitioner's obviousness analysis at this stage. We have reviewed Petitioner's arguments and the underlying evidence cited in support and are persuaded that, at this stage, Petitioner sufficiently demonstrates a reasonable likelihood of succeeding in its obviousness challenge to claims 1–13, 15–27, 29, and 30 based on Kester and Kennedy.

2. Ground 2: Obviousness based on Kester, Kennedy, and Honig

In its second unpatentability ground, Petitioner contends that claims 14 and 28 would have been obvious over Kester, Kennedy, and Honig. Pet. 48–63. This ground adds Honig for teaching the additional limitation in dependent claims 14 and 28 requiring a mask that defines acceptable behavior and reclassifying formerly acceptable objects as malware when they go beyond the permitted behavior. *See id*. Specifically, as Petitioner explains, "Kester describes a process by which a human administrator classifies application files based on certain collected data, and Ground 2 proposes that a PHOSITA would have been motivated to automate this process pursuant to Honig's machine learning teachings." *Id*. at 51. Other than as outlined above, Patent Owner does not additionally challenge Petitioner's Ground 2 obviousness analysis at this stage. We have reviewed Petitioner's arguments and the underlying evidence cited in support and are persuaded that, at this stage, Petitioner sufficiently demonstrates a reasonable likelihood of succeeding in its obviousness challenge to claims 14 and 28 based on Kester, Kennedy, and Honig.

III. CONCLUSION

After considering the evidence and arguments presented in the current record, we determine that Petitioner has demonstrated a reasonable likelihood of success in proving that at least one of the challenged claims of the '389 patent is unpatentable. We therefore institute trial on all challenged claims and grounds raised in the Petition. At this stage of the proceeding, we have not made a final determination as to the patentability of any challenged claim or as to the construction of any claim term. Any final determination will be based on the record developed during trial. We place Patent Owner on express notice that any argument not asserted in a timely-filed Response to the Petition, or in another manner permitted during trial, may be deemed waived, even if that argument was presented in the Preliminary Response.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–30 of the '389 patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '389 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

For PETITIONER:

Adam Seitz
Paul Hart
ERISE IP, P.A.
adam.seitz@eriseip.com
paul.hart@eriseip.com

For PATENT OWNER:

Brian Eutermoser
Russell E. Blythe
Mikaela Stone
KING & SPALDING LLP
beutermoser@kslaw.com
rblythe@kslaw.com
mikaela.stone@kslaw.com