

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SOPHOS LTD. & SOPHOS INC.,
Petitioner,

v.

OPEN TEXT INC.,
Patent Owner.

IPR2023-00699
Patent 8,418,250 B2

Before MICHELLE N. WORMMEESTER, AARON W. MOORE, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

RAEVSKY, *Administrative Patent Judge*.

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

I. INTRODUCTION

Sophos Ltd. and Sophos Inc. (collectively, “Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claims 1–30 of U.S. Patent No. 8,418,250 B2 (Ex. 1001, “the ’250 patent”). Pet. 1. Open Text Inc. (“Patent Owner”) filed a Preliminary Response (Paper 13, “Prelim. Resp.”).

Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless it is determined that there is a reasonable likelihood that the petitioner would prevail with respect to at least one of the claims challenged in the petition. After considering the parties’ arguments and evidence, and for the reasons set forth below, Petitioner demonstrates a reasonable likelihood of prevailing with respect to at least one of the challenged claims of the ’250 patent. Accordingly, we institute an *inter partes* review with respect to all challenged claims and grounds asserted in the Petition. 37 C.F.R. § 42.108(a) (2022).

Our factual findings and conclusions at this stage of the proceeding are based on the evidentiary record developed thus far. This is not a final decision as to patentability of the challenged claims.

II. BACKGROUND

A. Related Matters

The parties identify the following infringement lawsuits involving the ’250 patent: *Webroot Inc, et al. v. Sophos Ltd.*, No. 6:22-cv-00240-ADA-DTG (W.D. Tex.); *Webroot, Inc. et al. v. Trend Micro, Inc.*, No. 6:22-cv-00239-ADA-DTG (W.D. Tex.); *Webroot, Inc. et al. v. CrowdStrike Holdings, Inc. et al.*, No. 6:22-cv-00241-ADA-DTG (W.D. Tex.); and

Webroot, Inc. et al. v. AO Kaspersky Lab, No. 6:22-cv-243-ADA-DTG (W.D. Tex.) (collectively, the “related District Court litigation”). Pet. 3–4; Paper 4, 1.

The following *inter partes* reviews have also been filed against the ’250 patent: *CrowdStrike, Inc. v. Open Text Inc.*, IPR2023-00289 (PTAB Dec. 29, 2022; instituted July 21, 2023); *Trend Micro Inc. v. Open Text Inc.*, IPR2023-00655 (PTAB Mar. 2, 2023).

B. Real Parties-in-Interest

Sophos Ltd. and Sophos, Inc. identify themselves as the only real parties-in-interest (RPI) for Petitioner. Pet. 3. Patent Owner identifies Open Text Inc. and Webroot LLC as RPIs, as well as affiliates Carbonite, LLC, Open Text Corporation, and Open Text Holdings, Inc. Paper 4, 1.

C. The ’250 patent

The ’250 patent “relates generally to methods and apparatus for dealing with malware.” Ex. 1001, 1:4–5. Figure 2 of the ’250 patent is reproduced below.

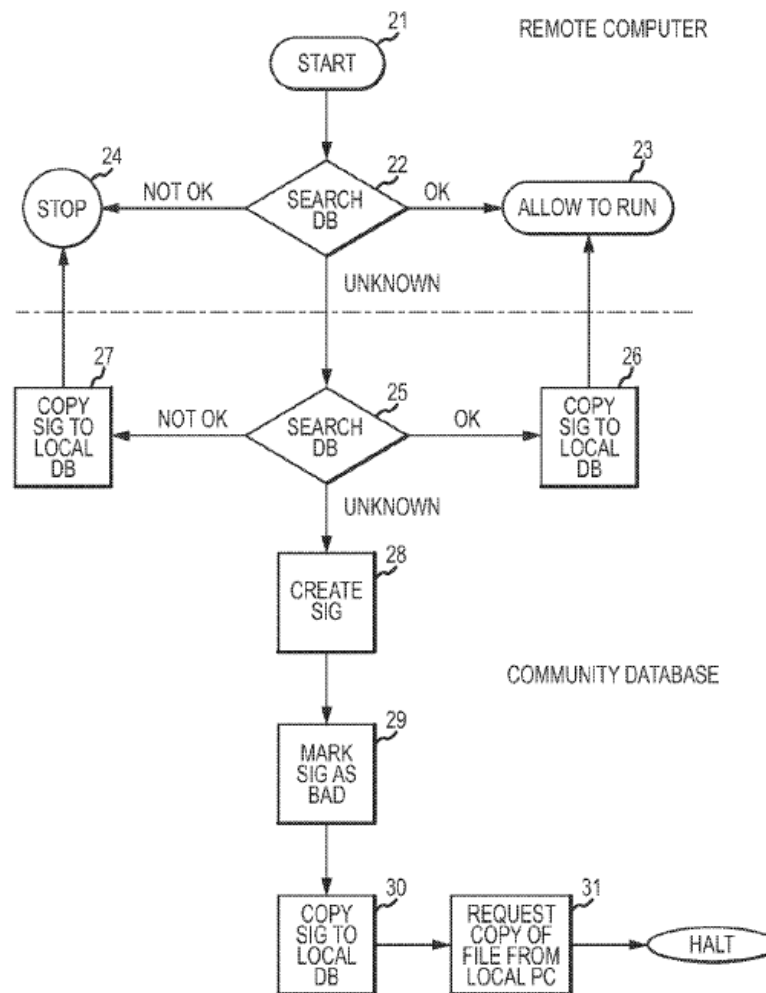


FIG.2

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 7:46–48, 8:17–18. 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 8:18–24. 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 8:24–33.

If the object is unknown locally, details are passed over a network, such as the Internet, for storage in, and comparison with, a community database that stores signatures representative of objects from multiple remote computers. *Id.* at 8:44–47. Such a community database is searched at step 25 for a signature for the object that has already been stored. *Id.* at 8:47–50. If a corresponding signature is 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 a corresponding signature is found and identified as unsafe, a copy is provided to the remote computer with such a designation at step 27. *Id.* at 8:60–9:10. 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 9:11–17. Such an unsafe designation may be changed as experience with the object is collected. *See id.* at 9:26–39.

D. Challenged Claims

Claim 1, below, is illustrative of the challenged claims. Petitioner’s claim element labels are included for reference.

1. A method of classifying a computer object as malware, the method comprising:

[a] at a base computer, receiving data about a computer object from each of plural remote computers on which the object or

similar objects are stored, the data including information about the behaviour of the object running on one or more remote computers;

[b] determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware;

[c] classifying the computer object as malware when the data indicates that the computer object is malware;

[d] when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware;

[e] automatically generating a mask for the computer object that defines acceptable behaviour for the computer object, wherein the mask is generated in accordance with normal behaviour of the object determined from said received data;

[f] running said object on at least one of the remote computers; automatically monitoring operation of the object on the at least one of the remote computers;

[g] allowing the computer object to continue to run when behaviour of the computer object is permitted by the mask;

[h] disallowing the computer object to run when the actual monitored behaviour of the computer object extends beyond that permitted by the mask; and,

[i] reclassifying the computer object as malware when the actual monitored behaviour extends beyond that permitted by the mask.

Ex. 1001, 20:19–50.

E. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability (Pet. 9):

Claim(s) Challenged	35 U.S.C. § ¹	Reference(s)/Basis
1, 2, 12–14, 24	103	Halperin, ² Mankins ³
1–30	103	Halperin, Mankins, Kirby ⁴

Petitioner relies on the declaration of Dr. Richard Newman (Ex. 1004).
Patent Owner relies on the declaration of Dr. Nenad Medvidovic (Ex. 2001).

III. ANALYSIS

A. Discretion under 35 U.S.C. § 314(a)

Patent Owner argues that we should exercise discretion under § 314(a) to deny institution in light of the related District Court litigation. Prelim. Resp. 3–23.

We consider the following factors when determining whether to deny institution under § 314(a) based on a parallel district court 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;

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011), revised 35 U.S.C. §§ 102, 103 effective March 16, 2013. The ’250 patent was filed before March 16, 2013, so we apply the pre-AIA versions of §§ 102, 103. Ex. 1001, code (22).

² U.S. Publication No. 2004/0111632 A1 to Halperin, published June 10, 2004 (Ex. 1006).

³ U.S. Patent No. 7,900,194 B1 to Mankins, issued Mar. 1, 2011 (Ex. 1008).

⁴ U.S. Patent No. 7,694,150 B1 to Kirby, issued Apr. 6, 2010 (Ex. 1007).

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.

Apple Inc. v. Fintiv, Inc., IPR2020-00019, Paper 11 at 5–6 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”). We also consider “several clarifications” made by the Director of the United States Patent and Trademark Office (“USPTO”). See USPTO Memorandum, Interim Procedure for Discretionary Denials in AIA Post Grant Proceedings with Parallel District Court Litigation, 2 (June 21, 2022) (“Interim Procedure”).⁵

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. Although Patent Owner asserts that a 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

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

favor of exercising authority to deny institution.” *Fintiv* at 9. The current scheduled trial date is August 19, 2024. *See* Ex. 1014, 6; Pet. 64; Prelim. Resp. 12. A final written decision in this case will issue no later than mid-October, 2024. Thus, the district court’s trial date is less than two months 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 because the trial date is the same for each defendant in five separate lawsuits with dozens of asserted patents. Pet. 65–66. In these circumstances, we treat this factor as neutral. *Cf. Cizion, LLC v. Kerr Machine Co.*, PGR2020-00065, Paper 10 at 26 (PTAB Dec. 3, 2020) (finding this factor neutral when the trial date was set three months prior to the anticipated final decision deadline, but the trial date was uncertain due to related trials being scheduled at the same time).

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 because the parties have already engaged in extensive discovery. Prelim. Resp. 14–17. 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. 1014, 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 the present petition, Petitioner[] will not assert that the challenged claims are invalid on the instituted grounds in the related litigation, nor any other possible prior art printed publication grounds based on the references in Grounds 1 and 2.” Pet. 68. This is broader than a *Sand Revolution* stipulation but somewhat less restrictive than a *Sotera* stipulation. See *Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24 at 11–12 (PTAB June 16, 2020) (informative); *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 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. We find this factor weighs against exercising discretion to deny institution.

5. *Overlap of Parties*

“If a petitioner is unrelated to a defendant in an earlier court proceeding, the Board has weighed this fact against exercising discretion to deny institution.” *Fintiv* at 13–14. Here, the parties are the same as in the related litigation. See Pet. 68–69; Prelim. Resp. 20–22. Accordingly, this factor does not weigh against exercising discretion to deny institution.

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. 69. Patent Owner asserts that the Petition’s merits fail to show even a reasonable likelihood of success. Prelim. Resp. 22–23. We address the merits of Petitioner’s challenges below. For the reasons we explain there, 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*

Based upon a holistic review of the above factors, we decline to exercise discretion under 35 U.S.C. § 314(a) to deny the Petition.

B. Principles of Law

Petitioner bears the burden to demonstrate unpatentability, and that burden never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

A claim is unpatentable as obvious if “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting 35 U.S.C. § 103(a)). We resolve the question of obviousness based on underlying factual determinations, including: (1) the scope and content of

the prior art; (2) any differences between the prior art and the claims; (3) the level of skill in the art; and (4) when in evidence, objective indicia of nonobviousness. *See Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966).

We apply these principles to the Petition’s challenges.

C. Level of Ordinary Skill in the Art

We review the grounds of unpatentability in view of the understanding of a person of ordinary skill in the art at the time of the invention. *Graham*, 383 U.S. at 13, 17. Petitioner asserts that

A person of ordinary skill in the art (“POSITA”) in June 2005 would have had at least a Bachelor’s degree in Computer Science, Computer Engineering, Electrical Engineering, or an equivalent discipline, and at least two years’ worth of experience developing dynamic malware detection and computer networking or network architecture, or a Master’s degree in a related field. Alternately, a POSITA could have four or more years of work experience in computer networking and in the development of client-server systems and dynamic malware detection.

Pet. 11 (citing Ex. 1004 § 17).

Patent Owner defines the level of skill as follows:

A person of ordinary skill in the art at the time of the invention . . . 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 would have had 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. . . . More advanced degrees or training in a related discipline or both can compensate for shorter work experience.

Prelim. Resp. 29 (citing Ex. 2001 ¶¶ 50–54). Patent Owner does not explain at this stage why its proffered level of skill differs from Petitioner’s. We note that both definitions are largely similar.

We are persuaded, on the present record, that Petitioner’s proposal is consistent with the problems and solutions in the ’250 patent and prior art of record. We thus adopt Petitioner’s definition of the level of skill for the purposes of this decision. Our decision would not have changed had we adopted Patent Owner’s definition of the level of skill.

D. Claim Construction

In *inter partes* review, we construe a claim using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b).

The parties do not propose any claim constructions. *See* Pet. 9–10; Prelim. Resp. 28–29. As no terms are in dispute, we determine that no terms require construction at this stage. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368 (Fed. Cir. 2019) (“The Board is required to construe ‘only those 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))).

E. Asserted Obviousness over Halperin and Mankins (Ground 1)

Petitioner contends that claims 1, 2, 12–14, and 24 would have been obvious over Halperin and Mankins. Pet. 17–44.

1. Overview of Halperin

Halperin discloses “detecting malicious activity in a computer network.” Ex. 1006, code (57). Halperin’s Figure 6 is reproduced below.

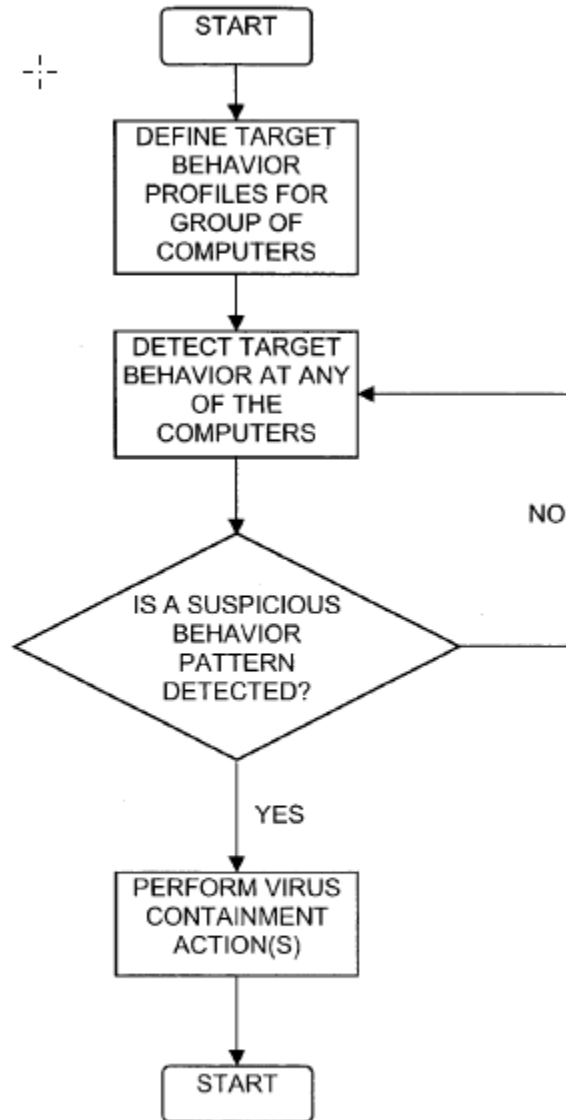


Fig. 6

Figure 6 is an “exemplary method of operation” of Halperin’s “computer virus detection and containment system.” Ex. 1006 ¶¶ 15, 16.

2. *Overview of Mankins*

Mankins discloses Kernel-based intrusion detection using Bloom filters. Ex. 1004, code (57). In one of many possible embodiments for detecting an intrusion attack, a Bloom filter is provided and used to generate a Bloom filter data object. *Id.* The Bloom filter data object contains data representative of expected system-call behavior associated with a computer program. *Id.* The Bloom filter data object is embedded in an operating system (“OS”) kernel upon an invocation of the computer program. *Id.* Actual system-call behavior is compared with the data in the Bloom filter data object. *Id.*

3. *Independent claim 1*

a. *Undisputed limitations*

Petitioner asserts that, to the extent the preamble is limiting,⁶ Halperin teaches or suggests it by disclosing, for example, “malicious software detection algorithms.” Pet. 24 (citing Ex. 1006 ¶ 74; Ex. 1004 ¶¶ 72–73).

Petitioner relies on both Halperin and Mankins for the limitation “[d] when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware.” *Id.* at 29–30 (citing Ex. 1004 ¶¶ 83–86). For example, in Halperin, Petitioner argues, virus containment actions are initiated (or not) depending on whether “correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior.” *Id.* at 29 (citing Ex. 1006, *passim*; Ex. 1004 ¶¶ 84–85). A POSITA would have understood that an object would be

⁶ We need not determine whether the preamble is limiting because on this record, Halperin likely discloses it.

classified as not malware if the correlated data does not correspond to a suspicious behavior pattern, Petitioner argues. *Id.* (citing Ex. 1004 ¶ 85).

For the limitation, “[f] running said object on at least one of the remote computers; automatically monitoring operation of the object on the at least one of the remote computers,” Petitioner relies on Mankins. *Id.* at 35–38 (citing Ex. 1004 ¶¶ 98–101). Petitioner points to Figure 3 of Mankins, arguing that in step 320, Mankins discloses “behavior of the computer program is monitored as it is executed by the computer 110.” *Id.* at 36 (citing Ex. 1008, 11:63–65).

For the limitation, “[g] allowing the computer object to continue to run when behaviour of the computer object is permitted by the mask,” Petitioner also relies on Mankins. *Id.* at 38–40 (citing Ex. 1004 ¶¶ 102–105). Petitioner contends that “[a]s long as the monitored system-call sequences have a match” in Mankins’ Bloom filter data object, the “operation is considered to be normal” and “the object or program will be permitted to continue to run.” *Id.* at 39 (citing Ex. 1008, 1:60–63, 2:8–10; Ex. 1004 ¶ 103).

Finally, for the limitation, “[h] disallowing the computer object to run when the actual monitored behaviour of the computer object extends beyond that permitted by the mask,” Petitioner relies on the combination of Halperin and Mankins. *Id.* at 40–41 (citing Ex. 1004 ¶¶ 106–108). According to Petitioner, if Mankins’ system does not find a match in the Bloom filter data object for a computer’s actions, “the observed system-call sequence is determined to be anomalous and may indicate an intrusion attempt,” and an alert is issued. *Id.* (citing Ex. 1008, 6:39–41, 12:7–14). Petitioner further contends that it would have been obvious to disallow the program from

running in light of Halperin’s disclosure that if suspicious behavior is detected, “the system can . . . initiate virus containment actions.” *Id.* at 41 (citing Ex. 1006 ¶ 90; Ex. 1004 ¶ 108).

Patent Owner does not dispute Petitioner’s argument regarding the preamble and these limitations at this stage. On this record, we agree with Petitioner that the combination of Halperin and Mankins likely teaches or suggests the preamble and these limitations.

b. [a] at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored, the data including information about the behaviour of the object running on one or more remote computers

Petitioner contends that Halperin discloses or renders obvious this limitation. Pet. 25–27 (citing Ex. 1004 ¶¶ 74–77). Petitioner asserts that Halperin discloses a base computer (“server 502”) that receives data about a computer object (“target behavior information” associated with a potential “virus”) from remote computers (“computers 500”). *Id.* at 25 (citing Ex. 1006 ¶¶ 36–37, 47) (emphasis omitted).⁷ Petitioner also asserts that a POSITA would have understood the “target behavior” and predefined suspicious events detected by Halperin’s computers and received by the server 502 to be “data about a computer object (*i.e.*, a potential **virus**).” *Id.* at 27 (citing Ex. 1006 ¶ 47; Ex. 1004 ¶ 77). In a similar vein, Petitioner argues that a POSITA would have understood Halperin’s “information regarding target behavior detected” at the computers 500 to include

⁷ We omit Petitioner’s text coloring throughout this Decision.

information about the behaviour of the object (i.e., a potential virus) running on one or more remote computers. *Id.*

Patent Owner disputes that Petitioner shows Halperin discloses or renders obvious “receiving data about a computer object” because “Petitioner does not explain how Halperin operates on individual objects.” Prelim. Resp. 46. Asserting that “[t]he ’250 patent’s object-focused approach distinguishes it from Halperin,” Patent Owner contends that “Halperin . . . examines aggregate, collective computer behavior for signs of a viral outbreak—without focusing on individual programs.” *Id.* at 46–47 (citing Ex. 2001 ¶¶ 55–63). “Halperin does not collect data about what objects perform what actions,” Patent Owner contends. *Id.* at 47. Rather, Patent Owner argues, “Halperin operates more like a trip wire, logging each instance of when a certain event is performed by a computer, as captured by a sensor.” *Id.* (citing Ex. 2001 ¶ 97).

Along those lines, Patent Owner views Halperin as teaching logging data about the computer’s or network’s behavior, detecting “many things that are not particular to any computer object.” *Id.* at 48 (citing Ex. 2001 ¶ 99). “Petitioner simply ignores that Halperin’s network-level behavior correlation uses different processes,” Patent Owner contends, “in pursuit of a different purpose, from those reflected in the ’250 patent’s object-centric approach.” *Id.* at 49. “Nothing about the system according to Halperin requires knowing what computer object is responsible for that activity,” Patent Owner asserts. *Id.* at 50. Thus, Patent Owner argues, Halperin’s “data is object agnostic.” *Id.*

At this stage, we find Petitioner’s arguments more persuasive. We agree with Petitioner, on this record, that Halperin’s disclosure of receiving

“target behavior information” associated with a potential “virus” teaches “receiving data about a computer object.” *See* Pet. 25 (citing Ex. 1004 ¶¶ 74–77; Ex. 1006 ¶¶ 36–37, 47). Claim 1 specifies that the data about the computer object “include[s] information about the behavior of the object running on one or more remote computers.” Halperin’s collected behavior information is data about the behavior of a virus running on the remote computers. Halperin teaches, for example, that “[a] computer virus can thus be detected by correlating behavior and/or data from different computers.” Ex. 1006 ¶ 37. Correlating this behavior data can result in determining that the behavior “corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers.” *Id.* ¶ 47.

Petitioner maps Halperin’s disclosed virus to the claimed “computer object.” Pet. 25, 27 (citing, e.g., Ex. 1004 ¶ 77). Patent Owner does not appear to dispute that Halperin’s virus is a computer object. *See* Prelim. Resp. 46–50. The ’250 patent refers to an object as follows: “[a]n object in this sense may be a computer file, part of a file or a sub-program, macro, web page or any other piece of code to be operated by or on the computer, or any other event whether executed, emulated, simulated or interpreted.” Ex. 1001, 7:63–66. Although we take no position at this stage on whether the specification defines “object” in this passage, Halperin describes viruses as “malicious software” and “malicious code,” which match the ’250 patent’s description of an object (e.g., “any other piece of code”). *Id.*; Ex. 1006 ¶¶ 73, 87.

At this stage, we are not persuaded by Patent Owner’s assertions that Halperin does not “operate[] on individual objects,” that “[t]he ’250 patent’s

object-focused approach distinguishes it from Halperin,” that Halperin does not “focus[] on individual programs,” that “Halperin does not collect data about what objects perform what actions,” and that Halperin’s system does not “require[] knowing what computer object is responsible for that activity.” Prelim. Resp. 46–47, 50. These statements are unavailing at this stage because they are not commensurate with the scope of claim 1. *See In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998) (“[The] proffered facts . . . are not commensurate with the claim scope and are therefore unpersuasive.”). Claim 1 does not recite “operat[ing] on individual objects,” an “object-focused approach,” “collect[ing] data about what objects perform what actions,” or “focus[ing] on individual programs.” Claim 1 also does not “require[] knowing what computer object is responsible for that activity.” Instead, limitation 1[a] broadly recites “receiving data *about* a computer object,” which we preliminarily determine above that Halperin discloses.⁸

On this record, we agree with Petitioner that Halperin likely discloses or suggests limitation 1[a].

⁸ This case is distinguishable from *Sophos Ltd. v. Open Text Inc.*, IPR2023-00633, Paper 20 (PTAB Sept. 12, 2023), which denied institution on a related patent (U.S. Pat. 8,726,389 B2) over similar Halperin-based grounds. There, the Board found that Halperin does not disclose “receiving . . . information including at least an identity of an object.” IPR2023-00633, Paper 20 at 9. Claim 1 here does not require receiving “an identity of an object.”

- c. [b] determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware*

For this limitation, Petitioner relies on Halperin. Pet. 27–28 (citing Ex. 1004 ¶¶ 78–79). According to Petitioner, Halperin discloses that the base computer “determine[s] whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers.” *Id.* (citing Ex. 1006 ¶ 47). An “indication that a computer virus may have infected those computers” is an example of the claimed indication “that the computer object is malware,” Petitioner asserts. *Id.* at 28 (citing Ex. 1004 ¶ 79).

Patent Owner contends that Halperin does not make “determin[ations] in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware.” Prelim. Resp. 50. In Patent Owner’s view, Halperin concludes that “a computer virus *may* have infected those *computers*,” and therefore “does not identify the virus itself, much less an object that might be malicious, as the claims require.” *Id.* at 51. Patent Owner asserts that Petitioner’s reliance on the “same false equivalence between objects and computer behavior” for this limitation fails for the same reasons as in the preceding limitation. *Id.* at 52.

On this record, Petitioner is more convincing. We agree that Halperin’s determination that its identification of suspicious behavior “as an indication that a computer virus may have infected those computers” is an example of the claimed indication “that the computer object is malware.” Pet. 28. Patent Owner again relies on an unclaimed limitation, which is

unpersuasive. The claim does not require “identify[ing] the virus itself,” as Patent Owner asserts, but only determining that the received data “indicates that the computer object is malware.” *See* Prelim. Resp. 51.

Accordingly, on this record, we agree with Petitioner that Halperin likely discloses limitation 1[b].

d. [c] classifying the computer object as malware when the data indicates that the computer object is malware

Petitioner again relies on Halperin for this limitation. Pet. 28–29 (citing Ex. 1004 ¶¶ 80–82). According to Petitioner, Halperin discloses, for example, “identify[ing] malicious code (from here on referred to as ‘viruses’).” *Id.* at 28 (citing Ex. 1006 ¶ 87). Petitioner also cites Halperin paragraph 73, which states that “malicious software has been identified.” *Id.* at 28; Ex. 1006 ¶ 73. Further, Petitioner quotes Halperin’s disclosure referring to “automatic identification of suspicious activity by a server . . . and approval by [an] operator that the suspicious activity is truly a virus.” Pet. 28 (citing Ex. 1006 ¶ 61). Petitioner also contends that “[a] POSITA would have further understood that when Halperin takes actions responsive to the detection of a virus, . . . it is because the system has classified the computer object as malware.” *Id.* at 28–29 (citing Ex. 1006 ¶ 90; Ex. 1004 ¶ 82).

Patent Owner contends that “Halperin’s detection of potential viral *activity* and initiation of an alarm or containment actions does not mean Halperin discloses or renders obvious *classifying* any particular object as *malware*.” Prelim. Resp. 52. Patent Owner views Petitioner’s quotations from Halperin as merely referring to the detection of virus activity, not “determining whether a particular object is malware, much less classifying it

as such.” *Id.* at 53–54 (citing Ex. 2001 ¶¶ 106–108). Patent Owner further disputes Petitioner’s contention that a POSITA would have understood Halperin’s actions responsive to virus detection to occur “because the system has classified the computer object as malware.” *Id.* at 55. Patent Owner charges Petitioner with making an inherency argument, but an unsupported, conclusory one. *Id.* In Patent Owner’s view, Halperin’s “disclosure of actions taken to *contain* a possible virus on a network does not inherently disclose or indicate to a POSITA that Halperin has *classified* any particular object as malware,” and particularly so “where none of the remedial containment actions Halperin discloses requires knowledge that a particular object might be or is in fact malware.” *Id.* at 56 (citing Ex. 1006 ¶¶ 48–56; Ex. 2001 ¶ 109).

We agree with Petitioner, on this record, that Halperin’s disclosures classify the computer object as malware when the data indicates that the computer object is malware. Halperin discloses that “malicious software has been identified,” that its system “works . . . to identify malicious code,” and that “most of the viruses in the system will be identified within [a] waiting period.” Ex. 1006 ¶¶ 73, 87. Halperin also discloses “automatic identification of suspicious activity by a server . . . and approval by [an] operator that the suspicious activity is truly a virus.” Ex. 1006 ¶ 61.⁹ On

⁹ Patent Owner appears to imply that Halperin’s disclosure of a human considering suspicious activity to be a virus cannot disclose the claimed classifying. *See* Prelim. Resp. 54 (“Instead, those containment actions . . . notify a human that symptoms of malware may have been detected.”). On this record, the claimed “classifying” does not preclude classifying by a human, as claim 1 contains no recitation of a device configured to perform the “classifying.”

this record, these disclosures are sufficient to support Petitioner’s contention that Halperin discloses “classifying the computer object as malware when the data indicates that the computer object is malware.” Thus, Patent Owner’s arguments that Halperin does not disclose “classifying” are unavailing at this stage.

Accordingly, we agree with Petitioner that Halperin likely discloses limitation 1[c].

- e. [e] automatically generating a mask for the computer object that defines acceptable behaviour for the computer object, wherein the mask is generated in accordance with normal behaviour of the object determined from said received data*

Petitioner argues that Mankins discloses or suggests limitation 1[e]. Pet. 30–35. Petitioner first notes that Halperin defines “target behavior profiles” but does not explicitly state how these profiles are generated. *Id.* at 30 (citing Ex. 1006 ¶ 47; Ex. 1004 ¶ 88). Then Petitioner explains that Mankins discloses using a “Bloom filter” to automatically generate a “Bloom filter data object containing data representative of normal system-call behavior” of a computer program.¹⁰ *Id.* at 30–31 (citing Ex. 1008, 3:40–43, 8:8–13, 11:24–45 (describing a training process that “may be performed

¹⁰ For context, Mankins explains that “the Bloom filter 175 generally consists of two components: a set of hash functions and a bit vector (e.g., the Bloom filter data object 180) of a given length.” Ex. 1008, 8:19–22. The hash functions are used to “encode predetermined unique system-call sequences into the bit vector.” *Id.* at 8:26–28. Mankins’ system hashes each system call sequence to obtain a value, which it indexes into the bit vector to search for a match. *Id.* at 8:30–36. Anomalous behavior is identified when the system-call behavior does not have a match in the bit vector. *Id.* at 3:53–55.

automatically to generate the Bloom filter data object”)). Petitioner asserts that “[i]t would have been obvious to a POSITA that Mankins’s ‘Bloom filter data object,’ which is ‘representative of “normal” computer program behavior’ . . . is an example of the ’250 Patent’s ‘mask for said object that defines acceptable behaviour for the object.’” *Id.* at 31 (citing Ex. 1001, 3:40–43, 4:22–23; Ex. 1004 ¶ 89). It also would have been obvious to generate Mankins’ Bloom filter data objects at the remote computers in the combined system, Petitioner argues, because Mankins discloses that its “intrusion detection system 100 may be implemented *in a distributed fashion over a network of computing devices.*” *Id.* at 31–32 (citing Ex. 1008, 4:29–31; Ex. 1004 ¶¶ 90–92). More generally, Petitioner contends that “a POSITA would have recognized that Mankins’s Bloom filter data object could be incorporated at either a remote computer or a base computer using the system architecture described in Halperin.” *Id.* at 21–22 (citing Ex. 1004 ¶¶ 64–66).

Patent Owner does not dispute that the Halperin/Mankins combination discloses limitation 1[e]. Rather, Patent Owner disputes that Petitioner has shown a motivation to combine Mankins with Halperin. Prelim. Resp. 38–44, 57–60. We address the parties’ motivation to combine arguments in a separate section below.

On this record, Petitioner persuades us that Halperin likely discloses limitation 1[e].

f. [i] reclassifying the computer object as malware when the actual monitored behaviour extends beyond that permitted by the mask.

Petitioner contends that Halperin and Mankins disclose or suggest limitation 1[i]. Pet. 41–42 (citing Ex. 1004 ¶¶ 109–111). According to

Petitioner, Mankins teaches that after the comparison of the monitored system-call behavior with data in the Bloom filter data object, “[i]f a match is not found, the observed system-call sequence is determined to be anomalous and may indicate an intrusion attempt” and take “predetermined actions designed to protect the computer.” *Id.* (citing Ex. 1008, 6:39–41, 11:8–11). Petitioner argues that “a POSITA would understand that taking actions to protect the computer indicates the computer object has been reclassified as malware.” *Id.* at 42 (citing Ex. 1004 ¶¶ 110–111). “At a minimum,” Petitioner argues, “it would have been obvious to reclassify the program that performed the system-call sequence flagged as an intrusion attempt as malware.” *Id.* (citing Ex. 1004 ¶ 111). Finally, Petitioner asserts that “[a] POSITA would have understood that Halperin’s disclosure of ‘virus containment actions’ and Mankins’s disclosure of ‘predetermined actions designed to protect the computer’ to include reclassifying the computer object as malware.” *Id.* (citing Ex. 1004 ¶ 112).

Patent Owner contends that “neither Halperin’s ‘virus containment actions’ nor Mankins’s ‘predetermined actions designed to protect the computer’ constitute classifying (or reclassifying) a computer object as malware.” Prelim. Resp. 61. Patent Owner reiterates that “Halperin nowhere identifies any actions as being specific to a computer object.” *Id.* Patent Owner also argues that Dr. Newman makes a “hand-waving” assertion that in the combination, taking virus containment actions in Halperin would have included reclassifying a program as malware. *Id.* at 62 (citing Ex. 1004 ¶ 112). As for Mankins, Patent Owner argues that it provides no elaboration on what “predetermined actions designed to protect the computer” might be. *Id.* Nothing in Mankins suggests that those actions

“be specific or limited to the program whose system call Mankins’ Bloom filter has flagged as suspicious,” Patent Owner argues. *Id.* at 63 (citing Ex. 2001 ¶ 121). Patent Owner continues, “[n]or would a POSITA think immediately reclassifying an object as malware based on a single errant system call was a proportionate response.” *Id.* Patent Owner also further criticizes Dr. Newman’s related testimony. *Id.* (citing Ex. 1004 ¶¶ 111, 120–122).

At this stage, Petitioner persuades us that the combination of Halperin and Mankins likely discloses this limitation. We agree that, on this record, Mankins’ “predetermined actions designed to protect the computer” would have included indicating that the computer object has been reclassified as malware. Pet. 41–42 (citing Ex. 1004 ¶¶ 110–111). We note that Patent Owner appears to concede as much when Patent Owner refers to “the program whose system call Mankins’ Bloom filter has flagged as suspicious.” Prelim. Resp. 63. If Mankins’ Bloom filter flags a program as suspicious, that is indeed reclassifying that program (i.e., an object) as malware. Although Patent Owner’s larger point is that Mankins’ responsive action is not “specific or limited to the program whose system call Mankins’ Bloom filter has flagged as suspicious,” neither is the claim so limited. *See* Prelim. Resp. 63. So long as Mankins’ Bloom filter reclassifies one computer object as malware, it is of no import that the Bloom filter’s responsive action might also include other programs, as Patent Owner implies.

Accordingly, Petitioner persuades us that the Halperin-Mankins combination likely discloses or suggests limitation 1[i].

g. Motivation to Combine

Petitioner contends that a POSITA would have been motivated to incorporate Mankins' Bloom filter mask into Halperin's detection system. Pet. 33–35; *see also id.* at 21–24. For example, Petitioner contends that it would have been obvious to “use Mankins's Bloom filter mask with Halperin to identify predefined suspicious behavior patterns and determine an object is malware if that computer object performs actions beyond its ‘normal (i.e. expected) system-call behavior.’” *Id.* at 34. This “would have been a simple substitution of one known behavior-based approach to malware behavior detection for another,” Petitioner contends. *Id.* (citing Ex 1004 ¶ 94). Further, Petitioner contends that the combination would have improved Halperin's system “by reducing false positives” due to Mankins' distributed approach. *Id.* at 34–35 (citing Ex. 1004 ¶¶ 95–96; Ex. 1008, 10:53–62 (referring to “detect[ing] a false positive” “when several network devices generate separate Bloom filter data objects”)). Petitioner also contends that a POSITA would have had a reasonable expectation of success because adding Mankins' Bloom filter to Halperin's system “would have been no more than using a known technique to improve a similar device in a similar way.” *Id.* at 35 (citing Ex. 1004 ¶ 97).

At this stage, after consideration of Patent Owner's arguments, which we address below, we determine that Petitioner has sufficiently established that one of ordinary skill in the art likely would have considered combining Halperin and Mankins with a reasonable expectation of success. For example, because Halperin teaches generating target behavior profiles, one of ordinary skill in the art naturally would have looked to other references describing how to generate target behavior profiles, such as Mankins. *See*

Ex. 1004 ¶ 94. As Dr. Newman persuasively testifies at this stage, “the substitution or addition of Halperin’s predefined suspicious behavior pattern with Mankins’s Bloom filter mask . . . , would have been a simple substitution (or addition) of one known behavior-based approach to malware detection for another.” *Id.* We also find persuasive that Mankins’ distributed technique would have reduced the occurrence of false positives, which, on this record, is a potential advantage further suggesting the combination. *See id.* ¶ 96.

Patent Owner raises the following arguments, which we address below in turn.

(1) Alleged teaching away

First Patent Owner contends that Halperin teaches away from Mankins because Halperin expressly teaches away from using a heuristic system like that disclosed in Mankins. Prelim. Resp. 39–40. Patent Owner refers to Halperin’s teaching that “antivirus software that employs heuristic techniques . . . often results in a false alarm . . . leading computer users to disable such software or set the sensitivity of such software so low to the point where new viruses are often not identified.” *Id.* at 39 (citing Ex. 1006 ¶ 6). Mankins produces “*both* positives and false *negatives*,” Patent Owner argues, by “approv[ing] behavior that it should flag as suspicious.” *Id.* (citing Ex. 2001 ¶ 71–74; Ex. 1008, 8:62–64).

We see several problems with Patent Owner’s teaching away argument at this stage. First, Patent Owner does not sufficiently explain how Mankins’ approach is a “heuristic system” of the type to which Halperin refers. *See* Ex. 2001 ¶ 72 (Dr. Medvidovic testifying, “I read Mankins to teach exactly what Halperin discourages,” but not explaining

how Mankins discloses a heuristic). Thus, even if Halperin does teach away from using a heuristic, it is unclear on this record whether Mankins discloses such a heuristic.

Second, Halperin warns of “false alarm[s],” but Mankins refers to “false positives,” not false alarms. Ex. 1006 ¶ 6; Ex. 1008, 8:61–64. Halperin’s concern is users disabling antiviral software or setting the sensitivity of such software so low to the point where new viruses are often not identified. Ex. 1006 ¶ 6. A “false positive” in Mankins is an improper indication that software is *not* a virus, which would *not* raise a virus alarm, so there would be no cause for a user to disable the antiviral software or reduce its sensitivity as Halperin warns. *See* Ex. 1008, 8:61–64 (“False positives refer to occurrences in which a Bloom filter 175 reports the existence of a match [indicating normal behavior] when in fact no such match is actually contained in the Bloom filter data object 180”); *see also id.* at 3:53–55 (“Anomalous behavior is identified when the actual system-call behavior does not have a match in the Bloom filter data object.”).

Third, Halperin claims to reduce, but not eliminate, false alarms. Ex. 1006 ¶¶ 59 (“designed to reduce false alarms”), 85 (“provide an improved ratio of virus detections to false alarms”), 90 (“[t]he lower the threshold the less false alarms the system will have”). Thus, one of ordinary skill in the art would have viewed another system, such as Mankins, which also admits to the possibility of some false positives, as not necessarily incompatible with Halperin’s system.

Finally, that Mankins also claims to reduce false positives suggests the compatibility of these systems, not their incompatibility. *See* Ex. 1008, 10:53–62 (“the different network devices can work together to identify false

positives”); Ex. 1004 ¶ 95 (Dr. Newman testifying, “Thus, the use of Mankins’s Bloom filter data object (‘mask’) approach in a distributed system such as Halperin would actually improve the system by reducing positives by improving the robustness of the ‘normal’ behavior data represented in the Bloom filter data objects.”).

(2) Alleged nonfunctionality of the combination

Patent Owner next contends that Petitioner’s proposed combination would not work. Prelim. Resp. 40–43. Patent Owner first notes that Petitioner appears to argue for either (1) storing Mankins’ Bloom filter data objects at Halperin’s central server or (2) storing Mankins’ objects on Halperin’s remote computers. *Id.* at 40 (citing Pet. 21–22). Patent Owner argues, “[n]either version of the system would represent an improvement of either reference’s system alone.” *Id.*

Centralized Bloom filters would not work, Patent Owner asserts, because Mankins teaches away from a “centralized” configuration, which “would cause significant delays and would be impracticable to use with complex computer programs.” *Id.* (citing Ex. 1008, 2:14–37; Ex. 2001 ¶¶ 76–77). We question this premise because the passage Patent Owner cites is in Mankins’ Background, which does not appear to refer to centralized Bloom filters. *See id.*; Ex. 1008, 2:14–37 (referring to shortcomings with “existing system-call-based intrusion detection techniques” but not referring to centralized Bloom filters per se).

Patent Owner raises several related disadvantages of centralized Bloom filters. Patent Owner argues that “[c]ombining all system-call behavior for all objects into a single Bloom filter would eliminate any benefit of Mankins, because different computer objects are expected to make

different system calls.” Prelim. Resp. 41 (citing Ex. 2001 ¶ 77). Patent Owner also asserts, “[e]ven if what Petitioner is actually suggesting is storing, on the central Halperin server, a different Mankins Bloom filter data object for each computer object running on each remote computer on the network, the system would quickly collapse under its own weight.” *Id.* (citing Ex. 2001 ¶ 77). Further, remote computers hashing and sending each system call in real time to a central server “would slow the remote computers to a crawl,” Patent Owner asserts. *Id.* at 41–42 (citing Ex. 2001 ¶ 77). And, finally, Patent Owner contends that “Petitioner’s contention that adding Mankins to the Halperin system would have little or no cost (Petition 24) is ludicrous on its face.” *Id.* at 42 (citing Ex. 2001 ¶ 79).

These arguments are all unavailing at this stage because they are all unsupported and speculative. Dr. Medvidovic’s testimony to these disadvantages does not adequately explain how these disadvantages would occur; nor does Dr. Medvidovic quantify these potential disadvantages. *See* Ex. 2001 ¶¶ 77–79. Further, the possibility that a centralized Bloom filter “would slow the remote computers to a crawl” or that “the system would quickly collapse under its own weight” does not take into account the hardware of the computers and network, which could potentially have been designed with sufficient speed and bandwidth to ameliorate these problems. Moreover, Patent Owner’s arguments are undermined by Mankins itself teaching a distributed, and not only centralized, approach. *See* Ex. 1008, 10:53–62. Thus, we give Dr. Medvidovic’s testimony on Patent Owner’s arguments little weight at this stage.

In any event, “[a] given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate

motivation to combine.” *Allied Erecting v. Genesis Attachments*, 825 F.3d 1373, 1381 (Fed. Cir. 2016) (citation omitted). At this stage, the speculative disadvantages Patent Owner raises do not outweigh the advantages of the combination Petitioner identifies, including using Mankins as a more detailed way to generate the target behavior profiles disclosed in Halperin, as well as the further possible reduction of false positives using Mankins’ distributed approach. *See* Ex. 1004 ¶¶ 94, 96.

Patent Owner also attacks Mankins’ distributed Bloom filter disclosure, contending that a distributed set of Bloom filters “might in fact impede” the operation of the system, would “cast doubt on both systems’ results,” and would “eliminat[e] any possible benefit of Halperin’s aggregate-behavior detection.” Prelim. Resp. 42–43 (citing Ex. 2001 ¶¶ 78, 79, 80, 86). These arguments are all likewise speculative and unavailing at this stage.

(3) Alleged non-detection of false positives

Patent Owner further argues that the combination would not assist in detecting false positives. Prelim. Resp. 43–44. Patent Owner contends that “even if Mankins’s system’s results disagree with Halperin’s, that will not be an indication that Halperin has returned a false positive.” *Id.* at 44 (citing Ex. 2001 ¶ 84). Relatedly, Patent Owner argues that “Petitioner offers no reason for privileging either system’s result over the other’s, and so offers no way to discern which positives are ‘false’ for *either* system according to the proposed combination.” *Id.* (citing Ex. 2001 ¶ 86). Thus, Patent Owner concludes, “[w]here the systems’ results disagree, all Petitioner’s proposed combination does is reduce a POSITA’s confidence that either system has produced a correct result.” *Id.* (citing Ex. 2001 ¶ 86).

Like Patent Owner's previous arguments, we view these arguments as speculative and unsupported at this stage.

(4) Additional arguments

Patent Owner further asserts that “[d]espite alleging that Mankins’s Bloom filter data objects would serve as the basis for Halperin’s correlation and identification of suspicious behavior patterns, Petitioner never maps this combination to claim 1’s preamble or limitations [1A] to [1C].” Prelim. Resp. 58. “Accordingly,” Patent Owner argues, “Ppetitioner failed to argue, let alone show how, Mankins’s Bloom filters would run at Halperin’s endpoint computers and provide the data Halperin uses for behavior correlation, or how that would allegedly meet those claim limitation[s].” *Id.* (citing Ex. 2001 ¶ 115). As Petitioner relies on Mankins only for limitations 1[d] *et seq.*, Patent Owner charges Petitioner with relying on hindsight. *Id.*

This argument is unavailing at this stage, as Petitioner is not obligated to rely on Mankins for claim limitations 1[a] through 1[c]. Patent Owner appears to view Petitioner as proposing a bodily incorporation of Mankins features into Halperin’s system, but we do not read the Petition that way. “The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art.” *MCM Portfolio LLC v. Hewlett-Packard Co.*, 812 F.3d 1284, 1294 (Fed. Cir. 2015) (quoting *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)).

Further, Patent Owner asserts that Petitioner fails to explain how Mankins would work with Halperin, so “the only technically feasible solution is to run Mankins *on every piece of software running on every*

computer in the network.” Id. at 59 (citing Ex. 2001 ¶ 118). This assertion is also speculative and unpersuasive.

Patent Owner also finds fault with Dr. Newman’s testimony that the combination “*could have been expected to improve detection* of previously unknown malware” because Dr. Newman uses the word “could” instead of “would.” *Id. at 60 (citing Ex. 1004 ¶ 95). We do not view Dr. Newman’s use of word “could” in this instance as undermining his testimony or undermining Petitioner’s arguments. Dr. Newman testifies in several places that the combination “would” have been obvious, including in the very paragraph Patent Owner points to. E.g., Ex. 1004 ¶¶ 92–97.*

For these reasons, we determine on this record that Petitioner has shown that one of ordinary skill in the art likely would have combined Halperin and Mankins in the manner claimed, with a reasonable expectation of success.

h. Objective Indicia of Nonobviousness

Patent Owner asserts, without explanation, “that objective indicia of nonobviousness exist and [that Patent Owner] reserves its right to provide evidence on this point, should the Board institute.” Prelim. Resp. 64 (citing Ex. 2001 ¶ 33). We give no weight to this conclusory assertion at this stage.

i. Summary as to Claim 1

Based on the preliminary record before us, Petitioner has shown a reasonable likelihood that claim 1 would have been obvious over the combination of Halperin and Mankins.

4. Independent Claim 13

Petitioner sets forth similar arguments for independent claim 13 as for claim 1. *See* Pet. 42. Patent Owner relies on the same arguments for this

claim as it does for claim 1. Prelim. Resp. 45–46. For similar reasons as discussed above, Petitioner has shown a reasonable likelihood that claim 13 would have been obvious over the combination of Halperin and Mankins.

5. Dependent Claims 2, 12, 14, and 24

Petitioner contends that dependent claim 2, 12, 14, and 24 would have been obvious over the combination of Halperin and Mankins. Pet. 43–44, 46–48, 57–59, 65–67. Patent Owner does not contest Petitioner’s arguments over these claims at this stage. We leave for trial the issue of whether Petitioner establishes that the combination of Halperin and Mankins would have rendered obvious claims 2, 12, 14, and 24.

F. Asserted Obviousness over Halperin, Mankins, and Kirby (Ground 2)

Petitioner contends that the combination of Halperin, Mankins, and Kirby would have rendered obvious claims 1–30. Pet. 45–63. Patent Owner does not dispute this ground, other than to raise the same disputes for independent claim 25 as it raises for claims 1 and 13. Prelim. Resp. 45–46. Accordingly, we leave the issue of whether Petitioner has proven the obviousness of claims 1–30 over this ground for trial.

IV. CONCLUSION

At this stage of the proceeding, we determine that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenges as to at least one challenged claim. At this preliminary stage, we have not made a final determination as to the patentability of the challenged claims or any underlying factual and legal issues.

V. ORDER

It is, therefore,

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of all challenged claims of the '250 patent is instituted with respect to all grounds of unpatentability set forth in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial commencing on the entry date of this Decision.

IPR2023-00699
Patent 8,418,250 B2

PETITIONER:

Ryan Iwahashi
GIBSON, DUNN & CRUTCHER LLP
riwahashi@gibsondunn.com

PATENT OWNER:

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