Trials@uspto.gov
571-272-7822

Paper 14
Entered: August 2, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SOPHOS LTD. and SOPHOS INC.,
Petitioner,

v.

OPEN TEXT INC.,
Patent Owner.

IPR2023-00491
Patent 9,413,721 B2

Before PATRICK M. BOUCHER, MICHELLE N. WORMMEESTER, and AARON W. MOORE, *Administrative Patent Judges*.

BOUCHER, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314(a)

Sophos Ltd. and Sophos Inc. (collectively, "Petitioner") filed a Petition pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1, 8, 9, 14, and 15 of U.S. Patent No. 9,413,721 B2 (Ex. 1001, "the

'721 patent"). Paper 1 ("Pet."). Open Text Inc. ("Patent Owner") filed a Preliminary Response. Paper 13 ("Prelim. Resp.").[1]

We have authority under 35 U.S.C. § 314 and 37 C.F.R. § 42.4. Applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we deny the Petition and do not institute an *inter partes* review.

I. BACKGROUND

A. The '721 Patent

1. Overview

The '721 patent "relates generally to methods and apparatus for dealing with malware." Ex. 1001, 1:29–31. Such methods and apparatus operate within a distributed network that includes multiple "remote" computers connected via the Internet to a "base computer" that may be in communication with a "community database." *Id.* at 3:59–4:21. Figure 2 of the '721 patent, which is identified in the drawing as "Prior Art," is reproduced below.

[1] On July 27, 2023, i.e., less than three weeks before the statutory deadline for determining whether to institute an *inter partes* review, Petitioner requested authorization to file a Reply to the Preliminary Response, with Patent Owner filing a Sur-reply, as well as to file a new stipulation that might bear on Patent Owner's argument that we exercise discretion to deny the Petition under *Apple Inc. v. Fintiv Inc.*, IPR2020-00019, Paper 11 (PTAB March 20, 2020) (precedential). Ex. 3001; *see* Prelim. Resp. 4–21. We denied the request. Ex. 3001. Petitioner's request comes too late to accommodate Petitioner's proposed briefing schedule within the statutory timeframe, and, as we explain below, we do not reach Patent Owner's *Fintiv* argument.

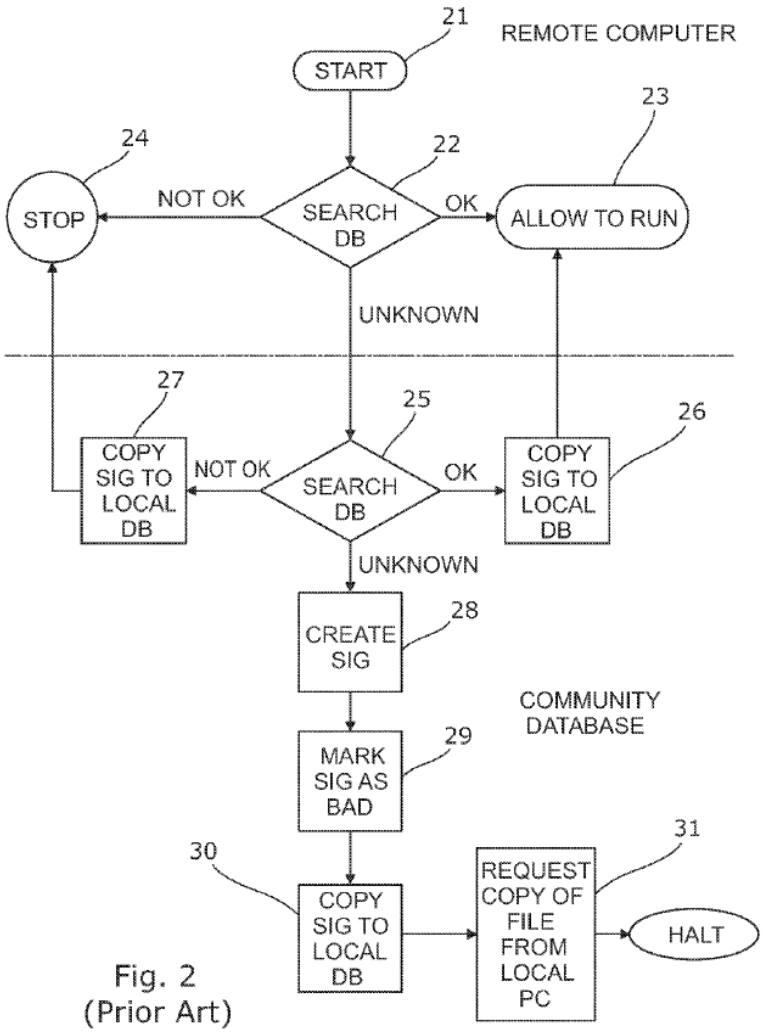

Fig. 2
(Prior Art)

Figure 2 is a flowchart illustrating a method that starts at step 21 by running an object, such as a process, at one of the remote computers. *Id.* at 4:22–23. At step 22, operation of such a process is hooked using local software running on the remote computer to search a local database for a signature or key representing that process and related objects. *Id.* at 4:23–29. If the signature indicates that the process is safe, it is allowed to run at step 23; if the signature indicates that the process is not safe, it is stopped at step 24. *Id.* at 4:29–38.

If the object is unknown locally, details are passed over a network, such as the Internet, for storage in, and comparison with, a community

database that stores signatures representative of objects from multiple remote computers. *Id.* at 4:60–63. Specifically, such a community database is searched at step 25 for a signature for the object that has already been stored. *Id.* at 4:63–66. If found and identified as safe, then "a copy of the signature or at least a message that the object is safe" is sent to the remote computer at step 26; similarly, if found and identified as unsafe, a copy is provided to the remote computer with such a designation at step 27. *Id.* at 5:9–26. If the object is unknown to the community database, a signature is created at step 28 and marked as unsafe at step 29. *Id.* at 5:27–32. Such an unsafe designation may be changed as experience with the object is collected. *See id.* at 5:50–63.

Figure 3 of the '721 patent is reproduced below.

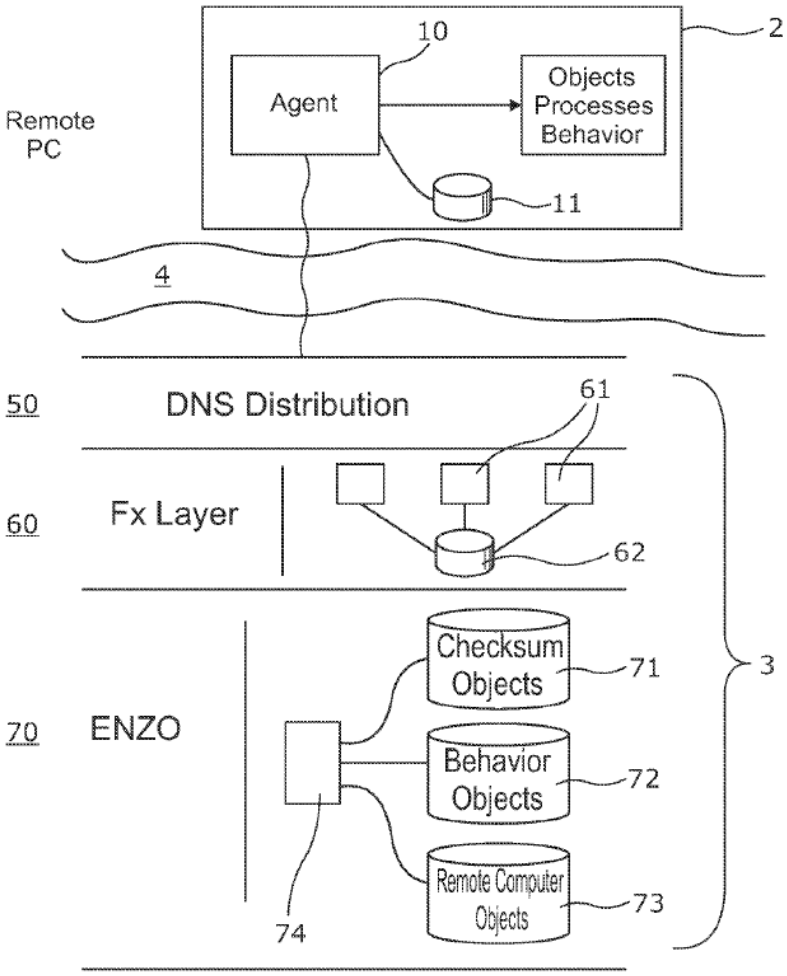

Fig. 3

Figure 3 shows an arrangement of the base computer. *Id.* at 8:40–41. Remote computer 2 has agent program 10, which monitors objects and their behavior on remote computer 2, and which may communicate with local database 11. *Id.* at 8:41–51. Agent program 10 also communicates with base computer 3 over the Internet via Domain Name Resolution System ("DNS") 50 to send details of new objects and behavior found on remote

computer 2, and to receive determinations of whether the objects are safe. *Id.* at 8:43–48, 9:13–15.

Base computer 3 has "FX layer" 60 with one or more "threat servers" 61 to which remote computers 2 are allocated. *Id.* at 9:16–23. FX layer 60 "makes real time decisions as to whether or not an object [4] is benign or malevolent based on the details of that object send from the remote computer." *Id.* at 9:24–26. Each threat server is connected to database 62, "which contains entries for all of the objects known to the base computer 3 and a classification of whether the object is safe or unsafe," as well as "rules for deciding whether unknown objects are safe or unsafe based on the information received from the remote computer 2." *Id.* at 9:26–32. Threat server 61 first searches database 62 for matching signatures, which can be a function of hashes derived from the file itself, event data involving object 4, and/or metadata about object 4. *Id.* at 9:32–37. If object 4 is unknown, web server 61 determines whether any of the rules classify object 4 as unsafe. *Id.* at 9:37–39. Threat server 61 then communicates back to remote computer 2 whether the object is safe, unsafe, or unknown. *Id.* at 9:39–43.

Information about objects 4 received by FX layer 60 from remote computers 2 is sent to "ENZO layer" 70 to maintain a master record. *Id.* at 9:47–52. This layer has one or more "central servers" 74 connected to master databases that aggregate all information received from all web servers 61 from all remote computers 2. *Id.* at 9:53–57. Such master databases may include: (1) object database 71, which has entries containing object signatures and metadata received about objects, *id.* at 9:60–64; (2) behavior database 72 populated by the event data sent from remote computers 2, *id.* at 9:65–10:3; and (3) computer-object database 73, "which

associates remote computers 2 in the community with objects observed on those remote computers 2 by associating objects with identification codes sent from the remote computer 2 during object detail transmission," *id.* at 9:4–8.

2. Illustrative Claim

Challenged independent claim 1 is representative of the challenged claims, and is reproduced below.

> 1. A method of classifying a computer object as malware, the method comprising:
>
> receiving, at a first threat server, details of a first computer object from a first remote computer, wherein the details of the first computer object include data uniquely identifying the first computer object;
>
> determining, by the first threat server, whether the first computer object has been previously seen by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server;
>
> receiving additional information about the first computer object from the first remote computer when the first computer object has not been previously seen;
>
> storing the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen;
>
> providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer;
>
> increasing a count associated with a number of times that the first computer object has been seen, and providing the increased count associated with the number of times that the first computer object has been seen to the central server; and

> receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database.

Ex. 1001, 24:18–53.

B. Evidence

Petitioner relies on the following references:

Liu	US 2006/0075504 A1	Apr. 6, 2006	Ex. 1005
Tuvell	US 2008/0086773 A1	Apr. 10, 2008	Ex. 1006
Kester	US 2005/0223001 A1	Oct. 6, 2005	Ex. 1007

In addition, Petitioner relies on a Declaration by Richard Newman, Ph.D. Ex. 1003. Patent Owner relies on a Declaration by Alessandro Orso, Ph.D. Ex. 2001.

C. Asserted Grounds of Unpatentability

Petitioner challenges claims 1, 8, 9, 14, and 15 on the following grounds. Pet. 7.

Claim(s) Challenged	35 U.S.C. §[2]	References
1, 8, 9, 14, 15	103	Liu, Tuvell, Kester

[2] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C § 103. The '721 patent was filed on February 13, 2012, and claims the benefit of a provisional application filed on February 15, 2011. Ex. 1001 at codes (22), (60); *see* Pet. 5 n.1. We accordingly apply the pre-AIA version of § 103 herein.

D. Real Parties in Interest

Petitioner identifies Sophos Ltd. and Sophos Inc. as real parties in interest. Pet. 2. Patent Owner identifies Open Text Inc. and Webroot LLC as real parties in interest. Paper 4, 1. "Out of an abundance of caution, Patent Owner further identifies the following affiliates: Carbonite, LLC; Open Text Corporation; and Open Text Holdings, Inc." *Id.*

E. Related Matters

Both parties identify the following district court litigations as related matters involving the '721 patent: *Webroot, Inc. v. Sophos Ltd.*, No. 6:22-cv-240 (W.D. Tex.); and *Webroot, Inc. v. Forcepoint LLC*, No. 6:22-cv-342 (W.D. Tex.). Pet. 2; Paper 4, 1. Patent Owner advises that "[t]hese cases are now consolidated, along with three others" as *Webroot, Inc. v. AO Kaspersky Lab*, No. 6:22-cv-00243 (W.D. Tex.) ("the related litigation").

Patent Owner further identifies certain *inter partes* review proceedings involving patents that are "not related to the '721 Patent, but which [are] also asserted in the related district court litigations," namely IPR2022-01522, IPR2023-00124, IPR2023-00126, and IPR2023-00289. Paper 4, 1–2.

III. ANALYSIS

A. Legal Principles

A claim is unpatentable for obviousness under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are "such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said

subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective indicia of nonobviousness, i.e., secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of "whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness")); *see In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

B. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham*, 383 U.S. at 17. "The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry." *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991). The "person of ordinary skill in the art" is a hypothetical construct, from whose vantage point obviousness is assessed. *In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998). "This legal construct is akin to the 'reasonable person' used as a

reference in negligence determinations" and "also presumes that all prior art references in the field of the invention are available to this hypothetical skilled artisan." *Id.* (citing *In re Carlson*, 983 F.2d 1032, 1038 (Fed. Cir. 1993)).

Petitioner proposes that a person of ordinary skill in the art "would have had at least a Bachelor's degree in Computer Science, Computer Engineering, Electrical Engineering, or an equivalent discipline, and at least two years' worth of experience developing computer networking or network architecture, or a Master's degree in a related field." Pet. 9. Petitioner adds that, alternatively, a person of ordinary skill in the art "could have four or more years of work experience in computer networking and in the development of client-server systems." *Id.* Petitioner supports its articulation of the level of ordinary skill in the art with testimony by Dr. Newman. Ex. 1003 ¶ 17.

Patent Owner's statement of the level of ordinary skill is generally similar, and supported with testimony by Dr. Orso, who characterizes the parties' respective positions as having "minor variations." Prelim. Resp. 27; Ex. 2001 ¶¶ 39–42. According to Patent Owner, a person of ordinary skill in the art "would have had a bachelor's degree in an accredited program of electrical engineering, computer engineering, or computer science, or a similar discipline, and have 2-3 years of practical work experience in the general fields of electrical engineering, computer science, networking communications, and/or device and network security." Prelim. Resp. 27. Patent Owner adds that "[m]ore advanced degrees and/or training in a related discipline can compensate for shorter work experience." *Id.*

For purposes of this Decision, we adopt Petitioner's proposal, which we find consistent with the level of skill reflected by the prior art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (the prior art may reflect an appropriate level of skill in the art). But we note that we would reach the same ultimate conclusion not to institute *inter partes* review if we were to adopt Patent Owner's proposal. *See* Prelim. Resp. 27 (Patent Owner stating that "[a]lthough Patent Owner's [person of ordinary skill in the art] definition differs slightly from Petitioner's, Patent Owner's positions and arguments do not change based on which [person of ordinary skill in the art] definition the Board applies"); Ex. 2001 ¶ 42 (Dr. Orso testifying that the "minor variations" in the parties' proposals "would not alter [his] opinions.").

C. Claim Construction

The Board uses "the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." 37 C.F.R. § 42.100(b) (2019); *see Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). According to Petitioner, the parties "disagree over the construction of certain terms in the parallel District Court litigation," but both parties propose that we apply the plain and ordinary meaning to all terms in evaluating the Petition. Pet. 7–8; Prelim. Resp. 26.

In light of this agreement, we do not find it necessary to construe any terms for purposes of this Decision. *See Nidec Motor Corp. v. Zhongshan*

Broad Ocean Motor Co., 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'" (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))). We nevertheless note that the district court determined that the plain and ordinary meaning of "object behavior information," recited in challenged claims 1, 9, and 14, "does not include the static attributes of the object." Ex. 2007, 3.

D. Overview of the Prior Art

1. Liu

Liu "relates to detecting and protecting computers from threats that can be spread over a computer network and more specifically to the use of remote expert systems in threat protection." Ex. 1005 ¶ 2. Figure 1 of Liu is reproduced below.

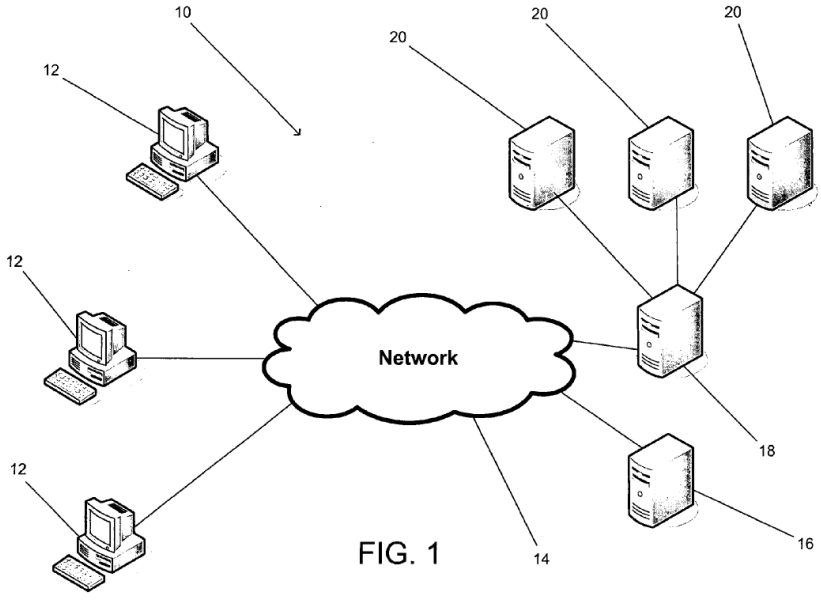

Figure 1 illustrates threat protection network 10, which includes computers 12 connected via network 14, alert server 16, and a threat identification

system. *Id.* ¶ 66. The threat identification system includes threat identification server 18, which is connected to isolated computers 20, each of which is isolated from the broader network. *Id.* "In many embodiments, the alert server 16 and the computers 12 form a secure peer-to-peer network." *Id.* ¶ 70.

Client software installed on each of computers 12 is executed as a background process and "is designed to operate in conjunction with the other aspects of the threat protection network to protect each of the computers from one or more classes of threat." *Id.* ¶ 67. When the client software encounters a potential unknown threat, the client can contact alert server 16. *Id.* If alert server 16 does not possess information about the potential threat, alert server 16 provides the potential threat to the threat identification system, "which exposes the isolated computers 20 to the potential threat and observes their behavior." *Id.* "Based upon the behavior of the isolated computers 20, the threat identification system can determine whether the potential threat is an actual threat," such as by using an expert system located on threat identification server 18. *Id.* "Once a determination has

been made, the alert server 16 can generate an update for distribution to the computers 12." *Id.*

2. *Tuvell*

Tuvell "relates generally to systems, devices, and methods for detecting malware in mobile networks and mobile devices." Ex. 1006 ¶ 2. Figure 11 of Tuvell is reproduced below.

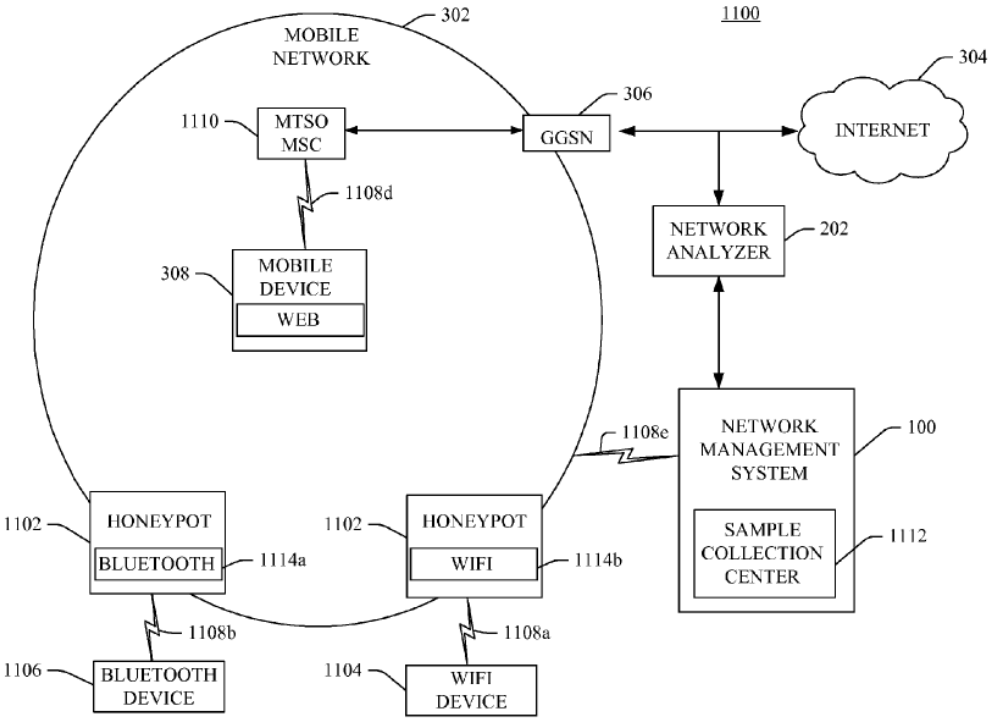

FIG. 11

Figure 11 depicts malware sample collection system 1100, used for obtaining samples of executable code spreading within mobile network 302 and sending those samples to sample collection center 1112 for analysis. *Id.* ¶ 73. Collection agents (also referred to as "honeypots" in Tuvell) 1102 are distributed within mobile network 302 at various network locations or sites to collect executable programs being monitored by protocol handler 1114

(examples including bluetooth protocol handler 1114a and WiFi protocol handler 1114b). *Id.* In operation, collection agent 1102 accepts incoming call attempts from malware-infected devices 1104, 1106 and forwards any transferred executables to sample collection center 1112 of network management system 100 using the provider's mobile network 302. *Id.* ¶ 74. Calls from collection agent 1102 may be switched through the provider's mobile network 302 using wireless data connection 1108e, or collection agent 1102 may send information to sample collection center 1112 across a public switched telephone network ("PSTN"). *Id.*

Figure 12 of Tuvell is reproduced below.

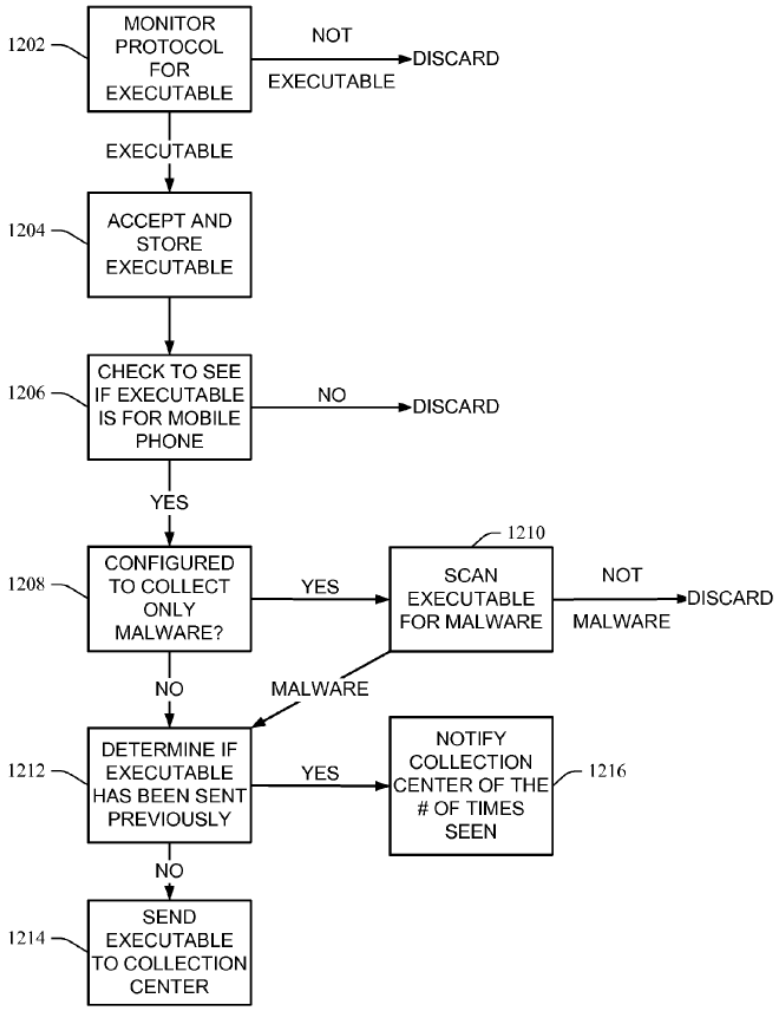

FIG. 12

Figure 12 is a flow diagram illustrating a method used by collection agents 1102. *Id.* ¶¶ 24, 85. At step 1202, collection agent 1102 monitors a protocol via protocol handler 1114, discarding those samples that do not contain executable code. *Id.* ¶ 85. At step 1204, collection agent 1102 stores those samples that contain executable code, and discards those that are not for mobile devices at step 1206. *Id.* ¶ 86. If collection agent 1102 is configured to collect only malware-infected executables, collection agent 1102 scans the executable for malware at step 1210, discarding those that do not. *Id.* ¶

87. At step 1212, collection agent 1102 determines whether the executable has been previously seen and sent to sample collection center 1112. If so, collection center 1112 is notified at step 1216 that the malware is being identified again; if not, the sample executable is net at step 1214 to sample collection center 1112 for further analysis and reporting.

3. Kester

Recognizing that employee activation of software applications can "pose new threats to an employer," Kester describes "monitoring and controlling application files" operating on computing devices. Ex. 1004 ¶¶ 3, 5. Figure 1 of Kester is reproduced below.

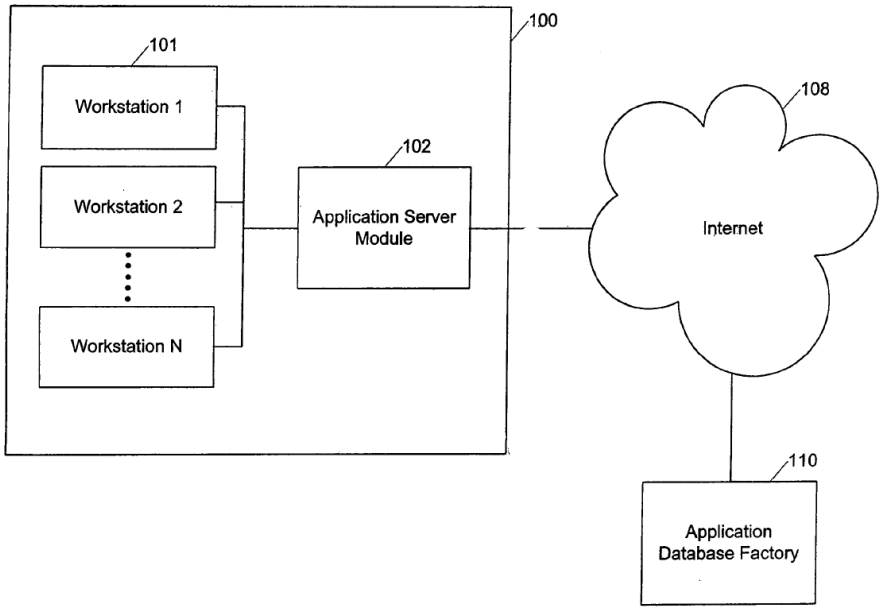

FIG. 1

Figure 1 "is a block diagram of a site collection system for controlling application files on a workstation." *Id.* ¶ 12. Multiple workstations 101, each of which includes a "workstation management module," are coupled to application server module 102, which communicates via Internet 108 to

upload and download applications with application database factory 110. *Id.* ¶¶ 27–30.

Each workstation management module maintains a "hash/policy table" that includes "one or more predetermined parsed properties and one or more policies" associated with various applications. *Id.* ¶ 32, 35. When a program on a computer or workstation is launched, the workstation management module calculates a hash for comparison with the hash/policy table. *Id.* ¶¶ 33–35. "If the hash corresponds to a hash stored in the hash/policy table . . . , the hash is applied in response to the launch of the requested application." *Id.* ¶ 76. "For example, an access privilege can include allowing the launched application to run on the workstation." *Id.* ¶ 31.

"To determine the access privilege for the workstation 101 and/or user, the workstation management module 101 can utilize a predetermined association between the launched application and one or more categories." *Id.* Such predetermined associations are made by a network administrator who "interfaces with the application server module 102 via [a] classification user interface" and "can classify uncategorized applications." *Id.* ¶ 50. In particular, the network administrator receives data from an application inventory database via the classification user interface "to select or create access privileges/policies/rules for users, workstation[s], and/or groups of users/workstations." *Id.*

E. Independent Claim 1

Petitioner challenges independent claim 1 as unpatentable under 35 U.S.C. § 103(a) over Liu, Tuvell, and Kester. Pet. 20–51. In doing so, Petitioner relies primarily on Liu as teaching the method recited in independent claim 1, but relies on Tuvell for those aspects of the claim related to "counting and distribution" and relies on Kester for those aspects related to "database storage." *Id.* at 25. Specifically, Petitioner relies on Liu alone for all limitations, except for (1) the "increasing a count" limitation, for which Petitioner additionally relies on Tuvell, (2) the "storing the details" limitation, for which Petitioner provides an alternative position involving Kester, *id.* at 38–39; and (3) the "providing contents" limitation, for which Petitioner additionally relies on both Tuvell and Kester. *Id.* at 40–49.

According to Petitioner, a person of ordinary skill in the art would have been motivated to combine the identified teachings of Liu, Tuvell, and Kester for "multiple reasons," and Petitioner supports those reasons with testimony by Dr. Newman. *Id.* at 22; *see* Ex. 1003 ¶¶ 68–75. Patent Owner disputes Petitioner's reasoning for combining the teachings of Tuvell with Liu, and also argues that Kester is not analogous to the claimed invention. *See* Prelim. Resp. 49–59. We do not reach these disputes between the parties because we determine that Petitioner does not adequately show that all limitations of the claim are met even within its proposed combination.

We focus particularly on those limitations related to a "central server," namely independent claim 1's recitation of (1) "providing contents of the second database to at least one database associated with *a central server*," Ex. 1001, 24:38–39 (emphasis added); (2) "providing the increased

count associated with the number of times that the first computer object has been seen to *the central server*," *id.* at 24:44–47 (emphasis added); and (3) "at least a portion of the contents of the at least one database associated with *the central server* include a subset of the details of the first computer object stored in the second database," *id.* at 24:50–53 (emphasis added). Within its proposed combination, Petitioner relies only on Liu to meet these recitations of a "central server." Pet. 43–46; *see also id.* at 48–49, 50–51.

Liu describes its threat-protection network as implemented within a peer-to-peer architecture, and Petitioner acknowledges as much. Ex. 1005, abst. ("In several embodiments, a secure peer-to-peer network is used to rapidly distribute information concerning the nature of the potential threat through the threat potential network."); Pet. 44 (Petitioner stating that "Liu describes a tiered distribution of updates within a secure peer-to-peer network"); *see* Prelim. Resp. 42–43 (Patent Owner stating that "Petitioner tacitly admits that Liu does not disclose a central server and also that its 'peer-to-peer' architecture is different from systems with a central server"). Nevertheless, Petitioner places considerable weight on Liu's limited disclosure of alternative embodiments in which "the functions of the alert server can be performed by one or more servers" and in which "the threat protection network can include numerous mirrored servers." Ex. 1005 ¶ 101.

Specifically, Petitioner bootstraps these disclosures to argue that "Liu discloses the 'central server' because any of the disclosed mirrored alert servers (or network of alert servers) in Liu is an example of the claimed 'central server.'" Pet. 44. This follows, according to Petitioner, in light of Dr. Newman's testimony that, because mirrored servers have copies of

server content, a person of ordinary skill in the art would have known that "the fact that the threat-protection network can include multiple mirrored servers would mean that other servers contain the same information as that stored on the first alert server." *Id.* at 44–45; Ex. 1003 ¶ 128. Alternatively, Petitioner relies on Dr. Newman's testimony to argue that a person of ordinary skill in the art "would also have found it obvious to implement the functionality of Liu's threat-protection server or servers in a hub-and-spoke architecture, with a central server, rather than a peer-to-peer architecture." Pet. 45 (citing Ex. 1003 ¶ 129).

There are a number of difficulties with Petitioner's position, which appears to be conceived with the aid of hindsight to reconstruct the claimed invention. *See Sensonics Inc. v. Aerosonic Corp.*, 81 F.3d 1566, 1570 (Fed. Cir. 1996) ("The invention must be viewed not after the blueprint has been drawn by the inventor, but as it would have been perceived in the state of the art that existed at the time the invention was made."). First, Petitioner considers each of the mirrored servers in its conception of Liu also to correspond to the claim's recited "threat servers." Pet. 50. As Dr. Orso testifies, "Liu's mirror servers are effectively identical to each other" and "even if Liu's mirror servers could be interpreted as teaching the claimed threat servers . . . [,] there is no 'central server' in Liu's peer-to-peer network of mirrored servers." Ex. 2001 ¶ 70.

Furthermore, as Dr. Orso also highlights, the '721 patent disparages the kind of duplication that Petitioner proposes though the use of mirror servers in Liu. *See id.* In particular, the '721 patent explains that "web servers 61 in a typical implementation will be dealing with huge amounts of data." Ex. 1001, 12:20–22. As a consequence, "it is impractical to store all

web data on all web servers 61 in all regions." *Id.* at 12:24–27. Indeed, the '721 patent specifically distinguishes its invention by adding that its "scheme has been found to reduce workload and traffic in the network by a factor of about 50 compared with a conventional scheme where typically each piece of data on being received by a web server would immediately be propagated to all other servers in the system." *Id.* at 12:55–59.

In light of these disclosures and Dr. Orso's testimony, we agree with Patent Owner that Petitioner's conception of Liu "would render the 'central server' superfluous and yield a system that suffers from the same problems in conventional systems that the '721 patent explicitly identified and improved on." *See* Prelim. Resp. 44. We also agree with Patent Owner's understanding of the implications of using mirror servers for both the recited "central server" and the recited "threat servers" as Petitioner proposes, because, "if every server on the network contained identical information, there would be no reason for threat servers to transmit information to the central server, since all servers would already have the same information." *Id.* at 44–45. Dr. Orso confirms these implications. Ex. 2001 ¶ 74 (Dr. Orso testifying that the duplication "conflicts with the role of the central server in the '721 patent. Because the first, second, etc., threat servers would all contain identical information, there would be no reason for threat servers to pull or pass information to the central server, since all the threat servers already have the same information—thereby obviating the central server.").

For these reasons, we determine that Petitioner does not make a sufficient showing that its proposed combination of Liu, Tuvell, and Kester meets the limitations of independent claim 1 that include a "central server." We accordingly conclude that Petitioner does not demonstrate a reasonable

likelihood of prevailing on its challenge of independent claim 1 as unpatentable under 35 U.S.C. § 103(a) over Liu, Tuvell, and Kester.

F. Independent Claim 9

Petitioner challenges independent claim 9 as unpatentable under 35 U.S.C. § 103(a) over Liu, Tuvell, and Kester. Pet. 57–59. Like independent claim 1, independent claim 9 includes limitations that recite a "central server." Ex. 1001, 25:47–26:24. Indeed, Petitioner characterizes independent claim 9 as "materially identical to claim 1, except claim 9 is a system claim [rather than a method claim," and relies on the same evidence and arguments as presented in challenging independent claim 1. Pet. 57–59 (referring to analysis of independent claim 1 for all limitations).

For the same reasons we express for independent claim 1, we determine that Petitioner does not make a sufficient showing that its proposed combination of Liu, Tuvell, and Kester meets the limitations of independent claim 9 that include a "central server." We accordingly conclude that Petitioner does not demonstrate a reasonable likelihood of prevailing on its challenge of independent claim 9 as unpatentable under 35 U.S.C. § 103(a) over Liu, Tuvell, and Kester.

G. Dependent Claims 8, 14, and 15

Claim 8 depends from independent claim 1, and claims 14 and 15 depend from independent claim 9. Petitioner challenges these claims as unpatentable under 35 U.S.C. § 103(a) over Liu, Tuvell, and Kester. Pet. 51–57, 59–62. Such dependent claims include the limitations of the underlying independent claims, including those limitations for which

Petitioner makes an insufficient showing. We accordingly conclude that Petitioner does not demonstrate a reasonable likelihood of prevailing on its challenge of dependent claims 8, 14, or 15 as unpatentable under 35 U.S.C. § 103(a) over Liu, Tuvell, and Kester.

H. Discretion Under 35 U.S.C. § 314(a)

As noted above, the '721 patent is the subject of parallel proceedings in the form of the related litigation. *Supra*, § I.E. Patent Owner asks that we exercise our discretion to deny the Petition based on the state of the related litigation. Prelim. Resp. 4–21. Because we deny the Petition on the merits, we do not reach this issue.

I. Conclusion

For the foregoing reasons, we conclude that the information presented in the Petition does not establish a reasonable likelihood that Petitioner would prevail in showing that at least one of claims 1, 8, 9, 14, and 15 of the '721 patent is unpatentable. Accordingly, we deny the Petition and decline to institute an *inter partes* review.

III. ORDER

In consideration of the foregoing, it is

ORDERED that the Petition is *denied*, and no trial is instituted.

PETITIONER:

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

PATENT OWNER:

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