UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SOPHOS LTD. AND SOPHOS INC.

Petitioners

v.

OPEN TEXT INC.

Patent Owner

Case IPR2024-00252

Patent No. 8,201,243

PATENT OWNER'S PRELIMINARY RESPONSE

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313–1450

TABLE OF CONTENTS

I. INTRODUCTION 1

II. BACKGROUND AND RELATED PROCEEDINGS.....2

A. District Court Litigation 2

B. Petitioner's First and Second Petitions 3

C. Replication of IPR2023-00731.....5

III. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a) AND *GENERAL PLASTIC* 6

A. The Board Has Denied Institution Of Serial Copycat Petitions Under *General Plastic*.....6

B. The Board Should Deny Institution Of Petitioner's Follow-On Petition.....8

1. Petitioner previously filed a petition directed to the same claims of the same patent. 8

2. When Petitioner filed the First Petition, Petitioner knew of the prior art asserted in the Second Petition. 11

3. When Petitioner filed the Second Petition, Petitioner had already received Patent Owner's preliminary response to the First Petition *and* the Board's decision denying institution. 11

4. Petitioner waited more than a year after learning of the asserted prior art before filing its Second Petition.....13

5. Petitioner provides no explanation for the time elapsed between the filings of its multiple petitions.....13

6. The finite resources of the Board favor denial.....14

7. The one-year final determination deadline does not support institution. 15

IV. THE PETITION SHOULD BE DENIED ON THE MERITS 16

A. THE '243 PATENT 16

1. Inadequacy Of The Prior Art & The Need For Improved Pestware Detection 16

2. Innovations Of The '243 Patent 17

3. Level Of Ordinary Skill In The Art 18

B. Overview Of The Relevant Prior Art 19

1. Overview Of Li 19

2. Overview Of Hartrell 20

3. Overview Of Yadav 21

4. Overview Of Mandujano 23

C. THE CHALLENGED CLAIMS ARE PATENTABLE 24

1. Ground 1: Petitioner Fails To Establish That Li and Hartrell Renders Obvious Every Limitation of The Challenged Claims 25

2. Ground 2: Petitioner Fails To Establish That Li, Hartell, And Mandujano Render Obvious Every Limitation Of The Challenged Claims 43

3. Ground 3: Petitioner Fails To Establish That Li And Yadav Render Obvious Every Limitation Of The Challenged Claims 45

4. Ground 4: Petitioner Fails To Establish That Li, Yadav, And Mandujano Disclose Or Render Obvious The Independent Claims Of The '243 Patent 50

5. Petitioners' Grounds Fail To Render Obvious All Dependent Claims 52

6. Other Limitations Not Addressed 52

7. There Are Secondary Objective Indicia Of Nonobviousness 53

V. CONCLUSION 53

TABLE OF AUTHORITIES

Page(s)

Cases

Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.,
800 F.3d 1375 (Fed. Cir. 2015) 24

General Plastic Industrial Co. v. Canon Kabushiki Kaisha,
IPR2016-01357, Paper 19 (PTAB Sept. 6, 2017).....*passim*

Harmonic Inc. v. Avid Tech., Inc.,
815 F.3d 1356 (Fed. Cir. 2016) 24

Sophos Ltd. and Sophos Inc. v. Open Text, Inc.,
IPR2023-00731, Paper 1 ("First Petition") (P.T.A.B. April 4, 2023) 3

Sophos Ltd. and Sophos Inc. v. Open Text, Inc.,
IPR2023-00731, Paper 22 (P.T.A.B. Nov. 1, 2023).....*passim*

Sophos Ltd. and Sophos Inc. v. Open Text, Inc.,
IPR2023-00731, Paper 23 (P.T.A.B. Nov. 2, 2023).....*passim*

Sophos Ltd. and Sophos Inc. v. Open Text, Inc.,
IPR2023-00731, Paper 25 (P.T.A.B. Dec. 21, 2023) 5

Valve Corp. v. Elec. Scripting Prods., Inc.,
IPR2019-00062, Paper 11 (P.T.A.B. Apr. 2, 2019) 14, 15

Videndum Prod. Sols., Inc. v. Rotolight Ltd.,
IPR2023-01220, Paper No. 9 (P.T.A.B. Jan. 24, 2024) 12

ZTE Corp. v. ContentGuard Holdings, Inc.,
IPR2013-00454, Paper 12 (PTAB Sept. 25, 2013) 4

Statutes

37 C.F.R. § 42.108(a).....6

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Professor Ron Schnell (Patent Owner Exhibit 2001, IPR2023-00731)
2002	*Curriculum Vitae* of Professor Ron Schnell (Patent Owner Exhibit 2002, IPR2023-00731)
2003	*Webroot, Inc. and Open Text Inc., v. Sophos Ltd.,* Case No. 6:22-cv-00240-ADA-DTG, Defendant's Preliminary Invalidity Contentions (W.D. Tex., Feb. 21, 2023) (excerpted)
2004	*Webroot, Inc. and Open Text Inc., v. Sophos Ltd.,* Case No. 6:22-cv-00240-ADA-DTG, Defendant's Final Invalidity Contentions Against Counterclaim Plaintiff Sophos Ltd. (W.D. Tex., Nov. 1, 2023) (excerpted)
2005	*Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.,* Case No. 6:22-cv-243-ADA-DTG, Claim Construction Order, Dkt. 391 (W.D. Tex. July 25, 2022)
2006	Email from Timothy Best (counsel for Petitioner) to trials@uspto.gov re IPR Proceedings: IPR2023-00699; IPR2024-00252; and IPR2024-00253, dated March 20, 2024
2007	*Sophos Ltd. & Sophos Inc. v. Open Text Inc.,* Case IPR2023-00732, EX-3002: Email dated Oct. 16, 2023 from trials@uspto.gov to Timothy Best (counsel for Petitioner)

Open Text Inc. ("Patent Owner") submits this Preliminary Response to the petition of Sophos Ltd and Sophos Inc. (collectively, "Petitioner") seeking *inter partes review* ("IPR") of U.S. Patent No. 8,201,243 ("the '243 patent").

I. INTRODUCTION

The instant IPR petition is Petitioner's second attempt to institute an IPR on the same patent. Under the factors set forth in *General Plastic Industrial Co. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 9-10, (PTAB Sept. 6, 2017) (§ II.B.4.i precedential), the Board should deny the petition.

First, the Board should deny institution under *General Plastic* because instituting this second petition raising the same arguments would reward Petitioner's failure to present its best evidence with its first petition. Allowing Petitioner to correct the problems Patent Owner identified in its first petition and that justified denying institution would encourage the kind of "multiple, staggered petition filings [that] are an inefficient use of the *inter partes* review process and the Board's resources," in addition to Patent Owner's. *General Plastic*, IPR2016-01357, Paper 19, at 21.

Second, the Board should deny institution for the additional reason that Petitioner fails to demonstrate a reasonable likelihood that it will prevail on the merits. The '243 patent discloses a pestware monitoring and identification system

that identifies an externally networked source from which a suspected pestware object originated and reports the source to an externally networked research entity. But none of the art on which Petitioner relies teaches or suggests those ideas. Instead, the cited art discloses identifying internal files or directories from which the pestware originated and alerting a human administrator that the internal file or directory shows signs of a malware infection. Because none of the cited art suggests identifying the externally networked source of a pestware object, let alone reporting that source to an external, networked research entity, the petition is not reasonably likely to succeed and must therefore be denied.

Third, Petitioner and Patent Owner have settled their dispute at issue in the district court litigation and have requested permission to file a joint motion to terminate this Petition.

Patent Owner respectfully requests that the Board deny the petition.

II. BACKGROUND AND RELATED PROCEEDINGS

A. District Court Litigation

Concurrent district court litigation between Patent Owner, Petitioner, and one additional co-defendant of Petitioner has been pending in a consolidated case in the United States District Court for the Western District of Texas since 2022. *Webroot, Inc. & Open Text, Inc. v. AO Kaspersky Lab*, Case No. 6:22-cv-00243 (W.D. Tex.).

The district court litigation has progressed significantly. The court has held three claim construction hearings and entered nine claim construction orders. Dkt. Nos. 235, 236, 293, 295, 296, 297, 391, 392, and 393. Petitioner served its Final Invalidity Contentions on November 1, 2023 (EX-2004). Petitioner and Patent Owner have settled their dispute in the district court litigation and have requested permission to file a joint motion to terminate this Petition. (EX2007.) (email from Petitioner's counsel requesting leave to file Joint Motions to Terminate IPR2023-00699; IPR2024-00252; IPR2024-00253.)

B. Petitioner's First and Second Petitions

In its first petition, Petitioner challenged claims 1–14 of the '243 patent on the grounds below. *See* Paper 1, *Sophos Ltd. and Sophos Inc. v. Open Text, Inc.*, IPR2023-00731 ("First Petition") (P.T.A.B. April 4, 2023).

Ground 1	Section 103(a)	Obvious over Li in view of Hartrell	Claims 1–14
Ground 2	Section 103(a)	Obvious over Li in view of Hartrell and Mandujano	Claims 1–14
Ground 3	Section 103(a)	Obvious over Li in view of Yadav	Claims 1–14
Ground 4	Section 103(a)	Obvious over Li in view of Yadav and Mandujano	Claims 1–14

In its current petition (Paper 1, "Second Petition"), Petitioner challenges the exact same claims using the exact same references as in its First Petition. *Compare* First Petition *with* Second Petition.

Patent Owner filed its preliminary response to the First Petition on August 10, 2023, primarily arguing that Petitioner failed to establish the public availability of the Li prior art reference, on which Petitioner relied for all of its grounds. IPR2023-00731, Paper 13. Petitioner thereafter sought to file a reply to supplement the record with additional public accessibility evidence, and the Board denied that request. (EX-2008 (denying Petitioner's request to file Replies to the Preliminary Responses). Petitioner moved to dismiss the First Petition on October 10, 2023, and on November 1, 2023, the Board denied the motion to dismiss. IPR2023-00731, Paper 22 at 3. The Board reasoned that "a petitioner should set forth its best evidence in a petition and not plan to dismiss and refile that petition when a preliminary response exposes its weaknesses." *Id*. at 3. The Board was "concerned about encouraging, unnecessarily, the filing of petitions which are partially inadequate." IPR2023-00731, Paper No. 22. (quoting *ZTE Corp. v. ContentGuard Holdings, Inc.*, IPR2013-00454, Paper 12 at 5–6 (PTAB Sept. 25, 2013) (informative)). The Board also noted that "[d]ismissing these petitions now, with knowledge of Petitioner's intent to refile new petitions, would condone the filing of inadequate petitions in a

trial-and-error approach." *Id*. at 4. The Board closed its opinion by stating: "Should Petitioner choose to file new petitions, the principles set forth in our decisions related to serial petitions will govern. *See, e.g.*, *General Plastic*, IPR2016-01357, Paper 19." IPR2023-00731, Paper 22 at 5.

On November 2, 2023, the Board denied institution of the First Petition. IPR2023-00731, Paper 23. In short, the Board agreed with the argument in Patent Owner's preliminary response that "Petitioner has not shown a reasonable likelihood that Li was accessible before the priority date of the '243 patent." (*Id.* at 15.) Petitioner moved for rehearing, and the Board denied the motion. IPR2023-00731, Paper 25. On December 8, 2023, while the rehearing motion was pending, Petitioner filed the Second Petition.

C. Replication of IPR2023-00731

The obviousness arguments Petitioner raises in its Second Petition are materially identical to those it raised in its First Petition. As discussed in more detail below, the only difference between the two petitions is that, in the Second Petition, Petitioner introduced additional evidence of the alleged public availability of the Li reference. (*See* Petition at 14.) In other words, the Second Petition attempts to address the First Petition's deficiencies, identified by Patent Owner, that resulted in its denial.

III. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a) AND *GENERAL PLASTIC*

In instances where petitioners seek to refile in order to correct errors that rendered their initial petitions inadequate, putting patent owners and the Board through the time and expense of a second institution proceeding, the Board has denied institution under *General Plastic*. Indeed, the Board has already indicated that the concerns addressed by *General Plastic* are applicable here. *See* IPR2023-00731, Paper 22 at 5 ("Should Petitioner choose to file new petitions, the principles set forth in our decisions related to serial petitions will govern. *See, e.g.*, *General Plastic*, IPR2016-01357, Paper 19.")

A. The Board Has Denied Institution Of Serial Copycat Petitions Under *General Plastic*.

In *General Plastic*, the petitioner filed a first set of petitions seeking *inter partes* review of two patents. *General Plastic*, IPR2016-01357, Paper 19 at 2–3. The Board denied institution of both petitions on the merits. *Id*. Then, nearly nine months after the first petitions, the petitioner filed follow-on petitions challenging the same patents. *Id*. For each of those follow-on petitions, the Board exercised its discretion, under 35 U.S.C. § 314(a) and 37 C.F.R. § 42.108(a), to deny institution. *Id*. at 8. In denying the follow-on petitions, the Board considered seven factors:

1. whether the same petitioner previously filed a petition directed to the same claims of the same patent;

2. whether at the time of filing of the first petition the petitioner knew of the prior art asserted in the second petition or should have known of it;

3. whether at the time of filing of the second petition the petitioner already received the patent owner's preliminary response to the first petition or received the Board's decision on whether to institute review in the first petition;

4. the length of time that elapsed between the time the petitioner learned of the prior art asserted in the second petition and the filing of the second petition;

5. whether the petitioner provides adequate explanation for the time elapsed between the filings of multiple petitions directed to the same claims of the same patent;

6. the finite resources of the Board; and

7. the requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than 1 year after the date on which the Director notices institution of review.

Id. at 9–10.

In explaining its decision to deny institution, the Board noted that "the same claims of the same patent were at issue in the follow-on petitions as in the first-filed petitions," and that the petitioner provided no explanation for the nine-month delay between petitions. *Id*. The Board found that its "resources would be more fairly expended on initial petitions, rather than follow-on petitions." *Id*. The Board recognized that failing to place any restrictions on follow-on petitions would allow

petitioners to "strategically stage their prior art and arguments in multiple petitions, using [the PTAB] decisions as a roadmap." *Id*. at 17.

B. The Board Should Deny Institution Of Petitioner's Follow-On Petition.

The *General Plastic* factors weigh against institution here.

1. Petitioner previously filed a petition directed to the same claims of the same patent.

Petitioner's two petitions both challenge the same claims of the '243 patent on nearly identical grounds. *Compare* IPR2023-00731 Paper 1 *with* IPR2024-00252 Paper 1. The Board denied institution of the First Petition because Petitioner failed to set forth sufficient evidence of public availability of the referenced prior art. IPR2023-00731, Paper 23. In denying Petitioner's motion to dismiss the First Petition, the Board also expressly explained that the principles of *General Plastic* would "govern" its decision on any subsequent petition. IPR2023-00731, Paper 22 at 5 ("Should Petitioner choose to file new petitions, the principles set forth in our decisions related to serial petitions will govern. *See, e.g.*, *General Plastic*, IPR2016-01357, Paper 19.")

Petitioner argues that *Code200* is instructive here because the First Petition was not evaluated on the merits. *See* Petition at 74-76 (*citing Code200 v. Bright Data Ltd.,* IPR2022–00861, Paper 18 at 2, 5 (PTAB Aug. 23, 2022) (Director decision,

precedential)). However, this petition is distinguishable from *Code200* because the petition in *Code200* was not "refined based on lessons learned from later developments." *Id*. at 5. Here, Petitioner's First Petition failed to show a reasonable likelihood that Li was accessible before the priority date of the '243 patent. IPR2023-00731, Paper 23 at 15. Petitioner's Second Petition uses a new declaration to address the Board's concerns regarding Li's public accessibility. Petition EX-1009. In other words, Petitioner is refining its First Petition to reflect lessons learned from Patent Owner's previous preliminary response and the Board's denial of institution.

Petitioner's first declaration regarding the public accessibility of Li relied on links instead of exhibits. IPR2023-731 EX-1009.When given the opportunity to correct the error and file the more permanent exhibits, Petitioner instead chose to file a motion to dismiss, which the Board denied. IPR2023-00731, Paper 22 at 5. In its decision denying institution, the Board found the declaration did not "cite any supporting evidence of record" and "'does not disclose the underlying facts or data on which the opinion is based' and is therefore 'entitled to little or no weight.'" *Id*. at 15 (quoting 37 C.F.R. § 42.65(a)).

In addition, the Board found that the declaration itself was not from a record custodian or anyone with personal knowledge of when Li was published. The

unsupported declaration failed to demonstrate "a reasonable likelihood that Li 'has been disseminated' or that Li was 'otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it.'" IPR2023-00731, Paper 23 at 15 (quoting *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.,* 511 F.3d 1186, 1194 (Fed. Cir. 2008)). As such, the Board found that Petitioner relied "on nothing more than speculation that Li was publicly accessible in the relevant timeframe." *Id*. at 18. Accordingly, the Board found Petitioner failed to satisfy its burden to show that Li was prior art to the '243 patent and denied the petition. *Id*. at 19.

Petitioners, using as a road map Patent Owner's arguments and the Board's analysis of their declaration and the evidence that would be necessary to demonstrate Li was publicly accessible prior to the '243 patent's filing date, ignored the Board's warnings in its denial of the Motion to Dismiss and filed the Second Petition. Not surprisingly, the declaration regarding Li's public accessibility in the Second Petition attempts to address many of the shortfalls identified by Patent Owner and the Board in the First Petition. In contrast to *Code200*, Petitioner clearly refined the Second Petition "based on lessons learned from later developments" and there is clear evidence of "road-mapping" to address the question of whether Li is actually prior art to the '243 patent. *Code200*, IPR2022–00861, Paper 18 at 5-6. Petitioner's

reliance on *Code200* for factors 1-3 is therefore misplaced, and this factor and factors 2 and 3 weigh strongly in favor of denying institution.

2. When Petitioner filed the First Petition, Petitioner knew of the prior art asserted in the Second Petition.

In the First Petition, Petitioner asserted the three references it then asserted again in the Second Petition (Li, Hartrell, and Mandujano). Petitioner knew of the prior art asserted in the Second Petition because it asserted that same art in the First Petition on April 4, 2023 (IPR2023-00731, Paper 1)—and in its February 21, 2023 Preliminary Invalidity Contentions in the district court proceedings (EX-2003). Because Petitioner knew of the art asserted in the Second Petition at the time of filing the First Petition—indeed, it had known of the prior art for at least four months *before* filing that First Petition—this factor weighs in favor of denying institution.

3. When Petitioner filed the Second Petition, Petitioner had already received Patent Owner's preliminary response to the First Petition *and* the Board's decision denying institution.

By the time Petitioner filed the Second Petition, Patent Owner had already filed its preliminary response to the First Petition on August 10, 2023. IPR2023-00731, Paper No. 13. On November 2, 2023, the Board denied institution of the First Petition because Petitioner failed to demonstrate a reasonable likelihood of prevailing with respect to any challenged claim. IPR2023-00731, Paper No. 23. In addition, the Board denied Petitioner's motion to dismiss the First Petition because

"a petitioner should set forth its best evidence in a petition and not plan to dismiss and refile that petition when a preliminary response exposes its weaknesses." IPR2023-00731, Paper No. 22. On November 8, 2023—nearly a month after the Board denied institution of the First Petition—Petitioner filed its Second Petition. There are no material differences between the obviousness arguments presented in the two petitions, apart from citations to additional declarations offered as evidence of the alleged public availability of the Li reference before the '243 patent's priority date. (*Compare* IPR2023-00731 Paper 1 *with* Petition; *see* Petition at 14 (citing EX-1015 & EX-1016.))

In other words, Petitioner filed the First Petition, received Patent Owner's preliminary response and the Board's decision denying institution based on the lack of evidence supporting the argument that Li was publicly accessible, and then filed the Second Petition reasserting the same grounds and merely adding evidence to which it had access when filing the First Petition. This is the precise fact pattern *General Plastic* cautions will waste the Board's resources: Petitioner used Patent Owner's preliminary response and the Board's analysis to develop a roadmap for a future petition in hopes of finding a ground that results in the grant of review. *General Plastic*, IPR2016-01357, Paper No. 19 at 17; *see also Videndum Prod. Sols., Inc. v. Rotolight Ltd.*, IPR2023-01220, Paper No. 9 (P.T.A.B. Jan. 24, 2024)

(denying institution when petitioner's second petition sought to cure the deficiencies of its previously denied petition by copying a third party's petition that was instituted but later terminated).

Accordingly, this factor weighs in favor of denying institution.

4. Petitioner waited more than a year after learning of the asserted prior art before filing its Second Petition.

As discussed above, more than a year passed—from November 1, 2022, until December 8, 2023—between Petitioner's first assertion of the prior art and filing the Second Petition. Indeed, given that Petitioner served its district court Preliminary Invalidity Contentions citing Li, Hartrell, and Mandujanao on November 1, 2022, (EX-2001), Petitioner must have known about those references even before that service date. Yet, Petitioner waited more than thirteen months—until December 8, 2023—to file its Second Petition. Petitioner offers no explanation for this delay. This factor therefore weighs in favor of denying institution.

5. Petitioner provides no explanation for the time elapsed between the filings of its multiple petitions.

Factor 5 examines why Petitioner delayed "between the filings of multiple petitions directed to the same claims of the same patent." *General Plastic* at 9–10. The First Petition—relying on the same primary references—was filed in April 2023. Nearly eight months then passed before Petitioner filed the Second Petition.

Petitioner failed to provide any explanation at all for the time elapsed between these two filings or why it could not have filed the evidence added in the instant petition. The plain explanation is that the First Petition was not instituted, and only afterward did Petitioner seek to try again, this time adding new purported evidence. Petitioner also clearly knew of the prior petition's deficiencies and sought leave to address the evidentiary issues months before the Board denied institution—presumably preparing the evidence for submission contemporaneously—yet Petitioner failed to file the Second Petition until a month after the First Petition was denied. Petitioner provides no explanation for that additional delay. Accordingly, this factor weighs in favor of denying institution.

6. The finite resources of the Board favor denial.

The Board has explained that "[i]n general, having multiple petitions challenging the same patent, especially when not filed at or around the same time … is inefficient and tends to waste resources." *Valve Corp. v. Elec. Scripting Prods., Inc.*, IPR2019-00062, Paper 11, 15 (P.T.A.B. Apr. 2, 2019) (precedential). Petitioner had its chance to file a petition using the best evidence it had available in November 2022. Petitioner did not. The Board should not expend its finite resources on a petitioner who filed a follow-on petition after its first try failed to demonstrate a reasonable likelihood of prevailing with respect to any challenged

claim based on the same references. As in *Valve*, Petitioner has filed serial and repetitive attacks against the same patent relying on the same prior art. "These serial and repetitive attacks implicate the efficiency concerns underpinning *General Plastic* and, thus, favor denying institution." *Valve*, IPR2019-00062, Paper 11, 15.

Further, as noted above, the parties have settled the district court litigation and will soon file a joint motion to terminate this and other IPR proceedings. (EX-2006) (email from Petitioner's counsel requesting leave to file Joint Motions to Terminate IPR2023-00699; IPR2024-00252; IPR2024-00253.) Instituting a duplicative IPR when the parties no longer have an active dispute would be particularly wasteful.

This factor weighs in favor of denying institution.

7. The one-year final determination deadline does not support institution.

Like the sixth *General Plastic* factor, the seventh factor, "the requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than one year after the date on which the Director notices institution of review," implicates efficiency. This factor is at best neutral because it is an inefficient use of the Board's time to review multiple petitions based on the same claims and the same prior art and to draft decisions on the same issues multiple times within a year.

Six of the seven *General Plastic* factors weigh in favor of denying institution—as was the case in *General Plastic* itself. IPR2016-01357, Paper 19, at 19. The Board should accordingly deny institution.

IV. THE PETITION SHOULD BE DENIED ON THE MERITS

The Board should deny institution for the additional reason that Petitioner fails to demonstrate a reasonable likelihood that it will prevail on the merits.

A. THE '243 PATENT

1. Inadequacy Of The Prior Art & The Need For Improved Pestware Detection

"Pestware" is a trojan, spyware, adware program, or malware program that collects information about a person or an organization. (EX-2010; EX-1001 1:43-54.) Much of the prior art anti-pestware or anti-virus software focused on scanning and stopping ***known*** pestware based on previously created pestware definitions. (EX-1001 1:63-65.) These prior art methods for detecting known pestware suffered from extensive delay—either while waiting for the pestware to be detected and a definition generated or in locating the pestware to create definitions in the first place. (EX-1001 1:65-67; EX-2001 ¶¶28-29.)

Accordingly, there was a need for an improved technique to efficiently determine whether files were safe or malware. (*Id.* ¶30.)

2. Innovations Of The '243 Patent

The '243 patent discloses identifying pestware by monitoring the activity of software in a reverse or "backwards" manner. Instead of looking for pestware files directly, the invention disclosed and claimed in the '243 patent monitors changes made to system resources, analyzes logs and traces of software execution, identifies patterns of behavior indicative of pestware, and classifies and categorizes detected pestware using heuristics and machine learning. (EX-1001 10:8-30.) The '243 patent uses heuristics modules to compare API call activities on the computer with weighted factors to make decisions relative to activities at the protected computer. (*Id*.)

Among the innovations of the '243 patent is the identification of an externally networked source from which a suspected pestware object originated. As stated by the applicant during prosecution, the prior art "is interested not in an externally networked source suspected of originating an attack (e.g., an Internet URL or Web site from which the pestware was downloaded), but in the internal network's user or process session through which the attack is made (i.e., the local 'victim' of the attack)." (EX-1002 167.) Unlike prior art systems, the '243 patent traces pestware activity both back to a pestware object ***and*** to a source that originated the pestware object. "As an example, if a pestware file is found on the file storage device 118,

then the cache index 243 of the browser cache 242 may be searched to identify the name of the file, *and if the originating URL is stored in connection with the file, the URL is identified as the source of the file*." (EX-1001 7:48-52.) This represents a significant improvement over the prior art not found in the references cited by the Petitioner.

The '243 patent also discloses reporting the source of the suspected pestware object to an "externally networked pestware research entity." (EX-1001, claims 1, 6, 12.) "In this way, the suspicious objects and the [sources] originating the suspicious objects may be further researched to establish the extent to which they may be a threat." (*Id.* 8:35-38.) As the applicant explained during prosecution, prior art systems may have maintained their own logs of suspicious activity, but the prior art does not disclose reporting suspected sources of pestware to an externally networked entity. (EX-1002 71.) Doing so enables the claimed invention to leverage significantly more resources to research and combat suspected pestware and its sources. None of Petitioner's references disclose this limitation.

3. Level Of Ordinary Skill In The Art

A POSITA at the time of the invention of the '243 patent 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. (EX-2001 ¶¶41-43.) More advanced degrees and/or training in a related discipline can compensate for shorter work experience. (*Id.*)

B. Overview Of The Relevant Prior Art

1. Overview Of Li

Li discloses a unified logging architecture that captures and analyzes correlations among entries on different types of logs on a single computer. Li discloses six different types of logs that often are stored in different formats from different sources, such that insight from cross-log or common analysis is challenging. Li's system ("UCLog") processes the logs through monitors, which audit, filter, and compare the data collected by the various loggers. (EX-1005 at 8). The monitors compare the data with existing models or signatures and send the compressed data to a centralized activity database for management and organization of the data. (EX1005 11.)

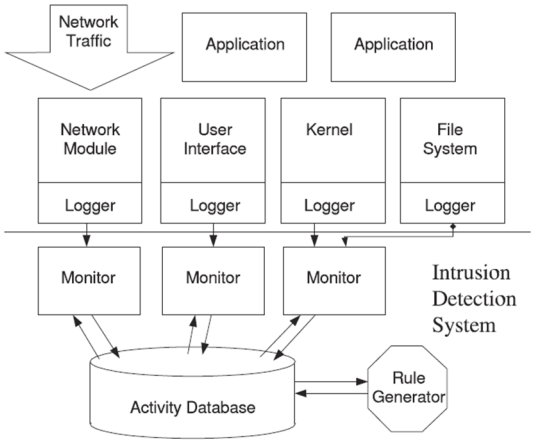

Figure 2. UCLog architecture

The monitors collaborate with other monitors of other loggers by sending queries

through the activity database to find correlated activities. (EX-1005 8, 11.) Based on the queries and correlation, the rule generator "produces the models for normal or abnormal behavior and signatures for previous intrusions." (EX-1005 14.) Rules are stored in the activity database as training data or sent directly to the monitors. (*Id*.)

Unlike the invention of the '243 patent, Li's disclosure ends at identifying a potential pestware object. Li does not disclose identifying an externally networked source of that pestware object. Li also does not disclose reporting the identity of the pestware object or its source to any other entity, let alone an externally networked pestware research entity.

2. Overview Of Hartrell

Hartrell discusses a malware analysis system that initiates after a locally executing anti-malware system detects a suspected infection. (EX-1006 2:39-44) The system takes pre- and post-infection "snapshots" to provide a record of events and activities that occurred so that the collective snapshots can be used by experts to trace the sequence that led to an infection, understand how the infection spread through the system, and observe the impact on the system after the infection. (EX-1006 2:48-57). A "categorization component" of the malware analysis system processes the snapshots and normalizes the snapshot data by labeling and associating activities in the snapshots with predetermined categories of system activities. (EX-

1006 4:30-32). The categorization process can be tuned by an administrator to improve the data's usefulness to a "commonality analysis component," which analyzes the output from the categorization component and labels activities as suspicious or potentially normal. (EX-1006 4:32-37.) An administrator can then mark recurring suspicious activities as malicious. (EX-1006 4:51-53.) A "response recommendation generator" also reviews the commonality analysis component output and makes recommendations for response to the system administrators. (EX-1006 5:13-30.) Based on the analysis of the snapshots, a system administrator can reconfigure the security policies to prevent future infections. (EX-1006 3:8-16.)

Hartrell differs from the invention of the '243 patent. For example, Hartrell is directed at identifying and stopping an *ongoing* malware attack. Hartrell does not disclose identifying the pestware object that may be instigating the attack or the source from which that pestware object *originated*. Hartrell also discloses only sending *recommendations* to other systems with respect to the ongoing attack; it does not disclose sending any information to enable any entity to further investigate a suspected pestware object.

3. Overview Of Yadav

Yadav discloses an integrated intrusion detection system that uses a dynamically controlled firewall for integrated network intrusion detection. Yadav's

system integrates firewall filtering information with network intrusion analysis and monitors blocked network communications, thereby reducing the amount of network traffic that needs to be monitored. (EX-1008 3:1-14.) The system of Yadav only performs intrusion analysis on packets blocked by a firewall. (EX-1008 at 3:5-10). The blocked packets are checked for patterns spanning multiple channels or communication channels. (EX-1008 4:27-30.) An application behaving abnormally is added to a watchlist and monitored more frequently. (EX-1008 4:52-58.)

In Yadav's system, when an unauthorized communication comes in, a copy is sent to the intrusion detector component, and the communication is blocked. (EX-1008 8:25-33). If an intrusion prelude pattern is detected, then the source of the communication is added to the list of potential intruders to be monitored. (EX-1008 8:56-59.)

Based on an administrator's post hoc review of the snapshots, the response recommendation generator generates recommendations, which are made available to system or security administrators. (EX-1008 5:13-30.) The administrators can then decide what corrective measures, if any, to implement based on the recommendations. (*Id*.)

Yadav differs from the invention of the '243 patent. Like Hartrell, Yadav is directed to identifying and stopping an *ongoing* malware attack. Yadav does not

disclose identifying the pestware object that may be instigating the attack or the source from which that pestware object *originated*. Yadav also discloses only sending *recommendations* with respect to the ongoing attack; it does not disclose sending any information to enable any entity to further investigate a suspected pestware object.

4. Overview Of Mandujano

Mandujano discloses a score-based system to determine whether an outbound object is malware using outbound intrusion detection (sometimes referred to as "OID"). Outbound intrusion detection does not protect local resources from being compromised by other systems, but rather prevents local resources from compromising other systems by monitoring outbound activity. (EX-1007 67.) According to Madujano, "[a]n advantage of the OID approach … is broader visibility: a host has total access and control over its own resources." (*Id*. 70.) Specifically, Mandujano discloses using knowledge of the internal structures of a system to detect patterns that indicate abnormal behavior and define signatures of illicit activity. (*Id*. 78.) Armed with a more thorough understanding of the origin of the actual attack program and underlying commands used, an outbound intrusion detection system can provide potential victims with targeted security measures, thereby conserving resources. (*Id*. 71.)

Petitioner does not assert that Mandujano discloses or renders obvious identifying an externally networked source of a potential pestware object or reporting the identity of that source to an externally networked pestware research object. Mandujano does not teach these limitations.

C. THE CHALLENGED CLAIMS ARE PATENTABLE

The petition presents four grounds challenging the claims of the '243 patent:

Ground 1	Section 103(a)	Obvious over Li in view of Hartrell	Claims 1-14
Ground 2	Section 103(a)	Obvious over Li in view of Hartrell and Mandujano	Claims 1-14
Ground 3	Section 103(a)	Obvious over Li in view of Yadav	Claims 1-14
Ground 4	Section 103(a)	Obvious over Li in view of Yadav and Mandujano	Claims 1-14

"In an *inter partes* review, the burden of persuasion is on the Petitioner . . . . Failure to prove the matter as required by the applicable standard means that the party with the burden of persuasion loses on that point—thus, if the fact trier of the issue is left uncertain, the party with the burden loses." *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378-79 (Fed. Cir. 2015); *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (noting that a petitioner has

the "burden from the onset to show with particularity why the patent it challenges is unpatentable").

Petitioner fails to show a reasonable likelihood of success as to any challenged claim because Petitioner has not shown that: (1) Li was publicly accessible before the priority date; (2) any of Petitioners' combinations render obvious every limitation of the challenged claims. Specifically, Petitioner fails to demonstrate that any of the cited prior art, alone or in combination, discloses or renders obvious at least the limitations (1) "identifying… a reference to an identity of an externally networked source of the suspected pestware object;" and (2) "reporting the identity of the particular externally networked source to an externally networked pestware research entity."

1. Ground 1: Petitioner Fails To Establish That Li and Hartrell Renders Obvious Every Limitation of The Challenged Claims

Even if Petitioner had shown that Li were prior art, their first obviousness ground—Li in view of Hartrell—fails for at least three additional reasons: (1) neither Li nor Hartrell discloses or renders obvious "reporting… to an externally networked pestware research entity"; (2) neither Li nor Hartrell discloses or renders obvious "identifying … a reference to an identity of an externally networked source

of the suspected pestware object"; and (3) a POSITA would not have been motivated to combine Li and Hartell.

a) Li and Hartrell do not render obvious "reporting … to an externally networked pestware research entity."

Independent claim limitations 1[e], 6[d], and 12[e] each require "*reporting the identity of the externally networked source to an externally networked pestware research entity*." (EX-1001, cls. 1, 5, 12.)

Claim Limitation	Claim Language
1[e]	*"**reporting the identity of the particular externally networked source to an externally networked pestware research entity** so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware"*
6[d]	*"a reporting portion configured to generate a report that identifies the externally networked source of the file and **to report an identity of the externally networked source to an externally networked pestware research entity** so as to enable the externally networked pestware research entity to research*

	whether the externally networked source is a source of pestware"
12[e]	*"**reporting the identity of the particular externally networked source to an externally networked pestware research entity** so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware"*

Petitioner argues that Li alone and Li in view of Hartrell disclose this limitation. Both arguments fail.

(i) Li Does Not Disclose "reporting… to an externally networked pestware research entity"

Petitioner first argues that Li alone discloses "reporting … to an externally networked pestware research entity." But Li does not disclose an externally networked pestware research entity. As shown in Figure 2, Li's system design does not include any kind of research entity, let alone the claimed externally networked pestware research entity:

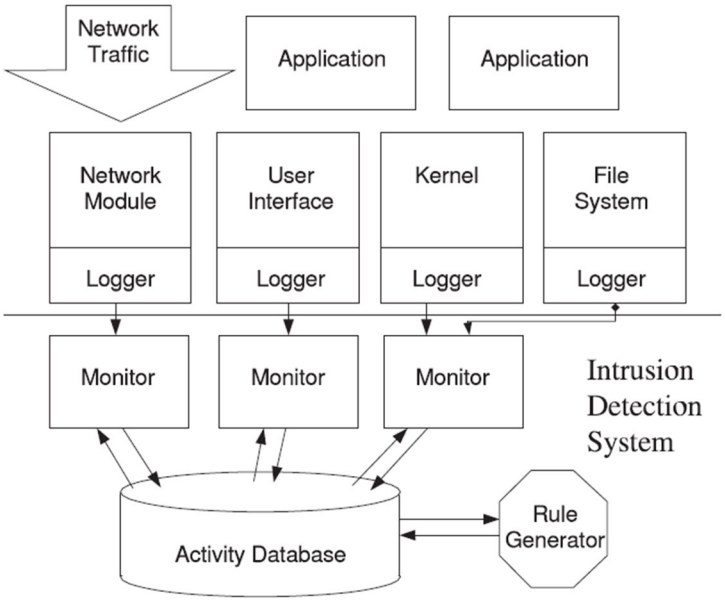

Figure 2. UCLog architecture

(EX-1005 8, Figure 2.)

Petitioner attempts to overcome this shortfall by correlating the claimed "*externally networked pestware research entity"* to Li's disclosure of a human reviewer. Petitioner claims that Li discloses this limitation because "Li states that the user interface of an IDS 'enables an administrator to view the output from the system,'" and because that interface is on a separate system, the administrator is externally networked. (Petition 28.) Petitioner cites nothing to support their speculation that the administrator views the output of the system on a separate, externally networked system.

Contrary to Petitioners' unsupported assertion, a POSITA would not understand a human administrator to be an externally networked pestware research entity. Li does not disclose or even suggest that an administrator reviews the output of the IDS on an externally networked system that might qualify as the claimed "pestware research entity." (EX-2001 ¶56.) To the contrary, Li discloses "running the activity database on a dedicated server" as a solution for sizable databases such as those running "on a large-scale network." (EX-1005 13.) Given this context, a POSITA would have understood that the "dedicated server" would be running *within* that "large-scale network." (EX-2001 ¶68.) Li does not disclose a server of any kind being externally networked, nor any indication that operating the server in such a way would be necessary or advantageous. (*Id.*)

The '243 patent claims all require an "externally networked pestware research entity." (*See* EX-1001, claims 1, 6, 12). Consistent with the claim language, the specification describes a "remote research entity." (EX-1001 9:50-52.) The specification distinguishes the remote research entity from a "research module," which locally searches activity logs and N files for information associating an object's suspicious activity to processes, which are related to "one or more files." (EX-1001 9:37-44.) This search provides information about the identity of the source of a suspicious process and/or files," and the source is then reported to a remote

research entity. (EX-1001 9:50-52.) ("Once the source of the suspicious object(s) is identified (Block **510**), the source is then reported (e.g., to a remote research entity) (Block **512**).")

In this regard, Li is similar to art the applicant distinguished during prosecution, U.S. 2005/0268112 ("Wang"). The applicant distinguished Wang as follows: "the event log described by Wang is not an externally networked pestware research entity. The event log is a file that resides within the computer that runs Wang's Gatekeeper engine software...Wang does not describe providing the event log to any externally networked entity...Further, Wang does not describe providing the event log to any externally networked entity. Rather, the event log and its data remain within the confines of Wang's computer that runs the Gatekeeper engine." (EX-1002 71.) The applicant distinguished the prior art because it addressed activities that were entirely internal to the computer without any external network involved, while the claims recited an externally networked entity. (*Id*.) As shown in Figure 2, all of the IDS activities disclosed by Li are internal to the computer, and involve no externally networked research entity.

(ii) Li In View of Hartrell Does Not Disclose "reporting… to an externally networked pestware research entity"

Petitioner argues in the alternative that Li in view of Hartrell also discloses "reporting… to an externally networked pestware research entity." Petitioner cites Hartrell's disclosure of alerting a system operator to a pattern of infected computer systems and providing recommendations to that same system operator. (Petition 28-29, EX-1006, 5:13-30.) But Hartrell does nothing to cure the deficiencies of Li.

Contrary to Petitioners' argument, a POSITA would not "recognize that the 'system operator' would be on an externally networked research entity." (Petition 28-29.) Hartrell's "system operator" is the operator of another potentially "infected computer system[]," not a research entity. (EX-1006 10:57-58.) Hartrell does not disclose that the system provides the operator with information sufficient to independently perform further research concerning the pestware; rather, the operator is simply "provide[d] a recommendation to block this web site." (*Id.* 10:49 Hartrell also does not disclose that an operator would use her computer system to further investigate the pestware, or that the alert provided would include enough detail to enable her to do so. Nor has Petitioner explained or shown how a human computer operator herself is "externally networked" to the Li computer system apart from the operator's computer. Thus, any connection to an operator's computer system would not recite an "externally networked pestware research entity" that provides a "report" sufficient "to enable the externally networked pestware research entity to

research whether the externally networked source is a source of pestware." (EX-1001, claims 1, 6, 12.)

Petitioner also argues that Hartrell's "centralized data store" satisfies the "externally networked pestware research entity" limitation. In support of this argument, Petitioner incorrectly asserts that Hartrell teaches that "[t]he centralized data store makes use of the website/IP address of the externally networked source to determine whether the externally network[ed] source is a source of pestware." (Petition 29.) Petitioner relies on Hartrell's disclosure of a "commonality analysis process" to support this assertion. (*Id.* (citing EX-1006 3:49-53, 10:44-50).) But Hartrell discloses that its "malware analysis system" conducts this "commonality analysis" to determine whether a particular website may be harmful. Hartrell teaches that its "malware analysis system" [is] running on each of the computer systems," (i.e., it is part of the internal network). It is not part of a separate externally networked entity. (EX-1006 10:36-37.) The malware analysis system then alerts the operators of various computer systems to block the suspicious website. (*Id.* 10:47-50.) Moreover, Hartrell does not disclose or suggest that its malware analysis system reports the results of its analysis to any pestware research entity, let alone an externally networked one, for any purpose, much less the recited purpose of researching whether the externally networked source is a source of pestware.

b) Li and Hartrell do not render obvious "identifying… a reference to an identity of an externally networked source of the suspected pestware object."

Independent claim limitations 1[d], 6[d], and 12[d] each require that the claimed system or method *identify the* "*externally networked source" of the file or pestware object*." (EX-1001, cls. 1, 6, 12.)

Claim Limitation	Claim Language
1[d]	*"accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from* ***so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from****"*
6[d]	*"a reporting portion configured to generate a report* ***that identifies the externally networked source of the file*** *and to report an identity of the externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware"*

12[e]	*"accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from* ***so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from****"*

As with the limitation discussed in the previous subsection, Petitioner argues that Li alone, and Li in view of Hartrell, disclose or render obvious this limitation. Both arguments fail.

(i) Li Does Not Disclose or Render Obvious "identifying… a reference to an identity of an externally networked source of the suspected pestware object"

Petitioner first argues that Li alone discloses the limitation "identifying … a reference to an identity of an externally networked source of the suspected pestware object." But Li contains no such disclosure. Contrary to Petitioners' argument, Li's system is limited to detecting intrusions; Li does not disclose the additional step of attempting to identify the *source* of an intrusion.

Li's system detects the presence of a computer virus by "captur[ing] correlations among entries in different types of logs." (EX-1005 1.) Li refers to various data sources for the log entries it monitors and correlates. For example, Li

discloses monitoring file input and output (or "I/O") at specific files or directories (which Li refers to as "sources") within an internal network. (EX-1005 19-20.) Li describes monitoring and correlating an "additional source"—the c:\recycler\directory—and states that adding this "additional source" could improve IDS accuracy. (*Id*. 20.) Li's disclosure does *not* teach tracing the origin of an object that may have caused the file to be created; rather, it merely generates a warning that the behavior of the *internal directory* is abnormal. *Id*. A POSITA would therefore understand Li's use of the term "source" to mean a data source, such as an internal file or directory. (EX-2001 ¶70.).

Petitioner relies on a single phrase containing the word "source" in Li: that the UCLog can be used to "***identify the source and the execution path of the occurring intrusion***." (Petition at 24 (emphasis in original) (citing EX-1005 at 3, 13).) Leaning on this single phrase—divorced from its context—Petitioner asserts that the "source" described in Li is a "source" of pestware. It is not. Li consistently uses the word "source" to describe a source of *data* gathered by the UCLog, not a source of pestware. Indeed, this is the key innovation described in Li: "UCLog organizes audit data from *heterogeneous sources* into a structured way and is closely integrated into the intrusion detection system." (EX-1005 25.)

Petitioners' preferred quote first appears as part of a single bullet point on page 3 of Li.[1] The first bullet point in that series makes clear what "source" the UCLog is "identify[ing]": "UCLog organizes all ***audit logs from heterogeneous sources*** in a very structured way and is closely integrated into the intrusion detection system." (*Id.* 3.) The remainder of Petitioners' cited language makes clear that the "source" Li refers to is one of the heterogenous sources that feeds the audit logs: "At an intrusion, UCLog can be used to automatically identify the source and the execution path of the intrusion, ***whereas most current systems require an administrator to manually examine the logs to find such information***." (*Id.*) Every other use of the term "source" or "sources" in Li confirms that a "source" is a source of *data* fed into the IDS:

- "… most of the previous work on intrusion detection focuses on activities generated by a single *source* …." (*Id.* 2.)
- "… few studies have been conducted on fusing audit log data from heterogeneous *sources* into a single framework for assessing suspicious behavior." (*Id.*)
- "These systems provide a centralized mechanism to log activities from heterogeneous *sources*…." (*Id.)*

[1] Petitioner incorrectly cites to page 2 of Li. (Petition 24.)

- "For example, it is very common for organizations to have dedicated servers that collect and store logs obtained from different *sources* (e.g. *syslogs* obtained from each host in the organization)." (*Id.* 10.)
- "Besides loggers, a monitor needs to interact with the centralized activity database to find correlated activities from other *sources*." (*Id.* 11.)
- "The database schema is crucial to correlate audit data from different *sources*." (*Id.* 13.)
- "… monitoring and correlating an additional *source* can help to improve the IDS accuracy."(*Id.* 20.)
- "Their study only monitors file I/O operations, whereas UCLog monitors activities from multiple *sources*." (*Id.* 23.)
- "… to improve IDS accuracy by correlating information from different and preferably disjoint *sources*." (*Id.* 25.)
- "UCLog organizes audit data from heterogeneous *sources* into a structured way…." (*Id.*)

None of Li's references to "source" or "sources"—including those identified by Petitioners—disclose or even relate to an externally networked source of a suspected pestware object.

Petitioner also argues, based on Li's disclosure, that it "would have been obvious to a POSITA to check the source IP address" of packet headers stored in the "WinDump Log" in order to "see from where the malware came [and] to identify a

potentially malicious internet source." (Petition at 26.) This argument fails for at least two reasons.

First, Petitioner fails to explain why a POSITA would be motivated to use packet headers stored in the WinDump Log to identify the source of an intrusion. As discussed above, Li is directed to a system for detecting the presence of an intrusion within a network, not obtaining additional information about the intrusion. Indeed, Li does not address identifying the *source* of an intrusion. Rather, Li is singularly focused on improving systems to detect intrusions themselves: "most of the previous work on intrusion detection focuses on activities generated by a single source, *resulting in many false positives and undetected intrusions*." (EX-1005 2.) Li does not disclose any reason why tracing back to the source of an intrusion once it has been identified would improve its intrusion detection system, for example by reducing either false positives or undetected intrusions. (*See generally*, EX-1005.)

Second, even if Petitioner was correct that POSITA would have been motivated to manually examine one of Li's data sources to identify an intrusion's source—which they would not have been—such a manual identification would not satisfy all limitations of any challenged claim. As discussed above in Section IV.C.1.a), the '243 patent's independent claims all require *reporting* the identity of an externally network source to an externally networked pestware research entity.

Petitioner does not explain how, under their Li-based obviousness theory, the results of a POSITA's source analysis would subsequently be reported to any entity at all. In fact, because neither Li nor Hartrell discloses identifying a pestware source through manual analysis by a human, neither discloses reporting the *results* any such analysis to an externally networked pestware research entity. Petitioners' argument that Li renders this limitation obvious for this additional reason.

Thus, Li does not disclose or render obvious "identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object."

(ii) Li In View of Hartrell Does Not Disclose "identifying… a reference to an identity of an externally networked source of the suspected pestware object"

Petitioner next argues in the alternative that Li in view of Hartrell also discloses "identifying … a reference to an identity of an externally networked source of the suspected pestware object." But Hartrell cannot cure the deficiencies of Li because Hartrell does not address pestware objects at all, let alone "an identity of a particular externally networked source that ***the suspected pestware object originated from***." (*E.g.*, EX-1001, claim 1.)

Hartrell's "malware analysis system" "monitors and records computer system *activities*." (EX-1006 Abstract.) There is no disclosure or suggestion of tracing a

specific *object* back to an externally networked source. The "objects" described in Hartrell are not pestware objects but "operating system objects that were manipulated." (*Id.* 3:6-7.) In other words, the "objects" identified by Hartrell are targets or victims of pestware, not pestware themselves.

Determining that "four infected machines visited the same web site prior to being infected" does not disclose or suggest identifying a "pestware object" that caused the infection. (*Id.* 3:48-49.) Hartrell's "commonality analysis" merely identifies that several systems visited the same website and subsequently became infected. This disclosure does not disclose or render obvious tracing any particular pestware object back to that source. Because Hartrell does not disclose identifying a pestware object, it also does not disclose identifying the externally networked source ***of*** a pestware object.

Even if the website identified by Hartrell's "commonality analysis" were an identified source of a pestware object (it is not), the methods taught by Hartrell to identify this information do not teach the relevant claim limitations. Hartrell's commonality analysis requires correlating data from *several* computer systems to identify a potentially malicious website that all of them visited. (EX-1006 3:47-51.) This does not meet the limitations of the '243 patent, which require identifying a source of pestware by analyzing the activity log of a *single* computer. (EX-1001

3:34-38.) The claims of the '243 patent recite that it is the "recorded information on the computer that relates the at least one file to an externally networked source." (EX-1001 at claim 6; *see also id.* at claim 1, 12 ("accessing … a portion of a recorded history … to identify a reference to an identity of a particular externally networked source".) The specification makes clear that identifying a relationship between the pestware object and its source means identifying a relationship between the two *within* the activity log. For example, "if the originating URL is stored in connection with the file, the URL is identified as the source of the file." (*Id.* 7:50-52.) Hartrell does not disclose identifying any such relationship. Hartrell merely flags websites that all infected computers visited, without tracing that website to the suspected pestware object via the activity logs.

c) Petitioner fails to show that a POSITA would have been motivated to Combine Li with Hartrell.

Even if the Li/Hartrell combination disclosed or suggested "identifying… a reference to an identity of an externally networked source of the suspected pestware object," which it does not for the reasons discussed in the previous section, Petitioner fails to demonstrate any motivation to combine Li and Hartrell. Petitioner asserts that a POSITA would be motivated to "aggregate the system-wide unified log information disclosed in Li within the centralized database described in Hartrell." However, Li *already discloses* an "activity database" to aggregate log information.

(EX-1005 12-14.) Li expressly contemplates that such a log may be used in a "large-scale network"—that is, a network running multiple computers—and offers solutions to manage such network-wide logging in an efficient manner. (*Id.* 13-14.) Petitioner fails to explain why a POSITA would abandon the database disclosed in Li for a different database, much less explain what advantages Hartrell's database offers over Li's.

Petitioner asserts that a combination of Li and Hartrell would "aggregate the system-wide unified log information disclosed in Li with the centralized database described in Hartrell." (Petition 17.) But Li by itself already does this. Li's activity database already "stores and manages audit data," which comes from the system-wide loggers, "in a very organized way." (EX-1005 12.) If a POSITA's motivation were to correlate system-wide data, the POSITA would not have needed to look anywhere else but Li.

Moreover, a POSITA would not have been motivated to substitute Hartrell's "centralized data store" for Li's "activity database" because the two operate differently and achieve different goals. Li's activity database aggregates *heterogenous* information from a variety of *different* types of data loggers on a *single* system to identify a potential intrusion. (*See* EX-1005 10-12 (identifying various types of loggers); *id.* 13 (explaining how the activity databased correlates this

disparate information); EX-2001 ¶69.) Conversely, Hartrell aggregates "normalize[d]" or *homogenous* information from the *same* types of data loggers on *multiple* systems to identify potential intrusions affecting all the systems. (*See* EX-1006 10:36-50 (describing a "commonality analysis" on "normalize[d] … snapshot data" from "ten computer systems"; (EX-2001 ¶ 69.) These systems operate in opposite ways. (*Id.*) They are not interchangeable. (*Id.*) Therefore, a POSITA would not have been motivated to attempt to substitute one for the other. Petitioners' obviousness combination of Li and Hartrell fails for this additional reason.

2. Ground 2: Petitioner Fails To Establish That Li, Hartell, And Mandujano Render Obvious Every Limitation Of The Challenged Claims

Ground 2 fails for the same reasons as Ground 1. In Ground 2, Petitioner argues in the alternative that adding Mandujano to their Li/Hartrell combination renders obvious claim limitations [1B] and [1C] and their corresponding limitations in independent claims 6 and 12, reproduced below:

Claim Limitation	Claim Language
1[b]	"*analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware*"

1[c]	*"identifying, based upon the activity, an object residing on the computer that is a suspected pestware object"*
6[b]	*"a heuristics module configured to identify an activity on the computer that is indicative of pestware residing on the computer and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold"*
12[b]	*"analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware"*
12[c]	*"identifying, based upon the activity, an object residing on the computer that is a suspected pestware object."*

Petitioner does not contend that Mandujano adds anything to the Li/Hartrell combination with respect to the "externally networked pestware research entity" and "externally networked source" requirements of claim limitations [1D] and [1E], respectively, and the corresponding claim 6 and 12 limitations. Because the Li/Hartrell combination does not render those limitations obvious for the reasons addressed above in Sections IV.C.1.a)-3, Petitioners' second obviousness ground fails for the same reasons as the first.

3. Ground 3: Petitioner Fails To Establish That Li And Yadav Render Obvious Every Limitation Of The Challenged Claims

For their third obviousness ground, Petitioner substitutes Yadav for Hartrell in the Lee/Hartrell combination of Ground 1, arguing that "Yadav would replace Hartrell in a similar combination with Li" for the following subset of limitations for which Petitioner relied on Hartrell in their first ground: 1[p]; 1[d]; 1[e]; 2[a]; 4[a]; 5[a]; 6[p]; 6[c]; 6[d]; 12[p]. (Petition 59-66.) But just as with the Li/Hartrell combination, Petitioners' Li/Yadav combination fails because (1) Yadav does not disclose or render obvious "reporting… to an externally networked pestware research entity;" (2) Yadav does not disclose or render obvious "identifying… a reference to an identity of an externally networked source of the suspected pestware object;" and (3) a POSITA would not have been motivated to combine Li and Yadav.

a) Petitioner fails to show that Li in view of Yadav renders obvious "reporting the identity of the particular externally networked source to an externally networked pestware research entity."

Petitioner fails to show that Yadav discloses reporting *of any kind* to an externally networked pestware research entity. Petitioner states that Yadav may "***report the intrusion to the central security server 292***." (Petition 61 (emphasis in original) (citing EX-1008 10:25-28).) But this singular reference to a "central security server" would not have suggested to a POSITA that Yadav's central security

server functions as a "pestware research entity." (Petition 61 (citing EX-1008 10:25-28).) Nor do Petitioner cites anything that would have suggested to a POSITA that Yadav's central server is externally networked. On the contrary, Yadav discloses that a key aspect of "network security is to install a firewall, which restricts and controls the flow of traffic between networks, *typically between an enterprise network and the Internet*." (EX-1008 1:51-54.) Yadav is expressly directed to "integrating firewall filtering information with network intrusion analysis" by "performing intrusion analysis on packets blocked by a firewall." (*Id.* 3:1-10.) In other words, the express purpose of Yadav is to protect an internal network (an enterprise network) from an external network (the internet). Given this context, it is clear that the "central security server" would be part of the internal network.

In short, Yadav does not disclose or suggest that its "central security server" is a pestware research entity, or is externally networked.

b) Petitioner fails to show that Li in view of Yadav renders obvious "identifying… a reference to an identity of an externally networked source of the suspected pestware object."

Li fails to disclose or suggest identifying an "externally networked source of the suspected pestware object…" for the reasons described above with respect to Ground 1. *See* Section IV.C.1.b) *supra*. Yadav does not cure this deficiency.

Yadav does not disclose or suggest identifying an "externally networked source of a suspected pestware object" because Yadav does not address pestware objects at all. The '243 patent describes its invention in part as "identifying … an object *residing on the computer* that is a suspected pestware object." (EX-1001 2:21-22.) It further explains that pestware is a "type of program[]." (*Id.* 1:43-54.) The claimed invention attempts to identify "a particular source that the suspected pestware object *originated from*." (*Id.* 2:25-26.) Petitioner points to no disclosure in Yadav that identifies a program residing on the computer that is a suspected pestware object, let alone any disclosure of an attempt to identify the origin of the suspected pestware object.

Rather than attempting to identify the source of a program residing on the computer, Yadav discloses identifying "a source of [an] intrusion prelude," as Petitioner notes. (Petition 60 (citing EX-1008 4:31-41).) An "intrusion" is defined by Yadav as "an attempt to break into and/or misuse a computing system," while an "intrusion prelude" is defined as "communication activities that typically precede an intrusion." (EX-1008 2:60-63.) In other words, Yadav discloses identifying and stopping an *ongoing* attempt to access or misuse the computer. By contrast, the '243 patent claims recite identifying an externally networked source of a suspected pestware object.

c) Petitioner fails to show that a POSITA would have been motivated to combine Li with Yadav.

Petitioner fails to demonstrate sufficient motivation to combine Li and Yadav. Petitioner asserts that a POSITA would have been motivated to "aggregate the log information, including information about the source of pestware, within the central security server described in Yadav." (Petition 58.) However, Li *already discloses* an "activity database" to aggregate log information. (EX-1005 12-14.) Li discloses "combining information from multiple computers in a central server." (Petition 58.) Li expressly contemplates that its IDS may be used in a "large-scale network"—that is, a network running multiple computers—and offers solutions to manage such network-wide logging in an efficient manner. (EX-1005 13-14.) This includes loggers that obtain "system-wide information," i.e., information from multiple computers, all of which is accessible via Li's activity database. (*Id.* 10.) Yadav's "central server" achieves nothing not already accomplished by Li's "activity database." Thus, Petitioner fails to explain why a POSITA would abandon the database disclosed in Li for a different database, much less explain what advantages the central server of Yadav offers over Li's activity database.

Moreover, a POSITA would not look to Yadav to modify Li because the two differ in their purpose and implementation. While Li focuses on holistic analysis and correlation of logs to understand system activities, Yadav focuses on targeting

malicious activities and unauthorized access attempts on specific network traffic channels. (*Compare* EX-1005 at 8 *with* EX-1008 at 3:5-10.) Li aims to provide a comprehensive view of system activities to improve long-term analysis, prevention, and response, while Yadav monitors only a small subset of network traffic to react in real time. (EX-2001 ¶84.) Yadav teaches that monitoring "only a small portion of network communications … blocked by a firewall." (EX-1008 3:3-10.) Li criticizes this approach and instead advocates a holistic multi-data-stream approach: "most of the previous work on intrusion detection focuses on activities generated by a *single source*, resulting in many false positives and undetected intrusions." (EX-1005 2.) A POSITA would not be motivated to improve upon Li by looking to the same types of systems that Li criticized.

A POSITA would not have looked to an intrusion detection system focused on real-time reactions to unauthorized network traffic to modify the log correlation system in Li. (EX-2001 ¶88.) A POSITA would not have looked to a system with a much more restricted scope to fulfill the now-perceived shortfalls of the whole-system approach disclosed in Li. (*Id.*) Certainly, a POSITA would not have looked to Yadav's system for an externally networked pestware research entity since such an entity was not disclosed in Yadav. (*Id.*) Thus, even if POSITA had sought to modify Li to incorporate an externally networked pestware research entity (they

would not have), they would not have turned to Yadav for guidance. (*Id.*) Petitioner thus falls short of meeting their burden to show that a POSITA would have modified Li based on the teachings of Yadav to disclose or render obvious any limitation of the challenged claims.

4. Ground 4: Petitioner Fails To Establish That Li, Yadav, And Mandujano Disclose Or Render Obvious The Independent Claims Of The '243 Patent

Ground 4 fails for the same reasons as Ground 3. In Ground 4, Petitioner argues in the alternative that adding Mandujano to their Li/Yadav combination renders obvious claim limitations [1B] and [1C] and their corresponding limitations in independent claims 6 and 12, reproduced below:

Claim Limitation	Claim Language
1[b]	"*analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware*"
1[c]	*"identifying, based upon the activity, an object residing on the computer that is a suspected pestware object"*
6[b]	*"a heuristics module configured to identify an activity on the computer that is indicative of pestware residing on the computer and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold"*

12[b]	*"analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware"*
12[c]	*"identifying, based upon the activity, an object residing on the computer that is a suspected pestware object."*

Petitioner does not contend that Mandujano adds anything to the Li/Yadav combination with respect to the "externally networked source" and "externally networked pestware research entity" requirements of claim limitations [1D] and [1E], respectively, and the corresponding claim 6 and 12 limitations. Because the Li/Yadav combination does not render those limitations obvious for the reasons addressed above in Sections IV.C.3.1-3, Petitioners' second obviousness ground fails for the same reasons as the first.

a) Mandujano does not cure the deficiencies of Li and Yadav identified in Ground 3.

In Ground 4, Petitioner relies upon Mandujano to support disclosure of limitations 1B, 1C, 6B, 12B, and 12C. Because Petitioner does not rely upon Mandujano to support any of the limitations that are not disclosed in Ground 3, Ground 4 fails for the same reasons described above.

b) Petitioner fails to identify any motivation to combine Li, Yadav, and Mandujano.

Petitioner summarily explains that "A POSITA would have been motivated to combine the teachings of Li and Yadav with Mandujano for the same reasons a POSITA would have been motivated to combine Li, Hartrell, and Mandujano." Hartrell and Yadav are two different references. Petitioner offers no explanation at all for why a POSITA would substitute the two in this combination. Petitioner has failed to meet their burden to show motivation to combine.

To the extent the Board entertains Petitioners' summary argument, it fails for the reasons explained in Ground 2. *See* section IV.C.2 *supra*.

5. Petitioners' Grounds Fail To Render Obvious All Dependent Claims

Because Petitioner has failed to establish that any of its grounds render obvious all limitations of the independent claims, Petitioner cannot show that such grounds render obvious dependent claims 2-5, 7-11, or 13-14.

6. Other Limitations Not Addressed

At this preliminary stage, Patent Owner addresses those deficiencies in the prior art which clearly show a lack of reasonable likelihood of the petition's success. Patent Owner's decision not to address certain limitations at this preliminary stage in no way reflects Patent Owner's agreement with the petition or lack of dispute as to additional limitations.

7. There Are Secondary Objective Indicia Of Nonobviousness

Patent Owner contends that secondary objective indicia of nonobviousness exist and reserves its right to provide evidence on this point, should the Board institute.

V. CONCLUSION

For the foregoing reasons, the Board should deny institution.

Date: March 22, 2024

Respectfully submitted,

KING & SPALDING LLP

/Brian Eutermoser/

Brian Eutermoser
Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER PRELIMINARY RESPONSE** specified in 37 C.F.R. § 42.24 have 10,824 words, in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24. This word count was prepared using Microsoft Word 365 V.2022.

Date: March 22, 2024

Respectfully submitted,

KING & SPALDING LLP

/Brian Eutermoser/

Brian Eutermoser
Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER PRELIMINARY RESPONSE** and all supporting **EXHIBITS 2001-2007** were served by filing the documents through the Patent Trial and Appeal Case Tracking System (P-TACTS) on March 22, 2024 and courtesy copies were also served via electronic mail, in their entireties on the following:

Josh Krevitt (*pro hac vice*)
Gibson, Dunn & Crutcher LLP
1881 Page Mill Road
Palo Alto, CA 94304-1211
Tel: (212) 351-2490
JKrevitt@gibsondunn.com

Kate Dominguez (*pro hac vice*)
Gibson, Dunn & Crutcher LLP
200 Park Avenue
New York, NY 10166-0193
Tel: (212) 351-2338
KDominguez@gibsondunn.com

Brian A. Rosenthal (*pro hac vice*)
Gibson, Dunn & Crutcher LLP
200 Park Avenue
New York, NY 10166-0193
Tel: (212) 351-2339
BRosenthal@gibsondunn.com

Timothy P. Best (*pro hac vice*)
Gibson, Dunn & Crutcher LLP
333 South Grand Avenue
Los Angeles, California 90071-1504
Tel: (213) 229-7659
TBest@gibsondunn.com

Counsel for Petitioners
Sophos Ltd. and Sophos Inc.

Date: March 22, 2024

KING & SPALDING LLP

/Brian Eutermoser/

Brian Eutermoser
Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.