UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SOPHOS, INC.,

Petitioner,

v.

FINJAN, INC.,

Patent Owner.

Case IPR2015-01022

Patent 8,677,494

PATENT OWNER'S PRELIMINARY RESPONSE
UNDER 37 C.F.R. § 42.107

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

On April 8, 2015, Sophos Inc. ("Petitioner") submitted a Petition to institute *inter partes* review ("IPR") of U.S. Patent No. 8,677,494 ("the '494 Patent"), challenging claims 1, 10, 14, and 18. Finjan Inc. ("Patent Owner") requests that the Board not institute *inter partes* review because Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing unpatentability of any of the challenged claims on the grounds asserted in its Petition, as required under 37 C.F.R. § 42.108(c).

The '494 Patent generally discloses systems and methods for protecting user computers from the suspicious operations that may be attempted by Downloadables. The claims require, *inter alia*, "receiving an incoming Downloadable," "deriving security profile data for the Downloadable" and "storing the Downloadable security profile data in a database." Ex. 1001 at 19–25. The Downloadable security profile ("DSP") data that is generated and stored in the database also must include "a list of suspicious computer operations that may be attempted by the Downloadable." (Id.).

The various references cited in Grounds A–D of the Petition do not disclose this approach to protect against malware because they do not derive security profile data for a Downloadable, a list of suspicious computer operations, or store Downloadable security profile data in a database. In contrast, the references cited

in the Petition are generally directed to identifying viruses that infect files of a computer system, (e.g., by running virus scans on the computer system) rather than determining the suspicious operations that a Downloadable intends to perform and then further including a list of these specific operations within a security profile that is generated for that Downloadable and then further storing the claimed security profile in a database. (*See* Ex. 1006 at 161). The *TBAV* reference explains that a virus is a computer program that appends itself to the end of the program it infects. (Id.). Petitioner repeatedly conflates virus signatures for ***viruses that infect files*** with the claimed Downloadable security profile data ***derived from the Downloadable***. In addition to these fundamental differences between Finjan's approach to protecting computers form malicious and those proposed in the Petition's cited references, Finjan notes a number of substantive and procedural reasons that the Board should decline to institute *inter partes* review.

First, the Board should decline to institute *inter partes* review of the challenged claims because Petitioner has failed to "specify where each element of the claim is found in the prior art patents or printed publications relied upon." (37 C.F.R. § 42.104(b)). For example, the Petition completely neglects to specify where any of the cited references disclose the feature of "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable," which is recited in each challenged

claim. Petitioner appears to hope that the Board will simply ignore this claim element, which as noted above, is at the heart of what distinguishes Finjan's approach with those of the prior art cited in the Petition.

Second, every one of Petitioner's assertions of obviousness based on combinations of the various references is inadequate as a matter of law. Each of Petitioner's statements regarding the motivation to combine one or more references is based on the references generally being directed to similar subject matter. *See, e.g.*, Petition at 27 ("TBAV and Ji are both directed to virus scanning software that can scan incoming downloaded files. Thus, at a minimum, it would have been obvious to one of ordinary skill in the art to apply the teachings of a receiver in Ji to the system of TBAV. (Ex. 1002 at ¶ 96)"). Each proposed Ground is, therefore, deficient as a matter of law because Petitioner improperly provides "mere conclusory statements" that the combinations are obvious rather than "articulating rational underpinning to support the legal conclusion of obviousness." *See KSR v. Teleflex*, 550 U.S. 398, 418 (2007).

Third, Petitioner impermissibly attempts to circumvent the page limits dictated under 37 C.F.R. § 42.24 by using claim charts to incorporate by reference broad passages of the references and by placing attorney argument in the claim charts in lieu of quotations of the evidence. These techniques are improper because Petitioner cannot impose on the Board "to re-construct Petitioner's

arguments and generally play archaeologist with the record." IPR2014-00475, Paper No. 10 at 14–16.

Although there are a variety of reasons why the '494 Patent is valid over Petitioner's asserted prior art references, this Preliminary Response focuses on only limited reasons why *inter partes* review should not be instituted. *See Travelocity.com L.P. et al. v. Conos Technologies, LLC*, CBM2014-00082, Paper 12 at 10 ("[N]othing may be gleaned from the Patent Owner's challenge or failure to challenge the grounds of unpatentability for any particular reason."). The deficiencies of the Petition noted herein, however, are sufficient for the Board to find that Petitioner has not met its burden to demonstrate a reasonable likelihood that it would prevail in showing unpatentability of any of the challenged claims.

II. THE '494 PATENT

A. Overview

Patent Owner's '494 Patent claims priority to a number of patents and patent applications, including U.S. Patents Nos. 6,804,780 (Ex. 1014), 6,092,194 (Ex. 1015), and 6,480,962 (Ex. 1016), with an earliest claimed priority date of November 8, 1996. (Ex. 1001 at 1:8–55). The '494 Patent incorporates each of these patents by reference.

The systems and methods of the '494 Patent protect personal computers (PCs) and other network accessible devices from "harmful, undesirable, suspicious

or other 'malicious' operations that might otherwise be effectuated by remotely operable code." (Ex. 1001 at 2:51–56). The protection paradigm involves deriving security profile data for an incoming Downloadable. (Ex. 1001 at 21:21; Ex. 1015 at 5:38–45; 9:20–22).

The Downloadable security profile ("DSP") data for each Downloadable includes a "list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable." (Ex. 1015. at 5:45–48). Additional information about the Downloadable can also be stored in the database, such as the date and time the profile was derived and URL from which the downloadable originated. (Ex. 1001 at 21:26–28; id. at 21:38–40). The DSP data can be derived in number of different ways, including by disassembling the machine code of the Downloadable. (Ex. 1015 at 9:20–24).

DSP data for a Downloadable is therefore derived from a particular Downloadable and is related to the Downloadable itself unlike, for example, a virus signature, which identifies a particular virus that can **infect** executable file. *See* Ex. 1008 at 9:16–19 ("A 'good' viral signature is one which is statistically unlikely to generate false positives when run on uninfected, legitimate programs, but will always identify the virus if it is present."). Security policies, which include policies specific to particular users and generic policies, can be compared

with the DSP data for an incoming Downloadable to determine whether to allow or block the incoming Downloadable. (Ex. 1015 at 4:18–24).

The derived DSP data is stored in a database. (Ex. 1001 at 21:24–25; Ex. 1015 at 4:14–19; 9:52–55). Because DSP data stored in this manner can be efficiently retrieved when a known Downloadable is encountered, the invention claimed in the '494 Patent allows accurate security decisions to be made without the need to generate profiles for all incoming Downloadables; additionally, there is no need for the Downloadable to be scanned for malicious operations at the destination device since the DSP data already lists malicious operations that may be attempted by the Downloadable, unlike the *TBAV*, *Chen*, and *Arnold* references, which all merely scan files already resident on a destination device. (*See* Ex. 1001 at 11:1–7).

B. The Prior Art

In stark contrast to the invention claimed in the '494 Patent, the prior art discloses methods for **identifying viruses** that infect files rather than deriving security profile data for incoming Downloadables. *See* Ex. 1006 at 1 ("[TBAV] is a comprehensive tool kit designed to protect against, and recover from, computer viruses."); id. at 161 ("A virus, which is simply another computer program, adds itself to the end of the program it infects."); Ex. 1008 at 2:26–29 ("[A] need has arisen to develop methods for automatically recognizing and eradicating previously

unknown or unanalyzed viruses on individual computers and computer networks."); Ex. 1009 at 9:1–2 (describing that a temporarily stored file is analyzed to determine if it contains a virus); and Ex. 1010 at Abstract ("The detection and removal of viruses from macros is disclosed.").

The cited references disclose two main methods of identifying viruses—signature scanning and heuristic scanning—neither of which corresponds to Finjan's approach as claimed in the '494 Patent. Signature scanning checks "for the appearance of [virus] signatures in a file" to find out of a program has been infected. (Ex. 1006 at 47). A virus signature is a "unique sequence of instructions" rather than either security profile data for a Downloadable or a list of suspicious operations that may be performed by the Downloadable. (Id.).

Heuristic scanning, on the other hand, is used to detect unknown viruses by detecting "suspicious instruction sequences" in a file. (Id. at 154). The actual virus detection is executed by assigning every suspicious instruction a heuristic flag that denotes a score; the score is then compared to a predefined limit. (Id. at 155). The heuristic scanning processes disclosed in the cited references do not derive security profiles for Downloadables, let alone security profiles for Downloadables that include a list of suspicious computer operations that may be performed by the Downloadable.

C. Challenged Claims

Petitioner challenges four claims of the '494 Patent, namely independent method claim 1, independent system claim 10, and claims 14 and 18, which depend from claim 10. Claim 1 is reproduced below:

> 1. A computer-based method, comprising the steps of:
>
> receiving an incoming Downloadable;
>
> deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and
>
> storing the Downloadable security profile data in a database.

(Ex. 1001 at 21:19–25). System claim 10 further recites the components "receiver," "Downloadable scanner," and "database manager." (*Id*. at 22:7–16). Claim 14 recites "wherein the Downloadable includes program script." (*Id*. at 22:26–27). Claim 18 recites "wherein said Downloadable scanner comprises a disassembler for disassembling the incoming Downloadable." (*Id*. at 22:37–39).

D. Prosecution History

The '494 Patent issued March 18, 2014, from U.S. Patent Application Serial No. 13/290,708, filed November 7, 2011.

III. CLAIM CONSTRUCTION

A. **"Downloadable"** (claims 1, 10, 14, and 14):

The proper construction of the term "Downloadable" in the context of the '494 patent is "an executable application program, which is downloaded from a

source computer and run on the destination computer." This is the exact definition provided in U.S. Patent Nos. 6,804,780 (Ex. 1014) and 6,092,194 (Ex. 1015), which the '494 patent is a continuation of, claims priority to, and incorporates by reference. (Ex. 1001 at 1:27–39; Ex. 1014 at 1:50–53; Ex. 1015 at 1:44–46). In fact, Petitioner already agreed to this definition in the concurrent litigation with Patent Owner (Finjan). (Ex. 2001 at 2).

Petitioner provides no explanation for modifying the previously agreed upon construction and, indeed, states that its proposed construction is consistent with the '494 Patent. (*See* Petition at 12–13). To the extent that Petitioner inserts the phrase "can be" to obscure the fact that Downloadables are programs that are intended to be run on destination computers, Finjan disagrees.

B. "suspicious computer operations" (claims 1, 10, 14, and 18)

The term "suspicious computer operations" needs no construction and the plain and ordinary meaning within the context of the claims should apply. *See, e.g., Interactive Gift Express, Inc. v. Compuserve, Inc.*, 256 F.3d 1323, 1331 (Fed. Cir. 2001) ("If the claim language is clear on its face, then our consideration of the rest of the intrinsic evidence is restricted to determining if a deviation from the clear language of the claims is specified."). This term "suspicious computer operations" appears in all of the challenged claims with its scope clearly set forth in the claims. For example, independent claims 1 and 10 recite claims recite "a list

of suspicious computer operations that may be attempted by the Downloadable" and that this "list" is included in the claimed "security profile data"[1] that is derived for the Downloadable. *See, e.g.*, claim 1(b) (reciting "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable")

Petitioner proposes that the term "suspicious computer operations" should mean "computer instructions that are deemed to be potentially hostile." Petitioner provides no reason to replace the common, well-understood term "computer operations" with "instructions." In fact, none of Petitioner's citations to the '494 Patent or to Finjan's '639 Provisional Application, mention the term "instruction." Rather, the true motivation for Petitioner's construction is because its proposed grounds rely upon the references' various disclosures of suspicious instructions to meet the claimed "suspicious computer operations." *See, e.g.*, Petition at 24, 40, and 46. Thus, Petitioner's construction serves no purpose at all except, to

[1] Notably, Petitioner improperly treats the term "security profile data for the Downloadable" as if it does not exist, and only asserts that the prior art teaches "a list of suspicious computer operations" and thus contrary to the well-established rule that "claims are interpreted with an eye toward giving effect to all terms in the claim." *Digital-Vending Services International, LLC v. The University of Phoenix, Inc.*, No. 11-1216 (Fed. Cir. Mar. 7, 2012)

improperly replace the inventor's chosen words in favor of words recited in its proposed prior art.

Petitioner's proposed construction should also be rejected because computer instructions are not "computer operations that may be attempted by the Downloadable." An instruction is a low-level programmatical construct, while an operation is a high-level command that the program actually performs. This distinction is reinforced by the claim language, which recites "computer operations ***that may be attempted by the Downloadable***" as well as the specification, which differentiates between "remotely operable code" and the "harmful, undesirable, suspicious or other 'malicious' operations that might otherwise be effectuated by remotely operable code." (Ex. 1001 at 2:54–64). Likewise, the '194 Patent describes the difference between machine code and the suspicious operations:

> Method 628 begins in step 705 with the code scanner 325 disassembling the machine code of the Downloadable. The code scanner 325 in step 710 resolves a respective command in the machine code, and in step 715 determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. 3).

(Ex. 1015 at 9:22–29).

C. "database" (claims 1, 10, 14, and 18)

Finjan submits that the proper construction of "database" is "a collection of interrelated data organized according to a database schema to serve one or more applications." This construction stays true to the claim language and most naturally aligns with the patent's description of the invention as well as the well-accepted definition of the term. (Ex. 2002 at 3). In fact, the district court in the concurrent litigation with Petitioner indicated that Patent Owner's construction follows the context of the patent and the well-understood accepted definition for database: "[b]ecause Finjan's definition appears to reflect both the context of the patent as well as a well-accepted definition of the term." (Ex. 2003 at 7).

Petitioner proposes to construe the term "database" as "any structured store of data" under the BRI. (Petition at 13). However, the Federal Circuit has held that "even with a more lenient standard of proof, the PTO ideally should not arrive at a different conclusion." *In re Baxter Int'l*, 678 F.3d 1357, 1365 (Fed. Cir. 2012). The goal of Petitioner's construction is to broaden the term database beyond the specification so that it reads upon the techniques described in the cited prior art (e.g. a log file). To the contrary, the Federal Circuit dictates that the broadest reasonable interpretation requires consideration of specification. *See Microsoft Corp. v. Proxyconn, Inc.*, Nos. 2014-1542, 2014-1543, 2015 WL 3747257, at *3 (Fed. Cir. 2015)("[A] construction that is 'unreasonably broad' and

which does not 'reasonably reflect the plain language and disclosure' will not pass muster."). FIG. 3 of the '194 Patent clearly illustrates that the security database 240 that stores DSP data 310 is completely different than a log file (i.e. Event Log 245), which would be captured under Petitioner's overbroad construction:

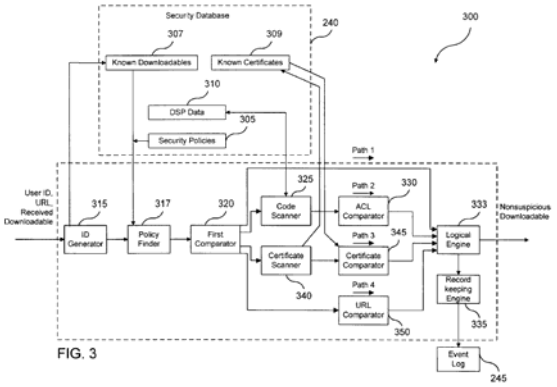

FIG. 3

Furthermore, the portion of the '494 Patent cited by Petitioner only reinforces Finjan's proposed construction by referring to referencing list separately from a database. Ex. 1001 at 17:10-13 (stating that a "referencing list, database or other storage structure(s)…" can be used to implement a protection scheme). The district court in the concurrent litigation has also rejected equating a database with a log file:

> The fact that a database is listed along with more simple files ***does not mean that the database includes or is equated with these types of files***. In fact, one could argue that this list serves to further differentiate a database from simpler files.

(Ex. 2003 at 5, n.1)(emphasis added).

Because there is no support for Petitioner's broader construction of "database" in the '494 patent, the PTAB should adopt Patent Owner's construction as following the '494 patent, adopted well-understood definition, and the law.

D. "program script" (claim 14)

Finjan submits that the term "program script" means "a program written in a scripting language (e.g. JavaScript™/Visual Basic scripts)." This construction is consistent with the '494 Patent, which lists examples of remotely operable code, including "downloadable application programs, Trojan horses and program code groupings, as well as software 'components,' such as Java™ applets, Active X™ controls, JavaScript™/Visual Basic scripts, add-ins, etc., among others." (Ex. 1001 at 2:59–64). This passage identifies JavaScript™/Visual Basic scripts separately from other software components, such as Java™ applets, Active X™ controls, and add-ins. (Id.).

Petitioner proposes that under the BRI, this claim feature should mean "a set of instructions that can be executed by a computer through an interpreter or some other program with a computer." (Petition at 14). However, the standard for claim construction to be applied in *inter partes* review is the broadest reasonable interpretation that a person of ordinary skill in the art would give the ***term in the context of the specification*** and ***in light of its ordinary meaning in the art***. 37 C.F.R. § 42.100(b); *In re Cuozzo Speed Techs., LLC*, 778 F.3d 1271, 1279-82 (Fed.

Cir. 2015). Although Petitioner asserts that its definition is based on a passage from the'639 application "regarding Downloadables containing Java applets or ActiveX applets," this passage actually states that a "Downloadable is an executable application program which is automatically downloaded from a source computer and run on the destination computer." (Petition at 14 (citing Ex. 1005 2:1–7)). Further, it does not state that Downloadables "contain" Java applets or ActiveX as asserted by Petitioner; rather the passage demonstrates that Java applets and Active X are ***examples of*** Downloadables. (Id.). Accordingly, Petitioner's proposed definition is not reasonable in the context of the specification.

Petitioner also cites a Microsoft Computer Dictionary (Ex. 1019) and asserts that its construction how "one of ordinary skill in the art would understand the term "program script" to have this meaning." (Petition at 14). However, Petitioner's proposed construction is inconsistent with this definition, which states that a script is a "type of program that consists of a set of instructions to an application or utility program." (Ex 1019 at 350). For example, Petitioner omits any requirement for the program script to be part of a program. Furthermore, the dictionary cited is from 1993–1994, at least a year before JavaScript was even introduced. (Ex. 2004 at 2 ("Introduced in 1995, JavaScript is now an international standard and is helping developers to more easily write cross-browser Dynamic

HTML.")). Thus, Petitioner's proposed definition is also not reasonable in light of its ordinary meaning in the art.

IV. THE ASSERTED REFERENCES

The proposed grounds rely on four references. Ground 1 proposes the combination of *TBAV* (Ex. 1006) in view of *Ji* (Ex. 1009) with respect to claims 1, 10, and 18. Ground 2 proposes the combination of *TBAV* in view of *Ji* and *Chen* (Ex. 1010) with respect to claim 14. Ground 3 proposes the combination of *Arnold* (Ex. 1008) in view of *Chen* and *Ji* with respect to claims 1, 10, 14, and 18. Ground 4 proposes the combination of *Chen* in view of *Arnold* and *Ji* with respect to claims 1, 10, 14, and 18. However, none of these references, individually or in combination, disclose at least the claimed features of "deriving security profile data for [a] Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable" or "storing the Downloadable security profile data in a database."

A. TBAV (Ex. 1006)

TBAV is a user manual for the ThunderBYTE Anti-Virus Utilities. Petitioner relies specifically on three of the utilities described in *TBAV*—namely, TbScan, TbScanX, and TbGenSig—as allegedly teaching various features of the challenged claims. *See generally,* Petition at 18–29.

TbScan is a manual virus scanner designed to help users scan their hard disks or floppy disks for viruses. (*TBAV* at 47). TbScan recognizes that viruses "consist of a unique sequence of instructions, called a signature" and determines whether a particular file/program has been infected with a virus by "checking for the appearance of such signatures." (Id.). TbScan can detect unknown viruses by using heuristic scanning to detect suspicious instructions sequences and abnormal program layouts. (Id.). After each scan, TbScan can either overwrite or append the scan results to an existing log file. (Id. at 61). In the event that new scan information is appended to an existing log file, the manual suggests deleting or truncating the log file periodically (Id.).

TbScanX is a memory-resident version of TbScan that automatically scans executed files as well as executable files after they are copied, created, downloaded, modified, or unarchived on the computer system. (Id. at 84). TbScanX is a signature scanner, not a heuristic scanner. (Id. at 2).

TbGenSig is a virus signature file compiler that enables a user to define virus signatures. (Id. at 170). A virus signature includes the name of the virus, the signature definition, and the types of files that should be searched for the signature definition. (Id. at 173).

1. TBAV IS NOT PRIOR ART UNDER 35 U.S.C. § 102(a)

Petitioner relies upon the assertion that TBAV was "publicly available by at least October 25, 1996, as evidenced by the fact that it was disclosed by a patent applicant in an Information Disclosure Statement …filed on October 25, 1996." (Petition at 17). However, the mere fact that the TBAV reference was disclosed in an IDS does not demonstrate public availability under 35 U.S.C. § 102(a).

For a reference to qualify as a printed publication under 35 U.S.C. § 102(a), "the one who wishes to characterize the information, in whatever form it may be, as a 'printed publication' … should produce sufficient proof of its dissemination or that it has otherwise been available and accessible to persons concerned with the art to which the document relates and thus most likely to avail themselves of its contents." *In re Wyer*, 655 F.2d 221, 227 (CCPA 1981). Here, the Petitioner has failed to provide sufficient proof that *TBAV* qualifies as a printed publication under 35 U.S.C.§ 102(a).

Instead, Petitioner has merely demonstrated an applicant mailed the *TBAV* reference to the Patent Office on October 25, 1996. (Petition at 17). This is not proof that it was "accessible to persons concerned with the art" as of that date. Nor can Petitioner rely on the Patent Office's subsequent publication of the associated file wrapper, because the application did not publish until the application issued as U.S. Patent No. 6,067,410 on May 23, 2000, over three years after the priority date

of the '494 Patent. (Ex. 2005 at 1). Furthermore, *TBAV* explicitly states that "No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form, by print, microfilm, or by any other means without written permission from ThunderBYTE B.V." (Ex. 1006 at 1, *TBAV* cover page). Thus, Petitioner has not met it burden to show that the *TBAV* reference was not "accessible to persons concerned with the art" as of October 25, 1996.

Indeed, the version of TBAV that the Petitioner submitted to PTAB for this IPR does not appear to be the same version received by the IDS at the PTO. Although, it is unclear what all the differences are, a simple comparison reveals noticeable differences with the version kept at the PTO (e.g. Ex. 1006 is 198 pages while the version kept at the PTO is 199 pages; EX. 1006 at 64 and 115 does not appear in the version received by the PTO; *compare* EX. 1006 at 198 *with* the version kept at the PTO at 199). Thus, because EX. 1006 is not the version of TBAV that was submitted to the Patent Office via the IDS, Petitioner's reliance on the IDS to authenticate that EX. 1006 was publically available as of October 25, 1996 is improper.

B. Ji (Ex. 1009)

Ji discloses a system for detecting and eliminating viruses on a computer network. (Ex. 1009 at Abstract). The Petition cites *Ji* for its disclosure of an FTP proxy server 60 located at a network gateway node 33 that "receives an inbound

file that a client is trying to download so the file can be scanned for viruses before being passed onto the client." (Petition at 27). A file received at the FTP proxy server is temporarily stored at the gateway node and scanned for viruses. (Ex. 1009 at 8:65–9:2). If no viruses are detected the file is transferred to the client while if a virus is detected the FTP proxy either transfers the file despite the virus or deletes the temporary file and enables retrieving of the infected file by a system administrator. (Id. at 9:7–20).

C. Chen (Ex. 1010)

Chen is directed to the detection and removal of viruses from macros. (Ex. 1010 at Abstract). *Chen* discloses a macro virus scanning module 304 that detects macro instruction combinations likely to be used by macro viruses. (Id. at 8:40–43). To determine whether a macro is infected with a virus, the macro virus scanning module accesses comparison data, which includes sets of instruction identifiers that identify combinations of suspect instructions in a decoded macro, and scans the macro to determine whether they include the instruction identifiers. (Id. at 8:58–67). If the macro includes a combination of suspect instructions, the macro virus scanning module flags the macro as infected and stores information associating the macro with the suspicious instructions in a data buffer. (Id. at 8:67–9:11).

D. Arnold (Ex. 1008)

Arnold discloses a signature-based virus scanner that periodically monitors a computer for anomalous behavior, deploys decoy programs to capture virus samples, extracts a viral signature from the decoy programs, informs network-connected computers of the occurrence of a viral infection, and generates a distress signal, if appropriate. (Ex. 1008 at 4:38–52). The extracted viral signature is selected from a number of candidate signatures and provided to a virus scanner, which can make use of the signature for signature-based scanning of a computer system. (Id. at 11:13–20).

V. SPECIFIC REASONS WHY THE CITED REFERENCES DO NOT INVALIDATE THE CLAIMS, AND WHY INTER PARTES REVIEW SHOULD NOT BE INSTITUTED

A. Ground 1: TBAV in view of Ji does not render the Challenged Claims obvious under 35 U.S.C. § 103(a)

1. *TBAV* in view of Ji fails to disclose: "receiving an incoming Downloadable"

Independent claim 1 recites "receiving an incoming Downloadable." (Ex. 1001 at 21:20). Independent claim 10 further recites a "receiver." Petitioner relies on *TBAV* for the claimed "receiving an incoming Downloadable" feature in its claim charts. *Ji* is only cited for its alleged disclosure of a "receiver."

Petitioner has not met its burden to demonstrate that *TBAV* discloses "receiving an incoming Downloadable" at least because the Petition gives no

patentable weight to the word "incoming," which modifies the term Downloadable in each of the challenged claims. *See In re Wilson*, 424 F.2d 1382, 1385 ("All words in a claim must be considered in judging the patentability of that claim.").

Petitioner asserts that the TbScan utility of *TBAV* "scans files on a computer system" and that the TbScanX "scans a file when it is downloaded" onto the computer system. (Petition at 24). No explanation is provided, however, regarding how these assertions correspond to the claimed feature of "receiving an incoming Downloadable" as required under 37 C.F.R.§ 42.104(b). (Id.).

TbScan and TbScanX are virus scanners that scan program files for viruses to determine whether "your system has been infected." (Ex. 1006 at 47). Indeed, both TbScan and TbScanX only scan files ***after they are already resident on a file system of the client computer*** and are, therefore, not "incoming Downloadables." The primary differences between the two utilities are that TbScan is entirely manual and can perform heuristic scanning while TbScanX only performs traditional signature scanning which be performed automatically after the files are "are copied, created, downloaded, modified, or unarchived on the client device." (Id. at 2; id. at 84). Despite *TBAV's* statement that "TbScanX is virtually identical to TbScan," a thorough review of *TBAV* reveals that TbScanX does not perform heuristic scanning. *See, e.g., id*. at 2 ("TbScanx is the memory resident version of

TbScan. **This signature scanner** remains resident in memory….")(emphasis added).

2. TBAV in view of Ji fails to disclose: "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable"

Independent claim 1 recites "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable." (Ex. 1001 at 21:21–23). Independent claim 10 further recites a "Downloadable scanner coupled with said receiver." In its discussion of this claim element, Petitioner relies only on *TBAV* in its claim charts and associated discussions.

As demonstrated above, *TBAV* does not disclose receiving incoming Downloadables. *See* Section V.A.1. For at least the same reason, *TBAV* cannot derive security profile data for the Downloadable. In addition to this fatal deficiency, Petitioner has not met its burden to demonstrate that *TBAV* discloses "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable" for at least two reasons.

First, Ground 1 never explains what teachings of *TBAV* correspond to the claimed "security profile data" and the claimed "list of suspicious operations" as shown below:

Claim 1(b)	**TBAV and Ji**
"deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable"	TBAV includes TbScan, which performs heuristic analysis of files. Heuristic analysis includes detecting suspicious instruction sequences within a file and applying heuristic flags to the file. The heuristic flags indicate the suspicious instructions. Ex. 1006, pp. 153-155, 180-185. TbScan performs scans of files, including files that have been downloaded, whenever TbScan is run. Ex. 1006, pp.47-48. Additionally, TbScanX (a memory resident version of TbScan) automatically scans a file when it is downloaded. Ex. 1006, pp. 1-2, 76-77, 84, 153-155, 180-185; Ex. 1002 ¶ 85.

(Petition at 24). Rather, Petitioner's claim chart is comprised of improper attorney argument that merely describes the two different kinds of scanning performed by TBAV: (1) the heuristic scanning performed by TbScan and; (2) the signature scanning performed by TbScanX, without providing the actual evidence from *TBAV* relied upon as allegedly teaching the claimed "security profile data" or the claimed "list." *See* IPR2014-00901, Paper 7 at 2 ("Explanations, characterizations, conclusions, or inferences drawn from the references are improper in a claim chart.").

Furthermore, the Petition attempts to circumvent the page limits by only presenting citations of the reference (e.g. 13 pages of TBAV) rather than making the cited evidence available in the Petition itself. *See* IPR2014-00475, Paper No. 10 at 14–16) (explaining how such techniques impermissibly circumvent the page limits dictated under 37 C.F.R. § 42.24 and improperly impose on the Board to improperly "re-construct Petitioner's arguments and generally play archaeologist

with the record."). It is Petitioner's burden to "establish that it is entitled to the requested relief" and to do so "[t]he petition must specify where each element of the claim is found in the prior art" and provide "a detailed explanation of the significance of the evidence." *See* 37 C.F.R. §§ 42.20(c), 42.22(a)(2), and 42.104(b)(4). Because Petitioner has not done so in its Petition, the Board should not institute a trial on Ground 1.

Furthermore, Petitioner improperly relies on attorney argument rather than evidence in its attempt to demonstrate that *TBAV* discloses the claimed "list of suspicious computer operations that may be attempted by the Downloadable." In particular, the Petition states, without support, that "because the heuristic flags indicate the suspicious instructions, the list of heuristic flags in the file is a list of suspicious instructions." (Petition at 24). But neither a ***"list*** of heuristic flags ***in the file***" nor "a ***list*** of suspicious instructions" are recited in the *TBAV* reference. Petitioner's unsupported "list" argument cannot take the place of evidence lacking in the record. (*See Estee Lauder Inc. v. L'Oreal, SA*, 129 F.3d 588, 595 (Fed. Cir. 1997) ("arguments of counsel cannot take the place of evidence lacking in the record.")).

Second, the Petition does not present evidence that every element of the "deriving" limitation is disclosed by *TBAV*. At most, Petitioner appears to identify *TBAV's* suspicious instructions as the claimed "suspicious computer operations

that may be attempted by a Downloadable." *See* Petition at 24 (asserting that "[h]euristic analysis includes detecting suspicious instruction sequences within a file and applying heuristic flags to the file"). As discussed above, the Petitioner applies the wrong construction. Specifically, instructions are not "operations that may be attempted by the Downloadable." *See* Section III above (discussing the proper construction for "suspicious computer operations").

Petitioner's assertion that suspicious instructions disclosed in *TBAV* correspond to the claimed suspicious operations therefore fails to properly consider the claimed "security profile data for the Downloadable" or the claimed "list" that is included in the claimed "security profile data," in contravention of the Federal Circuit's dictate that a *prima facie* case of obviousness must still account for all limitations of the claim. *See In re Royka*, 490 F.2d 981 (CCPA 1974) ("To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art.").

In fact, no element identified by Petitioner qualifies as the claimed "security profile data" that is stored in a database. Petitioner already relies on *TBAV's* log file to be the claimed "database" and the "suspicious instructions" to be the claimed "suspicious computer operations." *See* Petition at 24 ("a list of suspicious instructions"); Petition at 25–26 ("either or both of [the log file and the TBSCAN.SIG file] could be is [sic] a database…"). Conflating either the claimed

database or the claimed list of suspicious computer operations with the claimed security profile data is not allowed as it is well-established that "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970).

3. TBAV in view of Ji fail to disclose: "storing the Downloadable security profile data in a database."

Independent claim 1 recites "storing the Downloadable security profile data in a database." (Ex. 1001 at 21:24–25). Independent claim 10 adds that the storage of security profiles in a database must be performed by a "database manager." As a preliminary matter, *TBAV* in view of *Ji* does not teach storing Downloadable security profile data in a database because they do not teach the generation of the claimed security profile," as explained above in Section V.A.2. For both claims, Petitioner relies only on *TBAV* in its claim charts and discussions.

Claim 1(c)	**TBAV and Ji**
"storing the Downloadable security profile data in a database"	TBAV teaches that heuristic analysis results, including the heuristic flags describing the suspicious instructions, can be output to a file. Ex. 1006, p. 60; Ex. 1002 ¶ 88. TBAV also teaches using TbScan to extract instructions from files that are believed to be infected with viruses. The instructions form a signature for the virus infecting the file. TbGenSig adds the signature to the TBSCAN.SIG file. Ex. 1006, p. 165-168; Ex. 1002 ¶ 89.

(Petition at 25). This claim chart cites to five pages of the *TBAV* reference rather than providing evidence from *TBAV* that corresponds to the claimed "Downloadable security profile data" that is allegedly stored in a database. This

bare citation to the reference coupled with improper characterizations of the reference impermissibly invites the Board "to re-construct Petitioner's arguments and generally play archaeologist with the record."

The Petition proposes that two different files disclosed in *TBAV* (*i.e.* the log file and TBSCAN.SIG file) correspond to the claimed database that stores Downloadable security profile data. (Petition at 25–26). But the Federal Circuit dictates that even under the broadest reasonable interpretation, the Board's construction "cannot be divorced from the specification and the record evidence." *In re NTP, Inc.*, 654 F.3d 1279, 1288 (Fed. Cir. 2011). The Board's construction "must be consistent with the one that those skilled in the art would reach." *In re Cortright*, 165 F.3d 1353, 1358 (Fed. Cir. 1999). A person of ordinary skill in the art would understand from reading the specification of the '494 Patents that the claimed database of security profiles is not a log file. *See* Section III.E (distinguishing the claimed database (*e.g.* Security Database 240) from log files (*e.g.* Event Log 245)). Similarly, TBSCAN.SIG is not a database of security profiles, rather tit is a simple signature file that TbScan references for signature-based scanning. (Id. at 1). Thus, at least because the term database cannot be reasonably construed to include simple files, such as *TBAV's* log file and TBSCAN.SIG file, Petitioner has not demonstrated that *TBAV* discloses "storing the Downloadable security profile in a database."

Notably, the Petition does not even assert that the log and TBSCAN.SIG files are databases. Rather, Petitioner states that a POSITA "would understand either or both of these files ***could be*** is [sic] a database containing [sic] that contains one or more data entries" and that "at minimum, it would have been obvious to one of ordinary skill in the art in view of TBAV to store suspicious computer operations in a database." (Petition at 25–26). But Petitioner's rationale for a POSITA to modify *TBAV* is essentially a recitation of claim 1 itself, revealing reliance on impermissible hindsight to supply the requisite motivation to combine. *See Insite Vision, Inc. v. Sandoz, Inc.*, 783 F.3d 853, 859 (Fed. Cir. 2015)

Moreover, in an attempt to support this conclusory assertion, Petitioner cites to the Declaration of Dr. Clark, which is nearly identical to the Petition and which is also completely devoid of any evidentiary support that underpins Petitioner's assertion. (*See* Ex. 1002 ¶ 90). The Board should ignore these unsupported arguments because "[a]ffidavits expressing an opinion of an expert must disclose the underlying facts or data upon which the opinion is based." *See* Trial Practice Guide, 77 Fed. Reg. 48756; *see also* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."); IPR2014-00529, Paper 8 at 15 ("Merely repeating an argument from the Petition in the declaration of a proposed expert does not give that argument enhanced probative value.").

Dr. Clark's only citation supports the unrelated point that data in the files is made available for review by a user or use by TbScan at a later time. (Ex. 1002 at ¶ 90). Neither Dr. Clark's Declaration nor the Petition explain why or how a POSITA would have modified *TBAV* to store Downloadable security profile data in a database or how making data in files available of review corresponds to the claimed "storing security profile data in a Database" as required under 37 C.F.R. § 42.104(b)(4). *See* IPR2014-00529, Paper 8 at 15 (refusing to give weight to an expert declaration that "does not explain the 'how,' 'what,' and 'why' of the proposed combination of references.").

Furthermore, *TBAV's* log file is not used for storage of security profiles. When TbScan scans the computer for viruses, the results can be "output to log file." (Ex. 1006 at 60). In the default case, the results of each new scan will overwrite older output in the log file. (Id. at 61). Even if using the available "Append to existing log" option, *TBAV* "recommends that you delete or truncate the log file to avoid unlimited growth." (Id. at 61). Accordingly, *TBAV's* log file is simply provided for diagnostic purposes (*i.e.* to allow a user to examine the results of a scan). *See id*. at 62 (describing how the log file can be viewed and studied). In stark contrast, Patent Owner's invention as recited in the challenged claims requires "storing the Downloadable security profile data in a database" so that it

can be retrieved at a later time and compared against a security policy to determine "whether to pass or fail the Downloadable." (*See* Ex. 1015 at 6:13–20).

Petitioner's second theory relies on TbGenSig, which is a *TBAV* utility that allows a user to create his or her own signature. *See* Ex. 1006 at 165 ("***TbGenSig, an advanced user utility that enables you to define your own virus signatures***.... TbGenSig is a signature file compiler. ...If, however, you want to ***define your own virus signatures***, you will need this utility.")(emphasis added). *TBAV* does not explain exactly how to create a signature for "virus hunting." (Id.). But TBAV's "step-by-step assistance" demonstrates this is a complex manual process which results in the user created USERSIG.DAT file. (*See id*. at 165–168 ("This section offers ***step-by-step assistance*** in creating an emergency signature…")). Eventually, USERSIG.DAT file can be compiled into the TBSCAN.SIG file using the TbGenSig compiler. (Id. at 165). Rather than a database, the TBSCAN.SIG file is data file referenced by TbScan that includes "home-made" signatures so that "you can scan all your machines in search of the new virus." (Id. at 168).

Furthermore, *TBAV* does not disclose the "database manager" recited in independent claim 10, which adds that the storage of security profiles in a database must be performed by a "database manager." Here, the Petition simply repeats its previous "database" arguments for claim 1, without giving any patentable weight to the term "database manager." Petition at 28-29 (e.g. "it would have been

obvious to one of ordinary skill in the art in view of TBAV to store suspicious computer operations in a database.")

4. The Proposed Combination of TBAV with Ji is a Product of Hindsight Bias.

Ground 1 should also be denied because the Petition, does not "identify a reason that would have prompted a person of ordinary skill in the relevant field to combine elements in the way the claimed new invention does." *See KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007). In fact, the Petition does not identify any element of claim 1 that is disclosed by *Ji*, let alone identifying a reason that would have prompted a POSITA to combine elements of *Ji* and *TBAV* to reach the invention recited in claim 1. Thus, Petitioner's failure to provide the requisite motivation to combine reasoning dictates that Petitioner's argument that the combination of *TBAV* and *Ji* renders claim 1 obvious is insufficient as a matter of law. *See KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 418. ("[O]bviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.").

Rather, Petitioner only mentions *Ji* with respect to the "receiver" element claimed in independent claim 10. (*See* Petition at 27 ("To the extent TBAV does not explicitly describe a receiver, *Ji* teaches an FTP proxy server 60 that receives an inbound file….") First, this combination is insufficient because reliance on *Ji's*

FTP proxy for the claimed "receiver" does not cure *TBAV's* failure to disclose the claimed "receiving," "deriving," or "storing" limitations. Furthermore, the Petition fails to explain what would have prompted POSITA to add the FTP proxy server. The Petition's only rationale for combining these references is that "TBAV and Ji are both directed to virus scanning software that can scan incoming downloaded files." (Petition at 27). But many types of virus scanning software exist, so that fact alone is not sufficient support the legal conclusion of obviousness. *See OpenTV, Inc. v. Cisco Tech., Inc.,* IPR 2013-00328 (Paper No. 13) at *12-22 (2013) ("The mere fact that the [cited references] describe similar [] systems is not, by itself, a sufficient rationale for a person of ordinary skill in the art to have made the asserted combination.").

The record shows no reason for one of ordinary skill in the art to attempt to combine *Ji's* proxy server with *TBAV's* local virus scanning system. Thus, rather than demonstrating that a POSITA would have recognized a problem with *TBAV* that would justify the need for a FTP proxy server, Petitioner's addition of *Ji's* FTP proxy server to the system of *TBAV* succumbs to the trap of hindsight. *See Insite Vision, Inc. v. Sandoz, Inc.*, 783 F.3d 853, 859 (Fed. Cir. 2015) ("[d]efining the problem in terms of its solution reveals improper hindsight in the selection of the prior art relevant to obviousness."). In fact, "the challenger's 'burden is especially difficult when the prior art was before the PTO examiner during prosecution of the

application.'" *Al-Site Corp. v. VSI Int'l*, 174 F.3d 1308, 1323 (Fed. Cir. 1999). In the instant case, both *Ji* and *TBAV* were before the examiner during the '494 Patent prosecution making Petitioner's burden "especially difficult" to meet. (Ex. 1004 at 12, 129).

Indeed, the suggested combination of references would require a substantial reconstruction and redesign of the elements shown in *TBAV* as well as a change in the basic principle under which *TBAV's* anti-virus utilities were designed to operate. *See In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) ("If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious."). In *TBAV*, TbScan and TbScanX operate on files that are already resident on the computer system to "protect against, and recover from, computer viruses." (Ex. 1006 at 1). Accordingly, TbScan and TbScanX could not be operated on *Ji's* FTP proxy (identified as the claimed "receiver") because that FTP proxy would not have access to the files that TbScan and TbScanX are designed to scan. (Petition at 27).

B. Ground 2: TBAV in view of Ji and Chen does not render the Challenged Claims obvious under 35 U.S.C. § 103(a)

1. TBAV in view of Ji and Chen fail to disclose: "wherein the Downloadable includes program script"

Challenged claim 14 depends from independent claim 10. Ground 2 only adds *Chen* to the combination of *TBAV* and *Ji* of Ground 1 and only with respect to claim 14. Accordingly, the Board should decline to institute a trial on Ground 2 with respect to claim 14 at least for the same reasons as it should decline to institute a trial on Ground 1 with respect to claim 10. Furthermore, claim 14 recites "wherein the Downloadable includes program script." (Ex. 1001 at 22:26–27). In its discussion of this claim element, Petitioner relies on *TBAV* and *Chen* in its claim charts and discussions.

Petitioner begins by stating that *TBAV* discloses .DLL files "and other files than can contain executable code but are not program files." (Petition at 35). The Petition then asserts that Chen discloses macros and that "a macro is an example of program script." (Id.).

However, the Petition does not attempt to explain how any of these files, including *TBAV's* .DLLs and *Chen's* macros qualify as program scripts, let alone how the disclosures of *TBAV* and *Chen* teach a ***Downloadable that includes*** program script. (Id.). Accordingly Petitioner has failed to "specify where each element of the claim is found in the prior art patents or printed publications relied upon." 37 C.F.R. § 42.104(b). Indeed .DLL files and macros are not program scripts. A .DLL is a Dynamically-linked library (Ex. 1006 at 57) and macros are programs that generally replace the keystrokes of a user. (Ex. 1010 at 1:39–41).

Petitioner's reliance on the Declaration of Dr. Clark for the proposition that macros are program scripts should be ignored because the Declaration cites absolutely no evidence to support its assertion that "[a] macro is an example of program script …" (*See* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.")).

2. The Proposed Combination of TBAV and Ji with Chen is a Product of Hindsight Bias.

Petitioner provides insufficient rationale for modifying *TBAV* and *Ji* with *Chen*. The Petition's sole rationale for combining these references is derived directly from the Declaration of Dr. Clark. *See* Petition at 35–36 (citing Ex. 1002 at ¶ 115). In particular, Dr. Clark states that "[a] macro is an example of program script often executed automatically without the user's knowledge and thus poses high potential threat," which is then used as the basis for the conclusory statement that "it would have been obvious to one of ordinary skill in the art to apply the teachings of Chen to the system of TBAV to allow the system of TBAV to scan for viruses in both executable files and files containing program script." (Ex. 1002 at ¶ 115).

However, Dr. Clark cites no evidence to support the assertion, which is the only predicate for his obviousness conclusion. (Id.). Therefore, the Board should ignore Dr. Clark's Declaration. (*See* 37 C.F.R. § 42.65(a) ("Expert testimony that

does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.")). The Petition is nearly identical to the Declaration and cites no other evidence to substantiate its basis for the conclusion of obviousness; the fact that its arguments are repeated in the Dr. Clark's Declaration does not give them any additional weight. *See Kinetic Technologies, Inc. v. Skyworks Solutions, Inc.*, IPR2014-00529, Paper 8 at 14–15 ("Merely repeating an argument from the Petition in the declaration of a proposed expert does not give that argument enhanced probative value.").

C. Ground 3: Arnold in view of Chen and Ji does not render the Challenged Claims obvious under 35 U.S.C. § 103(a)

1. Arnold fails to disclose: "receiving an incoming Downloadable"

Independent claim 1 recites "receiving an incoming Downloadable." (Ex. 1001 at 21:20). Independent claim 10 further recites a "receiver." As addressed above, the Petitioner gives no weight to the word "incoming," which modifies the term "Downloadable" to clarify that the Downloadable is located at the intermediate computer rather than at the destination device. *See* Section VI.B.1. Petitioner's claim chart relies on *Arnold* and *Ji* for this feature.

Like *TBAV's* TbScan, Arnold's "automatic immune system" operates on the data processing system that may include an "undesirable software entity such as a computer virus, worm, or Trojan Horse." (Ex. 1008 at Abstract). The disclosed

method includes an anomaly detector that monitors a data processing system for anomalous, potentially virus-like behavior, which demonstrates that *Arnold* is concerned only with activity of files already resident and running on the computer. (Id. at 4:60–65). *Arnold* accordingly does not disclose "receiving an incoming Downloadable." As demonstrated below, moreover, Petitioner provides insufficient motivation to modify *Arnold* with *Ji*. *See* Section V.C.5.

2. Arnold in view of Chen and Ji fail to disclose: "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable"

Independent claim 1 recites "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable." (Ex. 1001 at 21:21–23). Independent claim 10 further recites a "Downloadable scanner coupled with said receiver." (Id. at 22:7-10). In its discussion of this claim element, Petitioner relies on *Arnold* and *Chen* in its claim charts and discussions.

Petitioner has not met its burden to demonstrate that *Arnold* and *Chen* disclose "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable." In fact, the Petition never explains what in *Arnold* and *Chen* is alleged to correspond to the claimed "security profile data" or the claimed "list" as shown in the claim chart:

Claim 1(b)	**Arnold, Chen, and Ji**
"deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable"	Arnold teaches deriving a signature for a virus by analyzing an invariant section of code from a program. Ex. 1008, col. 10, l. 63 – col. 11, l. 20; col. 10, ll. 15-20; Ex. 1002 ¶ 128. Chen teaches comparing decoded binary code with instruction identifiers to reveal the presence of code portions corresponding to the instructions of the instruction identifiers. Ex. 1010, col. 14, ll. 13-64; Ex. 1002 ¶ 129.

(Petition at 40). Petitioner's claim chart is comprised of citations to broad passages of *Arnold* and *Chen* and attorney argument drawing inferences from the references without providing the evidence relied upon. For example, Petitioner concludes that "Arnold teaches deriving a signature for a virus by analyzing an invariant section of code from a program" without even demonstrating that the cited portions correspond to the claimed "security profile data" or the claimed "list." *See* IPR2013-00552, Paper 6 at 20–21 (indicating that providing such summaries and citations alone does not support institution of trial—rather, a petitioner must show how and why each limitation is invalid in view of the prior art). Because Petitioner has not met its burden to "establish that it is entitled to the requested relief," "specify where each element of the claim is found in the prior art," and provide "a detailed explanation of the significance of the evidence," the Petition should be denied. *See* 37 C.F.R. §§ 42.20(c), 42.22(a)(2), and 42.104(b)(4).

Petitioner asserts that "Arnold teaches deriving a signature for a virus by analyzing an invariant section of code from a program" and that a POSITA would recognize that *Arnold's* signature is indicative of a sequence of suspicious operations because "it represents an invariant portion of code that caused observed anomalous behavior." (Petition at 41). As a preliminary matter, Petitioner has not explained how these assertions correspond to elements of the claim language. At most, Petitioner asserts that *Arnold's* signature is "indicative of a sequence of suspicious computer operations." (Id.). Arnold is completely unaware of potentially hostile operations that may be attempted by a program, let alone generating a security profile that includes list of such operations. Arnold is concerned with identifying "invariant code portions" and processing them into "valid signatures" using a multi-step n-gram probability-based technique (where "n-gram is an instance of n consecutive bytes, where n=1 (uni-gram) to some arbitrarily large value."). (Ex. 1008 at Fig. 8, 10:64–66).

As a result, *Arnold's* virus signatures are simply portions of virus code used to detect viruses (e.g., using string matching). (Ex. 1008 at 9:13–35). *Arnold* teaches the use of "decoy programs" to "attract and obtain one or more samples of [an] unknown virus." (Id. at 6:3–7). If a decoy program is found to have changed from the original, the changed portion is assumed to be a virus and is isolated from the decoy program. (Id. at 7:3–8). Invariant portions of the virus, such the one

shown in FIG. 6B code are then identified by filtering "out all portions of the virus which are observed to or are likely to vary from one instance of the virus to another." (Id. at 7:11–15).

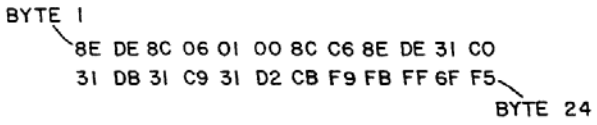

FIG. 6B

From the invariant portion of the virus, candidate virus signatures are identified, where the signatures "are all possible contiguous blocks of S bytes found in these 'probably-invariant' or 'substantially-invariant' byte sequences." (Id. at 8:66–9:1). *Arnold* does not describe performing any analysis of the virus signature to determine what operations the portion of code might perform, let alone whether those operations are suspicious operations but rather compares the candidate virus signatures to "a large corpus of typical programs" to identify one or more good virus signatures with a low false-positive probability. (Id. at 9:42–68). Accordingly, rather than a list of suspicious operations, *Arnold's* virus signature is merely a portion of virus code "which is statistically unlikely to generate false positives when run on uninfected, legitimate programs, but will always identify the virus if it is present." (Ex. 1008 at 9:16–19). As explained above, sections of virus code (*i.e.* instructions) present in *Arnold's* virus signatures cannot be equated with suspicious computer operations. (*See* Section III.B).

Petitioner also cites *Chen* with respect to this feature but, fatally, does not explain the "[d]ifferences between the claimed invention and" *Arnold*, or how *Arnold* is to be modified with *Chen* to meet the deriving feature recited in the challenged claims. *See Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17 (1966); *see also* CBM2012-00003, Paper 7 at 2–3 ("[A] Petition that does not state the differences between a challenged claim and the prior art, and relies instead on the Patent Owner and the Board to determine those differences, fails to adequately state a ground of obviousness and risks having the claim excluded from trial.").

Nor does Petitioner articulate a "rational underpinning to support the legal conclusion of obviousness" for its proposed combination of *Arnold* and *Chen*. (*KSR v. Teleflex*, 550 U.S. 398, 418 (2007)). As with the proposed combination of *Arnold* with *Ji* for the claimed receiving feature, the only motivation provided for combining *Arnold* with *Chen* is that they "are both directed to virus scanning software that can detect unidentified viruses within a file." *See OpenTV, Inc. v. Cisco Tech., Inc.*, IPR 2013-00328 (Paper No. 13) at *12-22 (2013).

Still further, *Chen* fails to cure the deficiencies of *Arnold* highlighted above. Petitioner merely states that *Chen* discloses "comparing decoded binary code with instruction identifiers to reveal the presence of code portions corresponding to the instructions of the instruction identifiers." (Petition at 40). However, there is no explanation of how this assertion corresponds to the claim language, which recites

"deriving security profile data," as required under 37 C.F.R. § 42.104(b). Indeed, although Petitioner is correct in stating that *Chen* scans files to reveal "the presence of the suspicious instructions within the file," this conclusion is not at all related to the claimed deriving feature. (Petition at 41; *see* Ex. 1010 at 14:48-51 (disclosing using a binary string "as an identifier for detecting a plurality of different suspect macro instructions"). That is, although *Chen* scans a file to detect "suspect macro instructions," *Chen* discloses neither "deriving security profile data for the Downloadable" or "a list of suspicious computer operations that may be attempted by the Downloadable" as recited in the challenged claims.

Indeed, the Petition never explains whether *Arnold's* system would be modifying *Chen* or vice versa or how *Chen* or *Arnold* could be modified with the other reference to meet the claimed "deriving" feature. This lack of analysis violates 37 C.F.R. § 42.22(a)(2), which requires "a detailed explanation of the significance of the evidence." Accordingly, not only has Petitioner not explained its obviousness rationale, the cited references, alone or in combination, do not disclose the claimed deriving feature recited in challenged claims.

3. Arnold in view of Chen and Ji fail to disclose: "storing the Downloadable security profile data in a database."

Independent claim 1 recites "storing the Downloadable security profile data in a database." (Ex. 1001 at 21:24–25). Independent claim 10 adds that the storage of security profiles in a database must be performed by a "database

manager." As a preliminary matter, *Arnold* in view of *Chen* and *Ji* does not teach storing Downloadable security profile data in a database because they do not teach derivation of the claimed security profile data, as explained above in Section V.C.2. In its discussion of this claim element, Petitioner relies only on *Arnold* in its claim charts and discussions.

Petitioner only provides a claim chart for this feature, which appears to map *Arnold's* teaching of "identifying valid signatures from among candidate signatures…and storing them in a database" with the claimed "storing the Downloadable security profile in a database." (Petition at 41).

Claim 1(c)	**Arnold, Chen, and Ji**
"storing the Downloadable security profile data in a database"	Arnold teaches identifying valid signatures from among candidate signatures using an invariant code identifier 38 and storing them in a database using an n-gram processor 40. Ex. 1008, col. 29, ll. 14-23; Ex. 1002 ¶ 131.

(Id.). Preliminarily, Petitioner's claim chart for this element is improper because Petitioner provides no discussion outside the claim chart regarding how *Arnold's* "valid signature" qualifies as the claimed "Downloadable security profile data." (Id.). Petitioner's characterization of the portion of the reference cited in the claim chart fails to cure this deficiency because fails to clearly demonstrate on its face that *Arnold* teaches the claimed storing feature. *See* IPR2014-00901, Paper 7 at 2–3 ("If there is *any* need to explain how a reference discloses or teaches a limitation,

that explanation must be elsewhere in the petition—not in a claim chart.")(emphasis in original).

Indeed, Petitioner's equation of storing a valid signature in a database as taught by *Arnold* with the claimed feature of "storing the Downloadable security profile data in a database" fails for several reasons. First, the Petition previously mapped *Arnold's* virus signatures to the claimed "list of suspicious operations," rather than the "Downloadable security profile data." *See* Petition at 40-41 ("the signature generated by Arnold is indicative of a sequence of suspicious computer operations"). Conflating these two claim elements is not allowed as it is well-established that "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970). Second, as previously demonstrated, *Arnold's* virus signatures are neither Downloadable security profile data nor a list of suspicious computer operations. *See* Section VI.C.3.

Furthermore, *Arnold*, *Chen*, and *Ji* fail to disclose the "database manager" recited in independent claim 10. Here, the Petition refers to *Arnold's* "n-gram processor 40" as the element that allegedly stores a valid signature in a database. (Petition at 43). However, Petitioner's summarization of the cited portion of *Arnold* mischaracterizes its n-gram processor, which processes candidate signatures rather than storing valid signatures in a database:

> The invariant code identifier 38 operates to identify invariant code portions of the sample(s) and to **provide the invariant code portions to the n-gram processor 40 as candidate signatures.**
>
> **After processing the candidate signatures in the manner described above**, a valid signature for the previously unknown type of undesirable software entity is stored within the SDB 74a for subsequent use by the scanner 74.

(Ex. 1008 at 29:14–23)(emphasis added).

4. Arnold in view of Chen and Ji does not disclose: "wherein the Downloadable includes program script

Claim 14 recites "wherein the Downloadable includes program script." (Ex. 1001 at 22:26–27). In its discussion of this claim element, Petitioner relies only on *Chen* in its claim charts and discussions. As previously discussed, however, Petitioner does not attempt to explain how *Chen's* macros qualify as program scripts, aside from citation to unsupported statements from Dr. Clark's Declaration, let alone how the disclosure of *Chen* teaches a ***Downloadable that includes*** program script. *See* Section V.B.1 above. Additionally, Petitioner repeats the same insufficient rationale for modifying *Arnold* with *Chen* for this feature as provided for the claimed deriving feature—namely, that *Arnold* and *Chen* "are both directed to virus scanning software." *See* Section V.C.2 above.

5. The Proposed Combination of Arnold with Ji is a Product of Hindsight Bias.

Arnold does not disclose receiving an incoming Downloadable. The Petition attempts to cure this deficiency by "apply[ing] the teachings of Ji of receiving a Downloadable to the system of Arnold." (Petition at 40). Petitioner's sole proposed rationale for combining these references is that "Arnold and Ji are both directed to virus scanning software that can scan files on a network-connected computer." (Id.) Yet this fact alone is not sufficient rationale for a person of ordinary skill in the art to have modified Arnold to include *Ji's* FTP proxy for receiving inbound files. *See OpenTV, Inc. v. Cisco Tech., Inc.*, IPR 2013-00328 (Paper No. 13) at *12-22 (2013). Indeed, many types of virus scanning software exist, and there are many types of computers that can connect to a network. Petitioner has simply not demonstrated that a POSITA would have been motivated to combine *Arnold* and *Ji* in the manner advanced in the Petition. *See KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007) (affirming that it "can be important identify a reason that would have prompted a person of ordinary skill in the relevant field to combine elements in the way the claimed new invention does.").

Furthermore, *Ji* utilizes a FTP proxy to prevent users' personal computers from ever receiving a virus. *See* Ex. 1009 at Abstract ("The FTP proxy server and SMTP proxy server… operate in a manner such that viruses transmitted to or from the network in files and messages are detected before transfer into or from the

system."). In contrast, Arnold's disclosed method only pertains to detecting viruses that are already extant on the client device. *See, e.g.*, Ex. 1008 at 6:3–7 (describing how decoy programs are deployed to attract and obtain samples of an unknown virus resident on the computer system). As such, modifying *Arnold* to run on *Ji's* FTP proxy would be contrary to the operating principle of *Arnold*, which requires the existence of unknown viruses ***on the system being scanned***. *See In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) (holding that a proposed modification or combination cannot change the principle operation of a prior art reference).

Moreover, Much like the proposed combination of *TBAV* and *Ji* discussed above in Section VI.A.4, Petitioner does not explain how *Ji's* proxy server would be combined with *Arnold's* local virus scanning system and has not, therefore, complied with 37 C.F.R. § 42.22(a)(2), which requires that the Petition provide "a detailed explanation of the significance of the evidence." Petitioner only asserts that "it would have been obvious to one of ordinary skill in the art to apply the teachings of Ji of receiving a Downloadable to the system of *Arnold* " without explaining how the two systems would be integrated. (Petition at 40). For example, Petitioner does not explain whether *Ji's* receiver would be added to *Arnold's* local computer system, if *Arnold's* virus scanner would be added to *Ji's* proxy server, or whether Petitioner envisioned some other combination. Nor has

Petitioner explained the consequences of applying the teachings of a receiver in "*Ji* of receiving a Downloadable to the system of *Arnold*," with respect to the claimed deriving and storing features.

D. Ground 4: Chen in view of Arnold and Ji does not render the Challenged Claims obvious under 35 U.S.C. § 103(a)

1. Chen fails to disclose: "receiving an incoming Downloadable"

Independent claim 1 recites "receiving an incoming Downloadable." (Ex. 1001 at 21:20). Independent claim 10 further recites a "receiver." Petitioner's claim chart relies on *Chen* and *Ji* for this feature.

As with Grounds 1 and 2 discussed above, Petitioner gives no weight to the word "incoming" in its treatment of Ground 3. *See, e.g.*, Section VI.B.1. Like *TBAV's* TbScan and *Arnold's* "automatic immune system," *Chen* merely scans files already resident on a computer file system rather than receiving an incoming Downloadable:

> The CPU 104, as directed by instructions received from the memory 106 as configured in accordance with the present invention, provides signals for accessing computer files, determining whether they include macros, locating the macros and scanning them to determine whether viruses including unknown viruses are present, and taking corrective action when such viruses are detected.

(Ex. 1010 at 5:3–9). Petitioner has therefore failed to demonstrate that *Chen* discloses "receiving an incoming Downloadable." As demonstrated below,

moreover, Petitioner provides insufficient motivation to modify *Chen* with *Ji*. *See* Section V.D.6.

2. Chen in view of Arnold and Ji fail to disclose: "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable"

Independent claim 1 recites "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable." (Ex. 1001 at 21:21–23). Independent claim 10 further recites a Downloadable scanner coupled with said receiver." In its treatment of this claim element, Petitioner relies only on *Chen* in its claim chart and provides no associated discussion regarding how the cited portion of *Chen* referred to in the claim chart corresponds to the claimed deriving security profile data feature:

Claim 1(b)	**Arnold, Chen, and Ji**
"deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable"	Chen teaches comparing decoded binary code with instruction identifiers to reveal the presence of code portions corresponding to the instructions of the instruction identifiers. Ex. 1010, col. 14, ll. 13–64; Ex. 1002 ¶ 148.

(Petition at 46). Accordingly, not only has Petitioner not specified "where each element of the claim is found in the prior art patents or printed publications relied upon" as required under 37 C.F.R. § 42.104(b)(4), but its claim chart improperly characterizes a large portion of *Chen* without explaining how the citation allegedly

meets the claim language and provides no other discussion of the element outside the claim chart. *See* IPR2014-00901, Paper 7 at 2–3.

Furthermore, Petitioner's citation to *Chen* and its characterization of the citation completely fail to correspond to the claim language. That is, although *Chen* scans a file to ***detect*** "suspect macro instructions," *Chen* discloses neither "deriving security profile data for the Downloadable" or "a list of suspicious computer operations that may be attempted by the Downloadable."

3. Chen in view of Arnold and Ji fail to disclose: "storing the Downloadable security profile data in a database."

Independent claim 1 recites "storing the Downloadable security profile data in a database." (Ex. 1001 at 21:24–25). Independent claim 10 further recites "a database manager coupled with said Downloadable scanner." In its discussion of this claim element, Petitioner relies on *Chen* and *Arnold* in its claim charts and discussions.

Petitioner first asserts that *Chen's* disclosure of "storing information associating a decoded macro to instruction identifiers in a data buffer" is equivalent to the storing feature recited in the challenged claims. (Petition at 46). As demonstrated above, *Chen* does not disclose deriving security profile data for a Downloadable" and cannot, therefore, store such data. (*See* Section V.D.3). Additionally, Petitioner fails to provide "a detailed explanation of the significance of" the cited "information associating a decoded macro in instruction identifiers"

as required under 37 C.F.R. § 42.22(a)(2) and how it relates to the "Downloadable security profile data" recited in the challenged claims. Indeed, *Chen's* only discussion phrase "information associating the decoded macro" shows that this "information" is placed in the data buffer for immediate treatment by a macro treating module "to selectively remove an unknown virus." (Ex. 1010 at 16:24–27). Thus, like the virus signatures of *TBAV* and *Arnold* discussed above, *Chen* is concerned with identifying a virus infecting a file (here, a macro) not with deriving security profile data for a Downloadable, let alone storing Downloadable security profile data in a database.

The Petition appears to recognize that *Chen* does not "explicitly describe storing the information in a database" and cites to *Arnold* in an attempt to cure this deficiency. However, as discussed above, *Arnold* also fails to disclose "storing the Downloadable security profile data in a database." (*See* Section V.C.4 above).

Petitioner also appears to recognize that Chen does not disclose a database manager as recited in independent claim 10 and cites to *Arnold* in an attempt to cure this deficiency. (Petition at 48). However as shown above, Petitioner's correspondence of *Arnold's* n-gram processor with the claimed database manager is misplaced. *See* Section V.C.3 ("*Arnold* mischaracterizes its n-gram processor, which processes candidate signatures rather than storing valid signatures in a database.").

4. The Proposed Combination of Chen with Arnold is a Product of Hindsight Bias.

Petitioner has not identified "a reason that would have prompted a person of ordinary skill in the relevant field to combine elements in the way the claimed new invention does." *See KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007). The Petition's only rationale for combining *Chen* with *Arnold* is that "Chen and Arnold are both directed to virus scanning software wherein data about detected malicious files is stored." However, these facts alone would not make it obvious to modify their features in the manner claimed. *See OpenTV, Inc. v. Cisco Tech., Inc.*, IPR 2013-00328 (Paper No. 13) at *12-22 (2013). Indeed, the Petition never explains whether *Chen's* system would be modifying *Arnold's* or how *Chen* or *Arnold* could be modified with the other reference to meet the claimed "storing the Downloadable security profile data in a database" in contravention of with 37 C.F.R. § 42.22(a)(2), which requires "a detailed explanation of the significance of the evidence."

Furthermore, a POSITA would not be motivated to store *Chen's* "information associating a decoded macro to instruction identifiers in *Arnold's* database. Rather than a database, *Chen* stores instruction identifiers in a data buffer for immediate use by a "macro treating module," which immediately replaces the located suspect instructions with benign instructions. *See* Ex. 1010 at 16:24–50 (describing how the macro treating module uses the set of instruction

identifiers in the data buffer to locate the suspect instructions in the macro and replace the suspect instructions with benign instructions). Because the replacement of suspect instructions occurs before the macro is run, information is temporarily stored in a data buffer. There would be no reason to store the "information" in a database because once the suspect instructions are replaced, the information would no longer be relevant. At least because a POSITA would have no reason to store *Chen's* "information" in a database, the proposed modification of *Chen* with *Arnold* is improperly based on hindsight bias. Accordingly, Petitioner not explained its obviousness rationale or demonstrated how the cited references disclose the claimed deriving feature recited in challenged claims.

5. Chen in view of Arnold and Ji does not disclose: "wherein the Downloadable includes program script

Claim 14 recites "wherein the Downloadable includes program script." (Ex. 1001 at 22:26–27). In its discussion of this claim element, Petitioner relies only on *Chen* in its claim charts and discussions. As previously discussed, however, Petitioner does not attempt to explain how *Chen's* macros qualify as program scripts, aside from citation to unsupported statements from Dr. Clark's Declaration, let alone how the disclosure of *Chen* teaches a ***Downloadable that includes*** program script. (*See* Section V.B.1 above).

6. The Proposed Combination of Chen with Ji is a Product of Hindsight Bias.

Chen does not disclose receiving an incoming Downloadable. The Petition attempts to cure this deficiency with reference to *Ji's* FTP proxy server. (Petition at 45). As with the combination of *Arnold* and *Ji* proposed for Ground 4, Petitioner's sole rationale proposed for combining *Chen* with *Ji* is that "Chen and Ji are both directed to virus scanning software that can scan files on a computer that communicates with other computers." (Id.). Therefore, for at least the same reasons identified above with respect to *Arnold* and *Ji*, Petitioner provides insufficient rationale for combining *Chen* with *Ji*. (*See* Section V.C.5 above; *see also OpenTV, Inc. v. Cisco Tech., Inc.*, IPR 2013-00328 (Paper No. 13) at *12-22 (2013). Furthermore, the Petition never explain why the files scanned in *Chen* must be incoming Downloadables and provides no reason to modify Chen to scan such files. (*See* Petition at 45–46). Nor, as with the proposed combinations of *Ji* with *TBAV* and *Arnold* discussed above in Sections VI.A.4 and VI.C.5, has Petitioner complied with complied with 37 C.F.R. § 42.22(a)(2) because it does not explain how *Ji's* proxy server would be combined with *Chen's* local virus scanning system.

VI. PETITIONER'S OBVIOUSNESS ARGUMENTS FAIL AS A MATTER OF LAW BECAUSE IT DID NOT CONDUCT A COMPLETE OBVIOUSNESS ANALYSIS

As the United States Supreme Court and the Federal Circuit has repeatedly stated, any obviousness analysis must include (1) the scope and content of the prior

art, (2) the differences between the prior art and the claims at issue, (3) the level of ordinary skill in the pertinent art, and (4) relevant secondary considerations of non-obviousness. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966)). Failure to address any one of these criteria is fatal to a challenger's obviousness argument as a matter of law. *See, e.g., Apple Inc. v. Int'l Trade Comm'n*, 725 F.3d 1356, 1365–66 (Fed. Cir. 2013) (vacated and remanded ITC's ruling of obvious, as ITC failed to consider all obviousness factors, including objective evidence of secondary considerations); *Ruiz v. A.B. Chance Co.*, 234 F.3d 654, 660 (Fed. Cir. 2000) (vacated a conclusion of obviousness because the fact-finder failed to make Graham factor findings). Petitioner's failure to present the Board with a complete obviousness analysis in its Petition is, as a matter of law, enough to deny the institution of a trial on Section 103 grounds.

In this case, Petitioner's failure to even consider the objective indicia of nonobviousness in support of its obviousness allegations is fatal to its obviousness arguments. *Plantronics, Inc. v. Aliph, Inc.*, 724 F.3d 1343, 1355 (Fed. Cir. 2013) ("This court has consistently pronounced that all evidence pertaining to the objective indicia of nonobviousness must be considered before reaching an obviousness conclusion."). The objective indicia of nonobviousness—also called "secondary considerations"—such as commercial acquiescence through the taking of licenses, commercial success, praise, and copying, are an important and critical

part of the obviousness analysis. Failing to provide any consideration of the secondary indicia of nonobviousness is a fatal flaw in Petitioner's Petition. Shockingly, the Petition did not address the objective indicia at all, ignoring the Federal Circuit's guidance that "[w]hether before the Board or a court, . . . consideration of the objective indicia is part of the whole obviousness analysis, not just an afterthought." *Leo Pharmaceutical v. Rea*, 726 F.3d 1346, 1357–58 (Fed. Cir. 2013). Secondary or objective indicia of nonobviousness are independent evidence of nonobviousness. *Id.*; *Ortho-McNeil Pharm., Inc. v. Mylan Labs, Inc.*, 520 F.3d 1358, 1365 (Fed. Cir. 2008). "Objective indicia 'can be the most probative evidence of nonobviousness in the record, and enables the court to avert the trap of hindsight.'" *Leo Pharm.*, 726 F.3d at 1358 (quoting *Crocs, Inc. v. Int'l Trade Comm'n*, 598 F.3d 1294, 1310 (Fed. Cir. 2010)) ("Here, the objective indicia of nonobviousness are crucial in avoiding the trap of hindsight when reviewing, what otherwise seems like, a combination of known elements.").

In other words, objective indicia of nonobviousness must always be considered. *Plantronics, Inc. v. Aliph, Inc.*, 724 F.3d 1343, 1355 (Fed. Cir. 2013). Such evidence "cannot be overlooked" and indeed can "serve to resist the temptation to read into the prior art teachings of the invention in issue." *Id.* (quoting *In re Cyclobenzaprine Hydrochloride Extended–Release Capsule Patent Litig.*, 676 F.3d 1063, 1076 (Fed. Cir. 2012)). *See also Rambus Inc. v. Teresa*

Stanek Rea, 731 F.3d 1248, 1257 (Fed. Cir. 2013) (overturning Board because it failed to consider objective indicia of nonobviousness).

In the active litigation between Patent Owner and Petitioner, Patent Owner has provided Petitioner with substantial evidence related to secondary considerations of nonobviousness. Thus, there is simply no excuse for Petitioner's failure to address this critical portion of the obviousness analysis—except for the fact that such analysis completely defeats Petitioner's obviousness arguments. The evidence of secondary considerations of nonobviousness provided to Petitioner included: industry praise; licensing of Finjan's patent portfolio, including the '494 patent, to several technology companies, including McAfee, Inc./Intel Corporation, Websense, Inc., Webroot Inc., Trustwave Holdings, Inc., M86 Security and Microsoft; copying by competitors; and commercial success. *See* Ex. 2006 at 8–13.

The fact that Petitioner chose to ignore this evidence, skip this important component of the obviousness analysis, and provide the Board with an incomplete obviousness analysis is basis alone for denying its obviousness arguments asserted in Grounds 1–4. Such objective indicia can be "the most probative evidence of nonobviousness in the record, and enables the court to avert the trap of hindsight." *Leo Pharm.*, 726 F.3d at 1358 (quoting *Crocs, Inc. v. Int'l Trade Comm'n*, 598 F.3d 1294, 1310 (Fed. Cir. 2010)).

VII. THE PROPOSED GROUNDS ARE CUMULATIVE

Petitioner's redundancy argument misunderstands the law and should be rejected. Although Petitioner alleges certain statements about the strengths of each ground, these statements are completely unsupported by any evidence. Furthermore, Petitioner omits any mention of the relative weaknesses of any . To the contrary, "the focus is on whether the Petitioner articulated a meaningful distinction in terms of relative strengths ***and weaknesses*** with respect to application of the prior art disclosures to one or more claim limitations." IPR2013-00523, Paper 26 at 4.

VIII. TBAV IS NOT PRIOR ART UNDER 35 U.S.C. § 102(a)

Petitioner relies upon the assertion that *TBAV* was "publicly available by at least October 25, 1996, as evidenced by the fact that it was disclosed by a patent applicant in an Information Disclosure Statement …filed on October 25, 1996." (Petition at 17). However, the mere fact that the *TBAV* reference was disclosed in an IDS does not demonstrate public availability under 35 U.S.C. § 102(a).

35 U.S.C. § 102(a) states that a person is entitled to a patent unless "the invention [or an obvious extension thereof under 35 U.S.C. § 103(a)] was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent." For a reference to qualify as a printed publication under 35 U.S.C.

§ 102(a), "the one who wishes to characterize the information, in whatever form it may be, as a 'printed publication' … should produce sufficient proof of its dissemination or that it has otherwise been available and accessible to persons concerned with the art to which the document relates and thus most likely to avail themselves of its contents." *In re Wyer*, 655 F.2d 221, 227 (CCPA 1981). This the Petitioner has not done.

Petitioner has merely demonstrated that the *TBAV* reference was known to a single patent attorney as of October 25, 1996. (Petition at 17). This is not proof that it was "accessible to persons concerned with the art" as of that date. It is certainly possible that the patent attorney who submitted the *TBAV* reference to the United States Patent & Trademark Office received the reference in confidence, perhaps via representation of the authors of the *TBAV* reference in intellectual property matters. Petitioner at least has not demonstrated otherwise as is its burden.

IX. CONCLUSION

Petitioner has not established a reasonable likelihood that it will prevail in establishing that claims 1, 10, 14, and 18 of the '494 Patent are invalid. Finjan accordingly requests that the Board deny institution of *inter partes* review of the '494 Patent.

Respectfully submitted,

Dated: July 14, 2015

/James Hannah/

James Hannah (Reg. No. 56,369)
Paul Andre (*pro hac vice to be applied for*)
Michael H. Lee (Reg. No. 63,941)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
Tel: 650.752.1700 Fax: 212.715.8000

Attorneys for Petitioner

(Case No. IPR2015-01022)

SOPHOS, INC.,
v.
FINJAN, INC.,

Case IPR2015-01022
Patent 8,677,494

PATENT OWNER'S EXHIBIT LIST

Exhibit-2001 *Finjan, Inc. v. Sophos, Inc.*, 14-cv-1197-WHO (N.D. Cal.), Dkt. No. 54 ("Joint Claim Construction and Pre-Hearing Statement")

Exhibit-2002 IBM Dictionary of Computing

Exhibit-2003 *Finjan, Inc. v. Sophos, Inc*., 14-cv-1197-WHO (N.D. Cal.), Dkt. No. 73 ("Sophos Claim Construction Order")).

Exhibit-2004 *Innovators of the Net: Brendan Eich and JavaScript* available at https://web.archive.org/web/20080208124612/http:/wp.netscape.com/comprod/columns/techvision/innovators_be.html

Exhibit-2005 Screenshot of bibliographic data for U.S. Patent No. 6,067,410.

Exhibit-2006 *Finjan, Inc. v. Sophos, Inc.*, Case No.: 14-cv-01197-WHO (Plaintiff Finjan, Inc.'s First Supplemental Responses to Defendant Sophos Inc.'s First Set of Interrogatories (Nos. 1, 2, 3, 4, 5, 7, and 8), dated December 9, 2014

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), the undersigned certifies that a true and correct copy of the foregoing Patent Owner's Preliminary Response was served on July 14, 2015 by filing this document through the Patent Review Processing System as well as delivering via electronic mail upon the following counsel of record for Petitioner:

James M. Heintz, Esq.
Nicholas J. Panno, Esq.
DLA Piper (US) LLP
11911 Freedom Drive, Suite 300
Reston, VA 20190
Sophos-Finjan-494IPR@dlapiper.com

/James Hannah/
James Hannah (Reg. No. 56,369)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road,
Menlo Park, CA 94025
(650) 752-1700