Trials@uspto.gov
571-272-7822

Paper 41
Entered: March 2, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

McAFEE, INC.,
Petitioner,

v.

CAP CO., LTD.,
Patent Owner.

Case IPR2015-01855
Case IPR2015-01877
Case IPR2016-00216
Case IPR2016-00222[1]
Patent RE42,196 E

Before DONNA M. PRAISS, PATRICK M. BOUCHER, and J. JOHN LEE, *Administrative Patent Judges*.

BOUCHER, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

[1]IPR2015-01855, IPR2015-01877, and IPR2016-00222 have been consolidated.

McAfee, Inc. ("Petitioner") filed four Petitions pursuant to 35 U.S.C. §§ 311–319 to institute *inter partes* reviews challenging claims of U.S. Patent No. RE42,196 E ("the '196 patent"). IPR2015-01855, Paper 1 ("Pet. 1855"); IPR2015-01877, Paper 2 ("Pet. 1877"); IPR2016-00216, Paper 1 ("Pet. 216"); IPR2016-00222, Paper 1 ("Pet. 222"). After consideration of the respective Preliminary Responses, we instituted review in each of the proceedings, and consolidated IPR2015-01855, IPR2015-01877, and IPR2016-00222. IPR2015-01855, Paper 14 ("Dec. 1855"), 20; IPR2015-01877, Paper 13 ("Dec. 1877")[2], 20; IPR2016-00216, Paper 8 ("Dec. 216"), 19; IPR2016-00222, Paper 8 ("Dec. 222"), 18. Across the four proceedings, review was instituted for claims 1–5, 7–12, 14, 15, and 32–35. Dec. 1855, 20–21; Dec. 1877, 20–21; Dec. 216, 19; Dec. 222, 18.

During the trial, Patent Owner timely filed a Response in each of the proceedings. IPR2015-01855, Paper 24 ("PO Resp. 1855"); IPR2015-01877, Paper 23 ("PO Resp. 1877"); IPR2016-00216, Paper 16 ("PO Resp. 216"); IPR2016-00222, Paper 16 ("PO Resp. 222"). Petitioner timely filed respective Replies to the Patent Owner Responses. IPR2015-01855, Paper 30 ("Reply 1855"); IPR2015-01877, Paper 28 ("Reply 1877"); IPR2016-00216, Paper 22 ("Reply 216"); IPR2016-00222, Paper 21 ("Reply 222").

Patent Owner filed a Motion to Amend the claims in each of the proceedings. IPR2015-01855, Paper 23 ("Mot. Amend 1855"); IPR2015-

[2] Because IPR2015-01855 was consolidated with IPR2015-01877 before further consolidation with IPR2016-00222, Paper 13 of IPR2015-01877 is identical to Paper 14 of IPR2015-01855.

01877, Paper 22 ("Mot. Amend 1877"); IPR2016-00216, Paper 19[3] ("Mot. Amend 216); IPR2016-00222, Paper 15 ("Mot. Amend 222"). Petitioner filed respective Oppositions to the Motions to Amend. IPR2015-01855, Paper 31; IPR2015-01877, Paper 29; IPR2016-00216, Paper 23; IPR2016-00222, Paper 22. Patent Owner filed respective Replies to the Oppositions. IPR2015-01855, Paper 35; IPR2015-01877, Paper 33; IPR2016-00216, Paper 27; IPR2016-00222, Paper 26.

A consolidated oral hearing for the four proceedings was held on December 7, 2016, and a copy of the transcript was entered into the record for each proceeding. IPR2015-01855, Paper 48; IPR2015-01877, Paper 46; IPR2016-00216, Paper 40; IPR2016-00222, Paper 39 (collectively, "Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the claims on which we instituted trial. Based on the record before us, Petitioner has shown, by a preponderance of the evidence, that claims 1–5, 7–12, 14, and 15 of the '196 patent are unpatentable.[4]

---

[3] The Motion to Amend filed in IPR2016-00216 "requests the Board to cancel claims 32-35 in the '196 patent." Mot. Amend 216, 1. Because we grant this request, we do not further discuss claims 32–35 in this Decision.
[4] There is considerable duplication in the content of documents filed in the different proceedings. In the interest of efficiency and clarity, we cite below to the record of one proceeding, usually IPR2015-01855, where the same argument or evidence has been filed in multiple proceedings. Unless otherwise indicated explicitly, citation below to a paper or exhibit should be understood to be a citation to the record of IPR2015-01855.

I. BACKGROUND

A. The '196 Patent

1. Overview

The '196 patent describes systems and methods for online diagnosing, remedying, and blocking of harmful information, such as computer viruses. Ex. 1001, col. 1, ll. 20–24. Identifying deficiencies in then-existing techniques for protecting against such harmful information—namely, manual installation of antivirus software and/or the use of post-infection responses—the '196 patent describes "a harmful information blocking program which is automatically transmitted and installed in the client system upon accessing to the web server via a computer network." *Id.* at col. 2, ll. 29–37; *see id.* at col. 1, l. 57–col. 2, l. 26.

Figure 2A of the '196 patent is reproduced below.

FIG. 2A

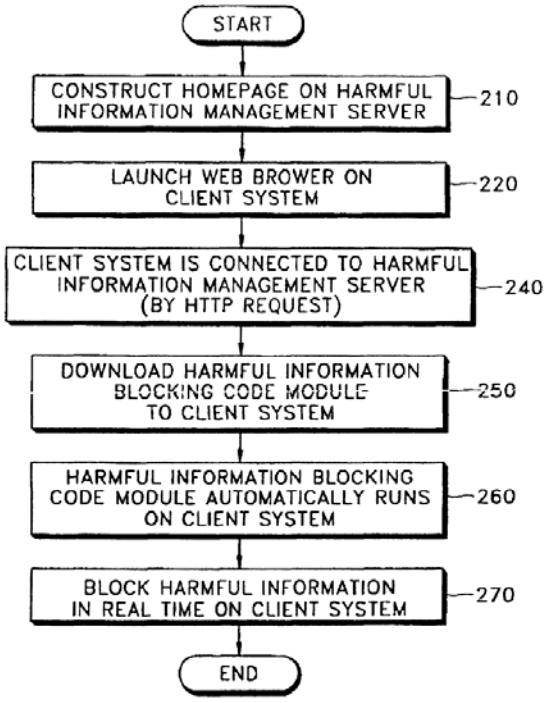

Figure 2A is a flowchart illustrating an online method of blocking harmful information. Ex. 1001, col. 4, ll. 32–34. After constructing a homepage on a server, launching a web browser on a client system, and connecting the client system to the server at blocks 210, 220, and 240, a harmful-information blocking-code module is downloaded to the client system at block 250. *Id.* at col. 4, l. 61–col. 6, l. 2. The module automatically runs on the client system at block 260 to block harmful information "in real time" at block 270. *Id.* at col. 5, ll. 40–44. The '196 patent discloses a similar embodiment in Fig. 2B and its related discussion that uses a second server to provide hyperlink information used in accessing the server. *Id.* at col. 6, ll. 1–28.

2. Illustrative Claim

Independent claim 1 of the '196 patent is illustrative of the claims at issue:

> 1. A method for blocking in real time harmful information in a file to be executed, the method comprising the steps of:
>
> (a) on a computer network through which a web server and a client system are linked to each other, the web server receiving a connection request from the client system over the computer network;
>
> (b) the web server transmitting a harmful information blocking code module to the client system; and
>
> (c) once the transmission of the harmful information blocking code module is completed, the harmful information blocking code module automatically running on the client system to block in real time harmful information including computer viruses,
>
> wherein the step (c) comprises steps of:

> (c1) inspecting file input/output (I/O) on the client system by hooking up file I/O routines,
>
> (c2) determining whether the file to be executed corresponding to the inspected file input/output in the step (c1) is harmful or not; and
>
> (c3) treating a file determined to be harmful in the step (c2) and executing the file, if it can be treated, and aborting the execution of the file determined to be harmful in the step (c2), if it cannot be treated.

Ex. 1001, col. 9, l. 54–col. 10, l. 10.

3. Prosecution History

The ’196 patent is a reissue of U.S. Patent No. 7,062,552 B2 (Ex. 1002, “the ’552 patent”). Ex. 1001, at [64]. The ’552 patent matured from the national-stage entry of PCT/KR00/01374, which claimed priority to two Korean applications. *Id.* at [30], [63].

During prosecution of the ’552 patent, in response to a rejection by the Examiner over U.S. Patent No. 5,960,170 (“Chen”), the Applicant amended independent claim 1 in two respects. First, the preamble was amended to add the phrases “in real time” and “in a file to be executed,” while simultaneously deleting a recitation that the harmful information “includ[es] computer viruses.” Ex. 2002, 91. Second, the entire “wherein” clause, including steps (c1), (c2), and (c3), was added to the claim. *Id.* Similar amendments were made to the other independent claims. The Applicant provided the following remarks to distinguish the amended claims from Chen:

> As discussed above, Chen describes targeting <u>all</u> files to be treated, regardless of whether they are to be executed.

> Accordingly, Chen's virus detection server must provide virus detection objects and/or tailored vaccines to the client computer until additional scanning is no longer required so as to treat the viruses in all files of the client computer.
>
> In contrast to Chen, the presently claimed invention blocks harmful information in a file to be executed in real time on a computer network. The presently claimed invention thus targets only the files to be executed by the client computer at the present time. Thus, it is not necessary for the client computer to treat all files in the client computer, thereby saving time and processing resources compared to the process in Chen.
>
> Furthermore, even if Chen's initial scan was limited to less than all of the files in the client computer, nowhere does Chen disclose or suggest any step of "inspecting file input/output (I/O) on the client system by hooking up file I/O routines," or that the subset of files would be the files that are currently being executed, as required by each of the independent claims.
>
> Lastly, Chen does not disclose or suggest aborting the execution of any file that is determined to be infected with a virus, but which cannot be treated. Chen merely discloses a virus treatment program.
>
> In sum, Chen lacks any disclosure or suggestion of at least the text portions of the independent claims highlighted above. Nor do any of the remaining applied references make up for the above-highlighted deficiencies in Chen.

Id. at 100–01. The claims challenged in these proceedings were not further amended during prosecution of the reissue '196 patent, and the Examiner made no remarks when allowing those claims that have a bearing on the issues presently before us. *See* Ex. 1004.

D. Instituted Grounds of Unpatentability

Petitioner relies on the following references.

Hodges	US 6,035,423	Mar. 7, 2000	Ex. 1005
Butt	US 6,728,964 B1	Apr. 27, 2004	Ex. 1006
Freund	US 5,987,611	Nov. 16, 1999	Ex. 1007 (IPR2015-01877)
Levergood	US 5,708,780	Jan. 13, 1998	Ex. 1012

Péter Ször, "Memory Scanning Under Windows NT," *Virus Bulletin Conference, September 1999*, pp. 325–346 (Virus Bulletin Ltd., 1999) (Ex. 1007 (IPR2015-01855), "Ször")

Jeffrey O. Kephart, Gregory B. Sorkin, Morton Swimmer, Steve R. White, *Blueprint for a Computer Immune System*, Proc. Virus Bull. Int'l Conf., 159–74 (Oct. 1–3, 1997) (IEEE) (Ex. 1035 (IPR2016-00216), "Kephart")

We instituted trial based on 35 U.S.C. § 103(a) over the following combinations of references. Dec. 1855, 20–21; Dec. 1877, 20–21; Dec. 216, 19; Dec. 222, 18.

References	Claim(s) Challenged
Hodges and Butt	1, 3, 7, 12, and 15
Hodges, Butt, and Ször	5
Hodges, Butt, and Levergood	8–11 and 14
Hodges, Butt, and Freund	4, 5
Hodges, Butt, and Kephart	2

E. Related Proceedings

The parties assert that the '196 patent is the subject of the following district-court proceedings: (1) *CAP Co. Ltd. v. McAfee, Inc.*, No. 3:14-cv-05068-JD (N.D. Cal.); (2) *CAP Co. Ltd. v. Microsoft Corp.*, No. 2:14-cv-01899 (W.D. Wash.); and (3) *CAP Co., Ltd. v. Symantec Corp.*, No. 3:14-cv-05071-JD (N.D. Cal.). Pet. 1855, 1–2; Paper 6, 1.

II. ANALYSIS

A. Claim Construction

The Board construes claims of an unexpired patent using the broadest reasonable interpretation in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of the broadest reasonable interpretation standard); Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012).

In the Institution Decisions, we made certain preliminary constructions. *See, e.g.*, Dec. 1855, 7–11. We consider the claim-construction issues anew in light of the full record developed during the trials. We note that our reconsidered constructions are consistent with the preliminary constructions.

1. Preambles

The preambles of challenged independent claims 1, 8, and 12 recite a method or system "for blocking *in real time* harmful information *in a file to be executed*" (emphases added). The preamble of challenged independent claim 10 similarly recites a method "for blocking *in real time* harmful information *in a file to be executed in real time*" (emphases added). As noted *supra*, the emphasized portions of these preambles were added by amendment during prosecution of the '552 patent in response to a rejection over Chen.

The parties take opposing positions on whether the preambles are limiting. Patent Owner contends that the preambles are limiting and that the

"in real time" recitation applies to each step recited in the claims, characterized by the parties as the "connecting," "transmitting," and "blocking" steps, despite somewhat different language among the challenged independent claims. PO Resp. 1855, 28–35. Conversely, Petitioner contends that the preambles are not entitled to patentable weight because, for each independent claim, "[t]he body of each claim sets forth all the limitations of the claimed invention," and because "[i]n view of the entire claim, the preamble merely states a purpose for the claimed method." Pet. 1855, 10, 11. According to Petitioner, even if the preambles *are* limiting, they require only that the "blocking" step be performed "in real time," and do not impose that requirement on the "connecting" and "transmitting" steps. Reply 1855, 8–9. These different views of the limiting scope of the preambles are fundamental to how the inventions are understood by the parties. PO Resp. 1855, 32 ("Construing the claim as requiring all the steps occur in real time results in a fundamentally different system."); Reply 1855, 9 ("[Patent Owner] is right" in that characterization).

"Generally, . . . the preamble does not limit the claims." *DeGeorge v. Bernier*, 768 F.2d 1318, 1322 n.3 (Fed. Cir. 1985). In particular, "it is assumed that the preamble language is duplicative of the language found in the body of the claims or merely provides context for the claims, absent any indication to the contrary in the claims, the specification or the prosecution history." *Symantec Corp. v. Comput. Assocs. Int'l, Inc.*, 522 F.3d 1279, 1289 (Fed. Cir. 2008).

Petitioner contends that "[i]n view of the entire claim, the preamble merely states a purpose for the claimed method," noting, in particular, that

the terms "block[] in real time," "harmful information," and "file to be executed" appear explicitly in element (c) of claim 1, which recites specifically *how* the harmful information blocking code module performs the function of "blocking in real time harmful information in a file to be executed." Pet. 1855, 11. Petitioner makes similar observations for independent claims 8, 10, and 12 to support its position. *Id.* at 11–12.

Patent Owner advances several arguments to support its contrary position. First, Patent Owner contends that "the preamble amendments were clearly added to distinguish Chen" and that "the mere fact that the preamble was amended in response to a rejection based on Chen is strong evidence that the patentee believed it clarified what 'the inventor[] actually invented and intended to encompass by the claim.'" PO Resp. 1855, 32 (quoting *Corning Glass Works v. Sumitomo Electric U.S.A., Inc.* 868 F.2d 1251, 1257 (Fed. Cir. 1989) (alteration by Patent Owner)). But the context in which the amendments were made during prosecution belies Patent Owner's position that they meant to apply the "in real time" recitation to all steps recited in the body of the claim. During prosecution of the '552 patent, the Examiner found that Chen taught automatic downloading, installation, and execution of an antivirus program, thereby anticipating some of the pending claims and rendering others obvious. Ex. 2002, 107–109. To overcome that rejection, the Applicant simultaneously amended the preamble and added the specific requirements for the "blocking" step as substeps recited in step (c) of claim 1, with similar amendments to the other independent claims. *Id.* at 91–96.

The Applicant distinguished Chen from the amended claims on three grounds: (1) Chen teaches scanning all files on the computer rather than a

particular "file to be executed," *id.* at 98; (2) Chen does not abort execution of harmful but untreatable files, *id.* at 99; and (3) Chen does not describe "inspecting file input/output (I/O) on the client system by hooking up file I/O routines, or that the subset of files would be the files that are currently being executed," *id.* at 101. We agree with Petitioner that "[n]one of those distinctions suggested that the claims were being amended to require the **connection** and **transmission** steps to occur in real-time, as each file was to be executed." Reply 1855, 7.

We further agree with Petitioner that Patent Owner's implication that this prosecution history distinguished Chen through the use of "tailored vaccines" to treat specific files is not supported by the remarks made by the Applicant. *See id*. (citing PO Resp. 1855, 29). The Specification of the '196 patent further makes clear that the web server transmits the blocking module in response to a *connection request*, not in response to a specific detected threat. *See* Ex. 1001, abst. (blocking module transmitted after connection request), col. 2, ll. 29–35 (invention "block[s] harmful information online [using blocking module that is] automatically transmitted and installed in the client system upon accessing to the web server"), Fig. 2A (steps 220–250), Fig. 2B (steps 230–255). Patent Owner's implication also is inconsistent with the Specification's description of detecting harmful information by the blocking module only after the client receives it. *See id*., col. 5, ll. 40–43 ("When the transfer of the [blocking module] is completed, the [blocking module] is automatically executed on the client 130 (step 260) and blocks in real time harmful information . . . ."). Furthermore, a contrary position was taken during prosecution of one of the Korean applications to which the '196

patent claims priority. Ex. 2004, 26 (arguing that the invention "does not provide specifically tailored vaccine for vaccinating viruses existing inside each client" but instead "provides the same real time [blocking module] to all the clients").[5]

Second, Patent Owner contends that "the body of the claims do not define a 'structurally complete invention' and the preamble does not only [] 'state a purpose or intended use for the invention.'" PO Resp. 1855, 32. But Patent Owner does not explain why a requirement that only the "blocking" step be performed "in real time" (as explicitly recited in the "blocking" step itself) results in a structurally incomplete method. *Id.* at 33.

We have reviewed the testimony of Patent Owner's witness, David Bernstein, who similarly expresses the opinion that "one skilled in the art would not view the body of the claims as defining a 'structurally complete invention' (certainly not the one described in the Specification) and would view the preamble as describing more [than] 'stating a purpose or intended

---

[5] Patent Owner makes the following assertion as part of its argument:

> The patentee also relied directly on the changed language in the preamble to distinguish Chen, quoting the amended preamble with a simple change in syntax: "In contrast to Chen, the presently claimed invention **blocks harmful information in a file to be executed in real time on a computer network**."

PO Resp. 1855, 29 (citing Ex. 1003, 17 (corresponding to Ex. 2002, 101)). In making this assertion, Patent Owner fails to make clear that it has modified the quotation drawn from the prosecution history by using boldface to change the original emphasis. The original argument made by the Applicant is: "In contrast to Chen, the presently claimed invention blocks harmful information in a file <u>to be executed</u> in real time on a computer network." Ex. 1003, 17; Ex. 2002, 101.

use for the invention.'" Ex. 2006 ¶ 124. Mr. Bernstein opines that, without giving weight to the preamble to require that all of the "connecting," "transmitting," and "blocking" steps occur "in real time," "the ['196] patent would not accomplish its fundamental objectives, statements in the specification regarding what the present invention consists of would not make sense, and portions of the file history [distinguishing] from Chen would not make sense." *Id.* But in expressing this opinion, Mr. Bernstein cites to no specific portions of the Specification or file history and makes broad conclusory statements.

Petitioner's expert, Atul Prakash, Ph.D, specifically "disagree[s] with Mr. Bernstein's position that the preamble is limiting and that the ['196] patent purportedly disclosed 'real time download of only the code necessary to block a single file to be executed.'" Ex. 1034 ¶ 108. Dr. Prakash testifies that "[t]his position of Mr. Bernstein also requires functionality in the steps of the methods that is not disclosed (implicitly or explicitly) in the specification." *Id.* at ¶ 110. Dr. Prakash explains that "[f]or Mr. Bernstein's theory to hold, a harmful information blocking code module would not be downloaded by '**only** online connecting to the harmful information management server' as the specification states, [Ex. 1001] at 9:20-25, but in response to a specific request that contains information about the single file to be executed." *Id.* (emphasis by Dr. Prakash). In addition, Dr. Prakash observes that the '196 patent lacks "a disclosure that file or threat information is sent in the request (and not just in the final notification step when a file cannot be treated)," as would be expected to support Mr. Bernstein's theory. *Id.* at ¶ 111.

We have considered the opinions of both experts, and give greater weight to the opinion of Dr. Prakash. *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"); *Qualtrics, LLC v. OpinionLab, Inc.*, 2017 WL 562460 at *5 (Fed. Cir. 2017) ("To the extent that the experts disagreed with each other . . . the Board chose to credit the testimony of Dr. Shamos over the testimony of Mr. Chisholm. . . . We discern no reversible error in that choice."). In doing so, we recognize that the following disclosure appears in the Specification of the '196 patent:

> In other words, the present embodiment provides the function of automatically providing the harmful information management server 110 with information on harmful information detected in the client 130. Accordingly, the harmful information management server 110 is allowed to acquire statistical data on harmful information, and *can thus instantaneously counteract the occurrence of an unidentified computer virus*, for example, by developing an effective antivirus program. In this manner, the harmful information management server 110 analyzes the unidentified harmful information from the client 130 to develop a proper treatment program, and provides an appropriate security service for blocking harmful information from attacking the client 130, with the latest version of the harmful information blocking code module. Therefore, []the present invention can prevent user computers from operating in an open network environment from damage caused by various harmful information.

Ex. 1001, col. 8, ll. 27–44 (emphasis added); *see* PO Resp. 1855, 10–12. Although this passage refers to "instantaneously counteract[ing]" the occurrence of a virus, that reference must be understood in the full context of the record, which includes the Applicant's disavowal during prosecution

of the priority Korean application of generating "specifically tailored vaccine for vaccinating viruses existing inside each client." Ex. 2004, 26; *see supra* at 12–13. Within this full context, the "instantaneous" action is understood as notification to the server that harmful information has been detected. *See* Reply 1855, 15. As Dr. Prakash testifies, the "appropriate reading of the phrase is that once a harmful but untreatable file has been identified on a client computer, a report is sent to the web server instantaneously, allowing the web server to start collecting information about the harmful file for systematic analysis and to start developing a treatment." Ex. 1034 ¶ 39.

Third, Patent Owner also contends that "Mr. Bernstein explains [that] the download of the harmful information blocking code module in real-time is an additional structure or steps underscored as important by the specification, which repeatedly describes the invention as actively blocking online threats, including ones never previously identified." PO Resp. 1855, 33. But neither Patent Owner nor Mr. Bernstein provides any citation to, or otherwise directs us to, where such "repeated" descriptions can be found in the Specification. Indeed, based on our review of the '196 patent Specification, we agree with Petitioner's characterization at the oral hearing that "the ['196] patent is clear in the intrinsic evidence, every figure, every explanation is that only the blocking is in real time. It doesn't say -- nowhere does it say that you connect in real time, and nowhere does it say that the transmission step is in real time." Tr. 13:4–9.

For example, Figure 2A, reproduced *supra*, conspicuously uses the phrase "in real time" only in block 270 ("blocking" step), but not in blocks

240 ("connecting" step) or block 250 ("transmitting" step); Figure 2B is similar. *See* Tr. 24:3–22. In addition, the '196 patent includes the following disclosure:

> For this case, the connection between the client 130 and the harmful information management server 110 is accomplished by a HyperText Transfer Protocol formatted request (HTTP request), and the transferring of the harmful information blocking code module from the harmful information management server 110 to the client 130 is performed by a HTTP response. In general, the HTTP request is carried out by typing the Universal Resource Locator (URL) of the harmful information management server 110 or clicking a hyperlink associated with the URL on the web browser.

Ex. 1001, col. 5, ll. 3–12. This disclosure of manual triggers is inconsistent with Patent Owner's position that a new blocking module is transmitted every time a file is to be executed, i.e. that the "transmitting" step must be performed "in real time." *See* Reply 1855, 12; Tr. 24:23–25:17. "A claim interpretation that excludes a preferred embodiment from the scope of the claim 'is rarely, if ever, correct.'" *Globetrotter Software, Inc. v. Elan Computer Group, Inc.*, 362 F.3d 1367, 1381 (Fed. Cir. 2004) (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)).

Fourth, Patent Owner contends that "finding the preamble non-limiting results in a construction that violates the plain and ordinary meaning of the claim" because "[t]he phrase 'blocking harmful information in a file about to be executed in real time by completing the steps of the method' clearly means **all** of the steps." PO Resp. 1855, 33. We explored this argument at length at the oral hearing. Tr. 11:5–24:2. Ultimately, we are

not persuaded by this argument in the context of countervailing indications in the Specification and file history, which do not convincingly evidence an intention by the Applicant for anything other than the "blocking" step to be performed in real time. Rather, the preamble renders the overall claim internally consistent by providing an antecedent for the "file to be executed" and merely reiterates what is already recited in the claim's body, namely that blocking harmful information "in a file to be executed" occurs "in real time."

For these reasons, we do not give patentable weight to the preambles. The only compelling construction of the preamble would be duplicative of limitations repeated explicitly in the bodies of the claims.

2. "harmful information"

Each of independent claims 1, 8, 10, and 12 recites blocking "harmful information including computer viruses." According to the Specification of the '196 patent, "[t]he term 'harmful information' collectively refers to an undesirable object or action that adversely [a]ffects computer systems and/or computer networks, including computer viruses, undesirable lascivious web sites on the Internet, and the act of illegally extracting personal information." Ex. 1001, col. 4, ll. 51–56. Petitioner proposes that we adopt the Specification's definition. Pet. 1855, 12–13. Patent Owner does not proffer a construction of the term.

For purposes of this Decision, we adopt the Specification's definition. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1316 (Fed. Cir. 2005) (citing *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002))

("[T]he specification may reveal a special definition given to a claim term by the patentee that differs from the meaning it would otherwise possess. In such cases, the inventor's lexicography governs.").

3. "harmful information blocking code module"

Each of independent claims 1, 8, 10, and 12 recites transmission of a "harmful information blocking code module" by a web server to a client computer or client system and running the "harmful information blocking code module" on the client computer or client system to "block in real time harmful information including computer viruses." Petitioner proposes that "harmful information blocking code module" be construed as "an executable program that blocks harmful information." Pet. 1855, 17–19. Patent Owner proposes that the term be construed as "code that is provided by a web server and is used to block potential harmful information in real time." PO Resp. 1855, 22–27.

We agree with Petitioner that Patent Owner's proposed construction seeks to add "additional limitations [that] are unwarranted." Reply 1855, 11. Specifically, the independent claims already recite that the "harmful information blocking code module" is transmitted by a "web server," and recite that the module is run or executed on the client computer or client system "to block in real time harmful information including computer viruses." The inclusion of "provided by a web server" and "in real time" in Patent Owner's proposed construction is, thus, redundant with other limitations recited explicitly in the claims.

In their arguments, the parties do not explicitly address Patent Owner's proposal to expand the scope of the "harmful information blocking code module" to block "potential" harmful information. *See* PO Resp. 1855, 22–27; Reply 1855, 11–15. Because Patent Owner does not articulate a clear reason for such an expansion, and because we do not independently discern a basis for such an expansion, we decline to adopt one.

The parties also differ in their proposed constructions whether the "harmful information blocking code module" should be construed as "a program" or as "code." Although we see insignificant impact emanating from this distinction, Petitioner does not explain why the module should be construed more narrowly as a "program," and we accordingly adopt the slightly broader phrasing proposed by Patent Owner.

In light of these considerations, we construe "harmful information blocking code module" as "code that blocks harmful information."

4. "block in real time harmful information"

Each of independent claims 1, 8, 10, and 12 recites that the harmful information blocking code module is executed to "block in real time harmful information including computer viruses." Petitioner proposes that "block in real time harmful information" means "prevent execution of harmful information in real time." Pet. 1855, 13–14. Patent Owner does not proffer a proposed construction of the phrase.

Petitioner contends that its proposed construction "reflects consistent usage of the phrase in the '196 Patent, which describes several ways in which harmful information in file I/O or network packet I/O may be blocked

in real time," and supports its contention with testimony by Dr. Prakash that the proposed construction "is used in the present sense in that harmful information is blocked at the 'present time,' and not some unknown future time or even a scheduled future time." *Id.* at 13; Ex. 1008 ¶ 127. We agree with Petitioner's reasoning that its proposed construction comports with the broadest reasonable interpretation and, therefore, adopt it herein.

5. "file to be executed"

Each of independent claims 1, 8, 10, and 12 recites blocking harmful information in a "file to be executed." Petitioner proposes that "file to be executed" means "file about to be executed." Pet. 1855, 15–17. Patent Owner does not propose a construction for the phrase. We agree with Petitioner that, in the context of the '196 patent, the phrase does not generically cover any executable file and "suggests that execution of the file is imminent, absent intervening action." *Id.* at 15 (citing Ex. 1008 ¶¶ 129–130).

Accordingly, we adopt Petitioner's proposed construction herein.

6. "according to information provided from a second web server"

Independent claim 8 recites "the client system connecting to the first web server over the computer network, according to information provided from the second web server to the client system." Independent claim 10 similarly recites "the connection request is issued by the client system according to information provided from a second web server after the client system is connected to the second web server." Patent Owner proposes that

the phrase "according to information provided from a second web server" means "information provided from a second web server about the file to be executed." PO Resp. 1855, 35–38.

Patent Owner argues that "[o]ne skilled in the art would understand that the connection request contains information regarding the threat," and contends that "[t]his is supported by the Specification." *Id.* at 36. But the disclosure relied on by Patent Owner is a grammatically incomplete sentence that is difficult to parse: "Since the second web server 120 provide hyperlink information for use in accessing the harmful information management server 10 as well as information relating to online services to the client 130 (step 235)." Ex. 1001, col. 6, ll. 6–9. Patent Owner asserts that "[i]n this case, the referenced online services are those provided by the second web server – that is the files and network packets that might contain harmful information." PO Resp. 1855, 37. But Patent Owner provides insufficient reasoning or evidence to support this inference.

We agree instead with Petitioner that "[t]he patent's only examples of information provided from a second web server are 'hyperlink information for use in accessing that harmful information management server 10 as well as information relating to online services to the client 130' and 'hyperlink information' that is preferably 'link information that directly enables the client 130 to receive the [blocking module] from the harmful information management server through a separate window.'" Reply 16 (quoting Ex. 1001, col. 6, ll. 6–15) (alterations by Petitioner). As Petitioner asserts, Patent Owner's "construction would exclude these embodiments because in neither case is the information 'about the file to be executed.'" *Id*. at 16.

The claim language itself is also at odds with the additional limitation that Patent Owner seeks to import through its proposed claim construction. In both claims 8 and 10, the information about the file to be executed is learned only after the client connects to the first web server, a blocking module is transmitted to the client, and the blocking module runs on the client and inspects the file by hooking file I/O. *See* Ex. 1001, col. 10, ll. 51–52 ("*once* the transmission of the harmful information blocking code module is complete" (emphasis added)), col. 11, ll. 14–15 ("*once* the first web server transmits a harmful information blocking code module to the client system" (emphasis added)). *See Phillips* at 1314 ("the claims themselves provide substantial guidance as to the meaning of particular claim terms," and "the context of the surrounding words of the claim also must be considered in determining the ordinary and customary meaning of those terms") (quoting *Vitronics* at 1582).

We decline to construe "according to information provided from a second web server" to incorporate such an unrecited limitation, and find it unnecessary to construe the term further. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (holding that "only those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy").

7. Other terms

Petitioner proposes constructions for "automatically running," "automatically executed," and "by hooking up file I/O routines." Pet. 1855,

19–22. We do not find it necessary to construe these terms explicitly. *See Vivid Techs.* 200 F.3d at 803.

B. Obviousness

All of Petitioner's challenges are based on obviousness under 35 U.S.C. § 103(a). A patent claim is unpatentable under 35 U.S.C. § 103(a) 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 ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

C. Obviousness of Claims 1, 3, 7, 12, and 15 Over Hodges and Butt

Petitioner challenges claims 1, 3, 7, 12, and 15 as unpatentable under 35 U.S.C. § 103(a) over Hodges and Butt. Pet. 1855, 38–48, 57–60; Pet. 216, 48–59; Pet. 222, 60. Hodges "relates to a method and system for maintaining and updating antivirus applications in computers attached to a computer network." Ex. 1005, col. 1, ll. 9–11. Figure 4 of Hodges is reproduced below.

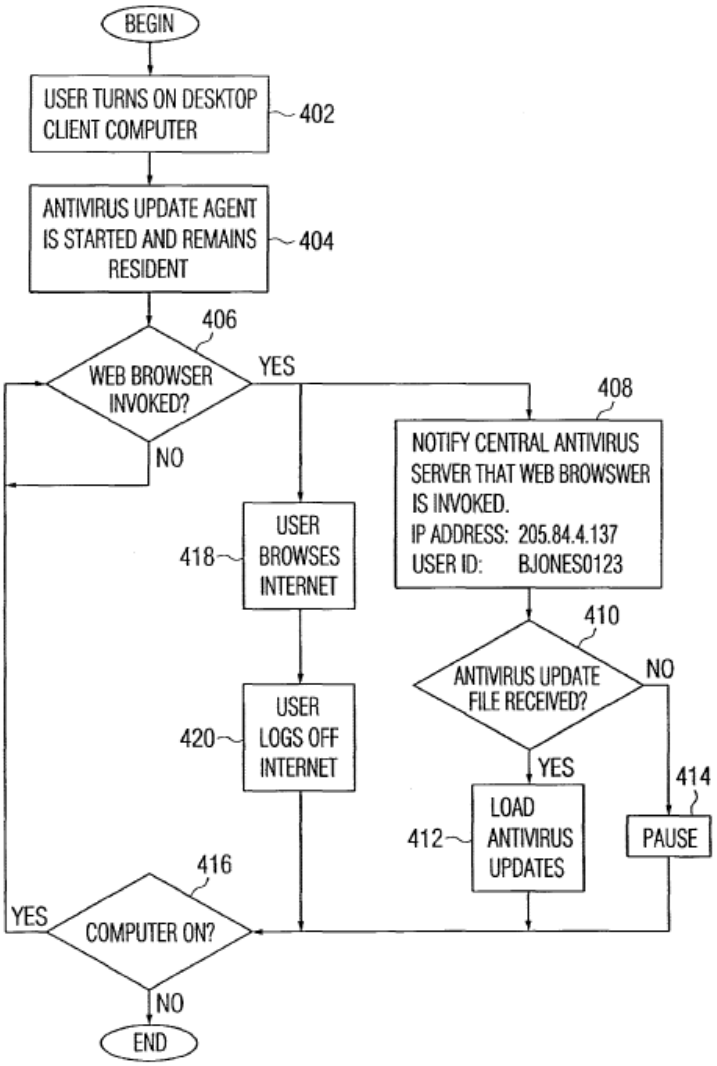

FIG. 4

Figure 4 shows steps taken by a client computer to maintain currency with a latest release of antivirus files stored at a central antivirus server. *Id.* at col. 7, ll. 9–10, col. 6, l. 64–col. 7, l. 1. When the client computer is turned on at step 402, antivirus application software is activated on the client computer, "usually automatically." *Id.* at col. 7, ll. 10–13. The antivirus application software scans for viruses on the client computer "by comparing all executable files, macro files, etc. against known virus signatures as

contained in a [virus-signature file]." *Id.* at col. 7, ll. 13–17. In one embodiment of Hodges, a desktop antivirus update agent is started at step 404, and remains resident in the client computer. *Id.* at col. 7, ll. 17–19.

When a web browser is invoked at step 406, the antivirus update agent transmits a sequence of information packets to the central antivirus server, including an IP address of the client computer and a unique user ID, enabling antivirus update files to be sent to the client computer by the server and loaded by the client computer. *Id.* at col. 7, ll. 20–43. Such loading "may be an automatic loading step, wherein the downloaded files automatically self-execute and insert the update file . . . into the appropriate directory of the client computer." *Id.* at col. 7, ll. 50–53. This virus-updating procedure may be carried out in the background, i.e., transparent to the user. *Id.* at col. 7, l. 62–col. 8, l. 5.

Butt discloses monitoring file input/output routines and a dynamic linked library ("DLL") to implement an interceptor function that scans files for viruses on access. Ex. 1006, col. 2, ll. 13–26. Of particular relevance to this Final Written Decision, Butt describes an interceptor function that uses file-system hooks to scan for viruses, taking remedial action if a virus is found, and returning control to the original program otherwise. *Id.* at col. 2, ll. 28–35.

Petitioner contends that each of the steps recited in independent claim 1, as well as corresponding structure recited in independent claim 12, is disclosed by Hodges, with the caveat that, to the extent Hodges does not disclose steps (c1)–(c3) of independent claim 1, such steps are disclosed by Butt. Pet. 1855, 38–48, 57–60.

With respect to step (a) of independent claim 1, which recites receiving a connection request from the client system over the computer network (the "connecting" step), Petitioner identifies Hodges's disclosure of a linked web server and client system, as well as Hodges's teaching that updated antivirus files could be retrieved from the web server after the web server received a connection request from the client system. *Id.* at 40–41 (citing Ex. 1005, abstract, col. 6, ll. 51–57, col. 4, l. 65–col. 5, l. 6 ("Each client computer intermittently notifies the central antivirus server that the client computer is actively coupled to the computer network. . . . [T]he central antivirus server transmits updated antivirus files to that client computer over the computer network.")). Petitioner supports its position with testimony by Dr. Prakash. Ex. 1008 ¶¶ 224–232. Petitioner sufficiently shows that the disclosure it identifies meets the claim limitation.

With respect to step (b) of independent claim 1, which recites that the web server transmits a harmful information blocking code module to the client system (the "transmitting" step), Petitioner draws a correspondence between the recited "harmful information blocking code module" and the antivirus software update pushed to the client computer, as disclosed by Hodges. *Id.* at 41–42. We agree with this identification in light of our construction of "harmful information blocking code module" *supra* because the antivirus software update is "code that blocks harmful information."

With respect to step (c) of independent claim 1, which recites the harmful information blocking code module automatically running on the client system to block in real time harmful information including computer viruses (the "blocking" step), Petitioner observes that "Hodges also

explained that real-time blocking of harmful information was known in the art, as '[c]ommon virus scanning software allows . . . on-access scanning of a file when that file is accessed by the operating system or an application.'" *Id.* at 43 (quoting Ex. 1005, col. 1, ll. 37–41) (alterations by Petitioner). We agree with Petitioner that the claim limitation is met by Hodges because "Hodges thus disclosed providing a client computer with updated antivirus programs, i.e., harmful information blocking code modules that automatically installed and executed to block in real time harmful information on a client computer." *Id.* (citing Ex. 1008 ¶¶ 252–254).

We also agree with Petitioner that the specific steps (c1)–(c3) of independent claim 1 are disclosed by Butt's interceptor function using file-system hooks to scan for viruses, a position that is not disputed by Patent Owner. *Id.* at 43–48.

Patent Owner raises counterarguments grounded in claim-construction positions that we reject for the reasons described above. First, Patent Owner contends that the preamble of independent claim 1 is limiting and that "the limitation requires that the real time blocking of harmful information be contemporaneous with the download of the harmful information blocking code module, which is neither taught nor suggested by *Hodges* and *Butt*." PO Resp. 1855, 52–53. Patent Owner repeats the argument in connection with step (c) of claim 1. *Id.* at 53–54. Because we disagree that the preamble is properly construed as limiting, and because we disagree that the proper claim construction requires such "contemporaneous" blocking and downloading, this argument is unpersuasive.

Second, Patent Owner contends that neither Hodges nor Butt teaches the web server transmitting a harmful information blocking code module to the client system, as recited in step (b) of claim 1, because "one skilled in the art would understand that the harmful information blocking code module is claimed as being transmitted in connection with a potential threat in a file to be executed." *Id.* at 53 (citing Ex. 2006 ¶¶ 100–113). As explained above, we disagree that the properly construed claim imposes such a requirement.

We also conclude that Petitioner articulates sufficient reasoning to combine the teachings of Hodges and Butt in the manner proposed. Petitioner contends that Hodges and Butt are in the same field of endeavor, namely protection of computers from harmful information, and that they address the same problem as the '196 patent by implementing remediation measures *before* such computers are damaged by the harmful information. *See* Pet. 1855, 31–33. Petitioner specifically observes that "Hodges taught virus detection by 'on-access scanning of a file when that file is accessed by the operating system or an application,'" and that "Butt taught a specific method of performing on-access scanning by hooking file I/O routines." *Id.* at 45 (citing Ex. 1005, col. 1, ll. 40–41). Petitioner accordingly reasons that "[b]ecause there were a finite number of predictable solutions for implementing on-access scanning, it would have been obvious to use Butt's methods to implement the on-access file I/O scanning suggested by Hodges," and supports that reasoning with testimony by Dr. Prakash. *Id.* at 45 (citing *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007); Ex. 1008 ¶¶ 175–185). We agree with Petitioner's reasoning, which Patent Owner does not contest in its Patent Owner Responses.

We have also considered Patent Owner's contention, made generically with respect to all of Petitioner's challenges, that "[s]econdary considerations support a finding of non-obviousness." PO Resp. 1855, 8. We agree with Petitioner that the evidence Patent Owner provides of such secondary considerations is "wholly inadequate" to support its position. *See* Reply 1855, 4. Patent Owner presents a short narrative contending that Petitioner introduced a product, the Global Threat Intelligence ("GTI") service, that "practice[d] the '196 Patent's claims," has been described as "revolutionary" and "unprecedented" in an article published eight years after the claimed invention, and has "maintained a position as a leader in Gartner's Endpoint Protection Platform Magic Quadrant report." PO Resp. 1855, 8–9.

These assertions, and the modest documentation provided to support them insufficiently support Patent Owner's positions. Although Petitioner concedes that "[a]t most, [Patent Owner] shows a connection request to a GTI server when McAfee antivirus products detect a potentially harmful file or network traffic," we agree with Petitioner that Patent Owner "has not shown that GTI practices the other limitations required by the claims, let alone that GTI's alleged commercial success directly resulted from the unique characteristics of the claimed invention." Reply 1855, 24–25. In particular, we agree with Petitioner that Patent Owner "has not shown that GTI inspects file I/O by hooking up file I/O routines or that it treats any harmful file, as required for all the challenged claims." *Id.* at 25. Accordingly, no presumption of the required nexus between the identified GTI product and the claimed invention attaches. *See WBIP, LLC v. Kohler*

Co., 829 F.3d 1317, 1329 (Fed. Cir. 2016) ("there is a presumption of nexus for objective considerations when the patentee shows that the asserted objective evidence is tied to a specific product and that product 'is the invention disclosed and claimed in the patent'") (citations and footnote omitted). Furthermore, even if Patent Owner were to establish that GTI is covered by the challenged claims, we would afford Patent Owner's proffered evidence of secondary considerations little weight because of the deficiencies in that evidence.

For example, in supporting its position that the GTI product enjoyed commercial success and industry praise, Patent Owner proffers a report (Ex. 2019) that provides no evidence of units sold or market share, and insufficiently attributes either commercial success or industry praise to the GTI product specifically, as opposed to Petitioner's products and services generally. *See Ex Parte Foodfresh Techs., LLC*, 2015 WL 411824 at *10 (PTAB Jan. 29, 2015) (invention's high ratings and availability at major retailers insufficient to show commercial success absent evidence of units sold and comparative data).

We conclude that Petitioner has demonstrated, by a preponderance of the evidence, that independent claim 1 is unpatentable under 35 U.S.C. § 103(a) over Hodges and Butt. Because independent claim 12 recites similar limitations in the context of a "system" rather than a "method," we also conclude that Petitioner has demonstrated, by a preponderance of the evidence, that claim 12 is unpatentable under 35 U.S.C. § 103(a) over Hodges and Butt.

Claim 3 depends from claim 1 and recites "requesting the client system user's approval for the execution of the step (c3)." Petitioner identifies disclosure in Butt that the "'user ***can also be queried*** as to whether to allow or deny access to an infected file," and that "'if the user chooses to deny access to the file, an open file failure is returned to the' application that attempted to access the file, thus aborting execution." Pet. 1855, 48 (citing Ex. 1006, col. 2, ll. 46–47 (alteration by Petitioner), col. 2, ll. 47–49). We are persuaded by Petitioner's argument, which is not addressed by Patent Owner independent of its arguments to underlying independent claim 1.

We conclude that Petitioner has demonstrated, by a preponderance of the evidence, that claim 3 is unpatentable under 35 U.S.C. § 103(a) over Hodges and Butt.

Claim 7 depends from claim 1 and recites that "the harmful information blocking code module executed in the step (c) continues to run on the client system even when the client system accesses another web server." Claim 15 depends from claim 12 and recites a similar limitation.

In addressing claim 7, Petitioner identifies disclosure in Hodges that an antivirus program was "run at computer startup, and also remain[ed] resident for scanning all files upon file access." Pet. 216, 48 (citing Ex. 1005, col. 2, ll. 9–21). Petitioner contends that a person of ordinary skill in the art "would understand this to mean that the antivirus program ran in the background for as long as the computer was on." *Id.* at 48–49 (citing IPR2016-00216, Ex. 1008 ¶ 401). Petitioner additionally identifies disclosure in Hodges for updating the software while a user browsed another web server, particularly as illustrated in Figure 4 of Hodges (reproduced

above). *Id.* at 49 (citing Ex. 1005, col. 7, ll. 17–19, col. 7, l. 64–col. 8, l. 5, col. 7, ll. 28–39). In particular, Figure 4 shows the central antivirus server providing the client system with update files at step 410, which the client update agent on the client system receives and loads at step 412, occurring in parallel with a user browsing the Internet at step 418. *Id.* at 49 (citing Ex. 1005, col. 7, ll. 40–45). "Hodges explained that the client system's activities, including browsing to different web servers, and 'operation of the client computer . . . as seen by the user [wa]s generally unaffected' by the antivirus software's operations, which included communication with the central anti-virus server to receive updated antivirus files." *Id.* at 49 (citing Ex. 1005, col. 7, l. 62–col. 8, l. 5, Fig. 4) (alterations by Petitioner). Petitioner makes substantially the same arguments in addressing claim 15. Pet. 222, 60, 49–50.

We are persuaded by Petitioner's arguments, which are not addressed by Patent Owner independent of its arguments to underlying independent claims 1 and 12. *See* PO Resp. 216, 41–44; PO Resp. 222, 60.

We conclude that Petitioner has demonstrated, by a preponderance of the evidence, that claims 7 and 15 are unpatentable under 35 U.S.C. § 103(a) over Hodges and Butt.

D. Obviousness of Claim 5 Over Hodges, Butt, and Ször

Claim 5 depends from claim 1 and recites that "the harmful information blocking code module executed in the step (c) checks whether current processes running on the client system are harmful or not."

Petitioner challenges claim 5 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Ször. Pet. 1855, 48–50.

Addressing techniques that viruses use to remain in memory, Ször discloses a memory scanner that works closely with an on-access virus scanner to prevent viruses from replicating when the memory scanner attempts to terminate a detected process. Ex. 1007, 1, 11. Petitioner identifies this memory scanner as performing the function recited in dependent claim 5, noting the disclosed interaction of the memory scanner with an on-access virus scanner, and supporting its argument with testimony by Dr. Prakash. Pet. 1855, 49–50 (citing Ex. 1007, 10; Ex. 1008 ¶¶ 270–290). Petitioner provides further reasoning to support its contention that "[c]ombining Hodges, Butt, and Ször was obvious." *See id.* at 50. In particular, Petitioner asserts that "Ször specifically recommended that memory scanning techniques be combined with on-access scanners like those taught in Hodges and Butt because an on-access scanner alone 'c[ould]not stop the virus replicating on the system since the active virus [*i.e.*, a process] c[ould] infect the [file] disinfected [by the on-access scanner] again.'" *Id.* (citing Ex. 1007, 11; Ex. 1008 ¶¶ 191–195, 292–295; *Perfect Web Techs., Inc. v. Info USA, Inc.*, 587 F.3d 1324, 1329 (Fed. Cir. 2009)) (alterations by Petitioner).

We agree with Petitioner that Ször teaches the limitation of dependent claim 5 for the reasons presented in the Petition, and Petitioner articulates sufficient reason with rational underpinnings to combine that teaching with Hodges and Butt. Petitioner's arguments are not addressed by Patent Owner

independent of its arguments to underlying independent claim 1. *See* PO Resp. 1855, 51–52.

We conclude that Petitioner has demonstrated, by a preponderance of the evidence, that claim 5 is unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Ször.

E. Obviousness of Claims 8–11 and 14 Over Hodges, Butt, and Levergood

Petitioner challenges claims 8–11 and 14 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Levergood. Pet. 1855, 50–57; Pet. 222, 35–53, 58–59. Levergood describes architectures for "processing service requests from a client to a server through a network." Ex. 1012, col. 3, ll. 7–8. In one implementation, a client computer interfaces with a single directory server to direct the client to different merchant web servers by having a user access a form page provided by the directory web server to prompt for merchant identifiers. *Id.* at col. 9, ll. 21–25, col. 9, ll. 33–40. The client automatically connects to the merchant web server after the directory web server receives the identifiers and transmits a REDIRECT response to the client browser. *Id.* at col. 9, l. 41–col. 10, l. 9.

Independent claims 8 and 10 are generally similar to independent claim 1, but correspond to the embodiment of Figure 2B of the '196 patent using a second server that provides information in accessing a first server. *See* Ex. 1001, col. 6, ll. 1–28. Petitioner repeats much of its analysis for claim 1, but contends that "[t]o the extent Hodges did not disclose explicitly that the client system connected to the push administration server 810 ('first

web server') according to information provided from the central antivirus server 808 ('second web server'), and were it not obvious, Levergood disclosed this claim element." Pet. 1855, 51–52.

Specifically, with respect to step (a) of independent claim 8, which recites a client system connecting to a "second" web server over a computer network through which the client system, second web server, and a "first" web server are linked, Petitioner observes that "Hodges disclosed a push administration system 810 (first web server) separate from the central antivirus server 808 (second web server) for providing updates to a client system 802." Pet. 1855, 51 (citing Ex. 1005, col. 10, ll. 20–23). With this structure, Petitioner sufficiently shows that the disclosure it identifies meets the claim limitation for reasons similar to those discussed *supra* in connection with independent claim 1.

With respect to step (b) of independent claim 8, which recites that the client system connects to the first web server "according to information provided from the second web server to the client system," Petitioner relies on Levergood's disclosure of transmitting a REDIRECT response to connect to a merchant web server. *Id.* at 52–53. Petitioner correctly notes that Levergood teaches implementing this functionality by receiving an identifier NUMBER from the client so that a directory server could provide the REDIRECT response with the target URL for the merchant server. *Id.* at 52. "Levergood thus disclosed the client system connecting to a first web server (Merchant Server) over the computer network, according to information provided from the second web server (Directory Server) to the client system." *Id.* at 53 (citing Ex. 1012, col. 9, l. 21–col. 10, l. 9).

Petitioner sufficiently shows that the claim limitation is met. Patent Owner's argument that Levergood fails to disclose the limitation because "the limitation requires that the client system connects to the first web server after receiving information *about the file to be executed* from the second web server" is unpersuasive because it attempts to incorporate unrecited limitations. PO Resp. 1855, 55 (emphasis added).

We are persuaded also that Petitioner explains sufficiently why one of ordinary skill in the art would have combined the multiserver architecture taught by Levergood with Hodges and Butt. Petitioner notes that "Hodges specifically contemplated a multiserver architecture over the Internet," and reasons that "[b]ecause there were a finite number of two-server architectures for delivering products or services over the Internet, it would have been obvious to try Levergood's architecture to implement Hodges's delivery system over the Internet." Pet. 1855, 54 (citing Ex. 1005, Fig. 8; Ex. 1012, col. 3, ll. 7–11; Ex. 1008 ¶¶ 206–213; *KSR*, 550 U.S. at 421). Petitioner supports its contention with testimony by Dr. Prakash. Ex. 1008 ¶¶ 206–213. As Petitioner reasons, "[t]he combination of delivering antivirus program updates for automatic installation (Hodges), monitoring of file access operations in real time (Butt), . . . and redirecting a client computer to a web server where it could obtain antivirus program updates (Levergood) did 'no more than one would expect from such an arrangement.'" *Id*. at 36 (citing *KSR*, 550 U.S. at 417).

Patent Owner responds to these arguments by characterizing the fields of invention to distinguish Levergood from Hodges and Butt, but makes only a conclusory statement that does not effectively rebut Petitioner's

argument: "one skilled in the art would have no motivation to combine *Levergood*, in the field of e-commerce authentication services, with *Hodges* and *Butt*, in the field of push technology updates and on-access scanning, respectively." PO Resp. 1855, 55–56 (citing Ex. 2006 ¶¶ 192–195[6]). The distinction Patent Owner draws does not diminish the relevance of Levergood for Petitioner's limited purpose because Levergood is at least "reasonably pertinent to the particular problem with which the inventor [was] involved," namely blocking harmful information, including computer viruses, over a computer network. *In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004).

The remaining elements of independent claim 8 are similar to elements of independent claim 1: (1) element (c) of claim 8 is substantially identical to element (b) of claim 1, except for the recitation of "first web server" instead of "web server"; (2) element (d) of claim 8 is identical to element (c) of claim 1; and (3) elements (d1)–(d3) of claim 8 are identical to elements (c1)–(c3) of claim 1, except for their labeling. Petitioner makes a sufficient showing for these elements of independent claim 8 for the same reasons discussed *supra* in connection with their counterparts recited in independent claim 1.

Independent claim 10 also recites limitations that have counterparts in claim 8, with the two claims differing primarily in that element (b) of claim 10 combines separate aspects of elements (a) and (b) of claim 8. Petitioner

[6] There appears to be an error in Patent Owner's citation to Mr. Bernstein's Declaration on page 56 of its Response in IPR2016-01855. The citation in the main text reflects what we understand the correct citation to be.

thus carries its burden with respect to claim 10 for the same reasons discussed in connection with claim 8.

Claim 14 depends from claim 12 and recites a second web server linked to the client computer such that "the second web server provides the client computer with hyperlink information used to access to [*sic*] the first web server." As such, it is a two-server system claim that corresponds to the two-server method claims 8 and 10. Claim 14 differs from those other claims in its narrower recitation of "hyperlink information" used to access the first web server, but such hyperlink information is within the specific scope of Levergood's teachings: "[e]ach Web page may contain . . . connections, known as 'hypertext links' ('links'), to other pages within the same server or even on other computers within the Internet." Ex. 1012, col. 2, ll. 16–20; *see id.* at col. 2, ll. 22–25 ("Each link is directed to a web page by using a special name called a URL (Uniform Resource Locator). URLs enable a Web browser to go directly to any file held on any Web server."); Pet. 222, 58–59.

We conclude that Petitioner has demonstrated, by a preponderance of the evidence, that claims 8, 10, and 14 are unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Levergood.

Claims 9 and 11 depend respectively from independent claims 8 and 10, and recite that "the harmful information blocking code module . . . continues to run on the client system even when the client system accesses another web server." In addressing this limitation, Petitioner identifies the following teachings in Hodges. Pet. 222, 49–50. First, Hodges discloses:

> The program SCAN.EXE is adapted to be used for any of the following types of virus scanning: virus scanning of system boot-sectors at startup, on-demand virus scanning at the explicit request of the user, and on-access virus scanning of a file when that file is accessed by the operating system or an application.

Ex. 1005, col. 2, ll. 13–18. Petitioner contends that a "person of ordinary skill in the art would understand this to mean that the antivirus program ran in the background for as long as the computer was on; otherwise the virus scanner would not be effective," and supports that contention with testimony by Dr. Prakash. Pet. 222, 49 (citing IPR2016-00222, Ex. 1008 ¶¶ 399–402). Petitioner further contends that "Hodges also disclosed that antivirus software could be updated while the user was accessing other websites," pointing to Figure 4, reproduced above. *Id.* at 50. "As shown in Hodges'[s] Figure 4, Hodges taught to update the software while the user browsed the Internet to other web servers." *Id.* We are persuaded by Petitioner's argument, which is not addressed by Patent Owner independent of its arguments to underlying independent claims 8 and 10.

We conclude that Petitioner has demonstrated, by a preponderance of the evidence, that claims 9 and 11 are unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Levergood.

F. Obviousness of Claims 4 and 5 Over Hodges, Butt, and Freund

Petitioner challenges claims 4 and 5 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Freund. Pet. 1877, 48–59. Claim 4 depends from claim 1 and recites additional steps (c4)–(c6) for inspecting

network I/O packets for harmful information, and blocking a communication port assigned for the packet I/O if any packet is determined to be harmful. As previously noted, claim 5 depends from claim 1 and recites checking "whether current processes running on the client system are harmful or not."

Freund relates to "system[s] and methods for regulating access and maintaining security of individual computer systems and local area networks (LANs) connected to larger open networks (Wide Area Networks or WANs), including the Internet." IPR2015-01877, Ex. 1007, col. 1, ll. 26–30. In particular, Freund discloses a client-based access-monitoring system with one or more client computers connected to a centralized enforcement supervisor that maintains a database of access rules, such as a list of URLs that an application could, or could not, access. *Id.* at col. 12, ll. 45–48, col. 13, ll. 2–13, col. 14, ll. 52–59, Fig. 3A. A copy of the access rules is maintained at the client computer, enabling a filter application to monitor, log, and filter processes, network communications, and file input/output. *Id.* at col. 13, ll. 23–33. As various client applications submit requests to a communications driver, a data-acquisition module "can intercept the communications for determining whether the request is permitted under the rules." *Id.* at col. 15, ll. 26–30. When a particular client application violates an access rule, the system takes remedial action, "including logging an exception log entry and, depending on the rules [for] the TCP/IP activity, the communication is either terminated, redirected, modified, or continued." *Id.* at col. 13, ll. 51–55. Notably, Freund discloses that "[t]he system should preferably be capable of filtering incoming data, including binary files, for detecting viruses and Trojan Horse programs." *Id.* at col. 9, ll. 14–16.

Petitioner contends that these and other processes described by Freund disclose the limitations of dependent claim 4 because they inspect network packet input/output on the client system, determine whether inspected packets are harmful or not, and block a communications port assigned for the packet input/output if a packet is determined to be harmful. Pet. 1877, 49–56. Petitioner further contends that "[i]t was obvious to combine Freund's network packet I/O inspection with on-access file scanning as taught by Butt and Hodges," because "Freund specifically combined network packet I/O scanning with on-access scanners like those taught in Hodges and Butt." *Id.* at 52 (citing IPR2015-01877, Ex. 1007, col. 13, ll. 57–65).

Patent Owner responds to these arguments with the brief contention that "Freund's remedial actions include dropping packets, but not blocking communication ports." PO Resp. 1877, 54 (citing Ex. 2006 ¶ 206[7]). Mr. Bernstein repeats the assertion without providing any additional details why Freund is not properly understood to disclose blocking communication ports. Ex. 2006 ¶ 226. Indeed, Petitioner identifies specific examples from Freund of blocking communication ports. *See* Reply 1877, 22–23. For example, Petitioner observes that "Freund disclosed blocking a harmful internet address, which is what the ['196] patent described as 'blocking a communication port.'" *Id.* at 23 (citing Ex. 1001, col. 7, ll. 26–38 (describing "prevent[ing] the access of undesirable lascivious web sites" as

[7] The citation to paragraph 206 of Mr. Bernstein's Declaration appears incorrect because it addresses Ször, not Freund. We presume that Patent Owner intended to cite to paragraph 226 of the Declaration.

blocking the harmful network packet I/O)). Petitioner further observes that Freund "also disclosed that '[s]ince the system of the present invention monitor[ed] the message traffic at the level of individual messages, the system [wa]s able to selectively block access, as dictated by the configurable rules.'" *Id.* (quoting IPR2015-01877, Ex. 1007, col. 19, ll. 57–60) (alterations by Petitioner). In addition, Petitioner notes Freund's teaching "to block harmful packets by failing the corresponding WinSock 'recv()' call, which also blocked the communication port assigned for such packets." *Id.* (citing IPR2016-01877, Ex. 1007, Fig. 12C, step 1222; Ex. 1034 ¶¶ 189–193).

After considering these identifications, we are persuaded that Petitioner adequately shows that the limitation is disclosed by Freund. Petitioner also provides sufficient reasoning for combining the identified teaching of Freund with Hodges and Butt. We are not persuaded by Patent Owner's contrary contention because we disagree that Petitioner has made an insufficient showing regarding the teachings of the combination of Hodges and Butt. *See* PO Resp. 1877, 7 (arguing that Freund is cited for "teachings that do not impact the essential features of the claimed system that are not taught *by Hodges* and *Butt*").

We conclude that Petitioner has demonstrated, by a preponderance of the evidence, that claim 4 is unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Freund.

With respect to claim 5, Petitioner contends that "Freund disclose[s] checking ongoing processes for harmfulness by checking their corresponding file activities." Pet. 1877, 57. Specifically, Freund discloses

"intercepting certain file activities and assigning them to the originating process" to "track files being created and changed by any process." IPR2015-01877, Ex. 1007, col. 4, ll. 64–66. Under certain conditions, intercepted file activities are analyzed to "allow[] the immediate application of internal or external virus checkers." *Id.* at col. 4, l. 67–col. 5, l. 5. We find this argument persuasive, and Patent Owner does not respond to this argument in its response.

We conclude that Petitioner has demonstrated, by a preponderance of the evidence, that claim 5 is unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Freund.

G. Obviousness of Claim 2 Over Hodges, Butt, and Kephart

Claim 2 depends from independent claim 1 and recites that "in the step (c3), if the file determined to be harmful in the step (c2) cannot be treated, the file is transmitted to the web server." Because this limitation is a conditional limitation of a method claim, it need not be found in the prior art if, under the broadest scenario, the method need not invoke the step. *Ex Parte Schulhauser*, Appeal No. 2013-007847, 2016 WL 6277792 (PTAB April 28, 2016) (precedential); *see Ex parte Katz*, 2011 WL 514314, *4 (BPAI 2011) (citing *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004)). In particular, the file need not be transmitted to the web server under scenarios in which the filed determined to be harmful in step (c2) can be treated.

Nevertheless, Petitioner cites Kephart for the limitation: "Hodges did not, however, explicitly discuss a scenario in which the disinfection program

was unable to extract the harmful information from the file. But Kephart did." Pet. 216, 46. Kephart bears a 1997 copyright notice, and Petitioner provides a Declaration by Dr. Richard Ford, who was a Consulting Editor of the publication in which Kephart appeared, to support its contention that Kephart is prior art to the '196 patent. IPR2016-00216, Ex. 1035; *see* IPR2016-00216, Ex. 1013. Dr. Ford testifies that "[t]he Seventh International Virus Bulletin Conference took place in San Francisco, California from October 2 to October 3 in 1997." IPR2016-00216, Ex. 1013 ¶ 22. Dr. Ford further testifies that Kephart "was presented to conference attendees during a scheduled workshop and was included in the Proceedings of the Seventh International Virus Bulletin Conference," and that "[e]ach conference attendee was provided with proceedings of the conference as part of their registration package." *Id.* ¶¶ 25, 28. The Seventh International Virus Bulletin Conference was attended by "[o]ver 250 researchers from all over the world in the computer security field." *Id.* ¶ 27. In addition, "Virus Bulletin made available proceedings of this conference both in hardcopy and on CD. The CD version of the presentations was offered for sale directly from Virus Bulletin after the conference." *Id.* ¶ 29.

We credit Dr. Ford's testimony, which sufficiently establishes that Kephart was published more than one year before December 31, 1999, the earliest potential effective filing date of the '196 patent. Therefore, Kephart

qualifies as prior art under 35 U.S.C. § 102(b).[8] *See* Ex. 1001, at [30], [63]. Patent Owner does not contest Kephart's status as prior art.

Kephart describes an "immune system for computers that senses the presence of a previously unknown pathogen, and within minutes automatically derives and deploys a prescription for detecting and removing it." IPR2016-00216, Ex. 1035, abst. Petitioner identifies disclosures in Kephart of capturing, compressing, and encrypting a sample when a heuristic identifies a potential virus, and transmitting the encrypted sample to an administrative computer via a secure protocol. Pet. 216, 46–47 (citing IPR2016-00216, Ex. 1035, 166). Petitioner's argument that Kephart discloses the limitation of claim 2 relies on certain inferences, namely that "[t]he 'sample data' described in Kephart would have included an encapsulated version of the infected file itself," and that previously unknown viruses were "untreatable." *Id.*

To support these inferences, Petitioner relies on testimony of Dr. Prakash. *See* IPR2016-00216, Ex. 1008 ¶¶ 383–389. We credit this testimony, with which Patent Owner's expert, Mr. Bernstein, agrees. Ex. 2006 ¶ 199 ("I agree that it teaches this element"). Instead, Patent Owner attacks Petitioner's analysis with respect to underlying claim 1, with

[8] To the extent Dr. Ford provides testimony that the content of Kephart was orally presented at the Seventh International Virus Bulletin Conference, we do not consider any such oral presentation as part of Petitioner's asserted grounds of unpatentability. "A petitioner in an inter partes review may request to cancel as unpatentable 1 or more claims of a patent . . . only on the basis of prior art consisting of patents or printed publications." 35 U.S.C. § 311(b).

which we disagree for the reasons expressed above. *See* PO Resp. 216, 44 ("With respect to claim 2, *Kephart* does not satisfy the failings of *Hodges* and *Butt* and their failure to teach or suggest independent claim 1.").

Petitioner further provides reasoning to support its contention that "[c]ombining the teachings of Hodges, Butt, and Kephart was obvious and something a person of ordinary skill in the art would have been motivated to do." Pet. 216, 47. In addition to contending that Kephart is also within the field of endeavor of protecting computers from harmful information, Petitioner contends that Hodges and Kephart disclose "complementary methods and systems because Hodges disclosed an improved method for delivering antivirus software, and Kephart disclosed the need for deriving and delivery of prescription for previously unknown viruses." *Id.* at 30–31. Petitioner further contends that all three references disclose methods for "counteracting previously unidentified computer viruses" and disclose "pre-existing building blocks for delivering improved antivirus programs that when put together without any modification perform[] all steps of the challenged claims." *Id.* at 32–33. Patent Owner does not challenge this reasoning, which we find persuasive.

We conclude that Petitioner has demonstrated, by a preponderance of the evidence, that claim 2 is unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Kephart.

H. Motions to Amend

Each of Patent Owner's Motions to Amend in IPR2015-01855, IPR2015-01877, and IPR2016-00222 contingently moves to substitute

original claims 1, 3–5, 8–12, 14, and 15 with new claims, if those claims are determined to be unpatentable. Mot. Amend 1855, 1. Specifically, "substitute claims 36, 40, 42, and 44 . . . are proposed to replace original independent claims 1, 8, 10, and 12, respectively," and "substitute claims 37-39, 41, 43, and 45-46 . . . are proposed to replace original dependent claims 3-5, 9, 11, and 14-15 [by] merely chang[ing] dependency from original claims 1, 8, 10, and 12 to substitute independent claims 36, 40, 42, and 44, respectively, and correct for antecedent basis." *Id.* Proposed substitute claim 36 (to replace independent claim 1) illustrates the nature of the amendments proposed for each of the independent claims (proposed added text underscored):

> 36. A method for blocking in real time harmful information in a file to be executed, the method comprising the steps of:
>
> (a) on a computer network through which a <u>harmful information management</u> web server and a client system are linked to each other, the <u>harmful information management</u> web server receiving a connection request from the client system over the computer network <u>in real time for the file to be executed</u>;
>
> (b) the <u>harmful information management</u> web server transmitting <u>in real time</u> a harmful information blocking code module <u>based on capability and statistical data as a response to the connection request</u> to the client system; and
>
> (c) once the transmission of the harmful information blocking code module is completed, the harmful information blocking code module automatically running on the client system to block in real time harmful information including computer viruses,
>
> wherein the step (c) comprises steps of:
>
> (c1) inspecting file input/output (I/O) on the client system by hooking up file I/O routines,

> (c2) determining whether the file to be executed corresponding to the inspected file input/output in the step (c1) is harmful or not; and
>
> (c3) treating a file determined to be harmful in the step (c2) and executing the file, if it can be treated, and aborting the execution of the file determined to be harmful in the step (c2), if it cannot be treated.

Id. at 2.

Patent Owner's Motion to Amend in IPR2016-00216 contingently moves to substitute original claims 1, 2, and 7 with new claims, if those claims are determined to be unpatentable. Mot. Amend 216, 1. Proposed substitute claim 36 (to replace independent claim 1) in IPR2016-00216 "is duplicative of substitute claim 36 of [Patent Owner's] Motion to Amend in IPR2015-01855" and in the other proceedings. *Id.* at 1; *see id.* at 2. Proposed substitute claims 37–38 in IPR2016-00216, "which are proposed to replace original dependent claims 2 and 7, merely change dependency from original claim 1 to substitute claim[] 36." *Id.* at 1. In addition, Patent Owner "requests the Board to cancel claims 32-35 in the '196 patent." *Id.*

We grant the request to cancel claims 32–35. We deny those portions of the Motions to Amend that seek to substitute the independent claims and the related substitutions of dependent claims.

In addition to other amendments, Patent Owner's proposed substitutions of the challenged independent claims seek to add that, in addition to the "blocking" step, the "connecting" and "transmitting" steps are performed "in real time." But for reasons that parallel those discussed

supra in Section II.A.1., we conclude that such additional limitations lack sufficient support in the Specification of the ’196 patent.

For example, the phrase “in real time for the file to be executed,” proposed to be added to the “connecting” step, does not appear in the Specification, and the Specification does not teach that the connection request is made in connection with a potential threat in a file to be executed. As discussed in detail *supra*, the ’196 patent instead discloses embodiments in which connection is triggered in response to *manual* actions, i.e. by typing a URL or clicking on a hyperlink, not when a potential threat in a file to be executed is detected. Ex. 1001, col. 5, ll. 9–12.

In addition, the proposed substitute claims seek to modify the “transmitting” step so that it is “based on capability and statistical data as a response to the connection request.” In addressing this proposed limitation, Patent Owner argues that “the harmful information management server receives a collection of quantitative information on harmful information detected in the client computer, *which it uses to instantaneously counteract the virus*.” Mot. Amend 1855, 11 (citing Ex. 2006 ¶ 134) (emphasis added). But as we explain *supra*, the passage that Patent Owner relies on is properly understood, in the full context of the record, as instead describing “instantaneous” notification to the server that harmful information has been detected. *See* Ex. 1001, col. 8, ll. 28–44. Moreover, such understanding is consistent with the Applicant’s argument during prosecution of the counterpart Korean application that the invention “does not provide specifically tailored vaccine for vaccinating viruses existing inside each

client," but instead "provides the same real time harmful information screening module to all the clients." Ex. 2004, 26.

During the oral hearing, Patent Owner expressly agreed that

> it would be fair to say that, on the one hand, either [the] intrinsic evidence indicates the claim[s] should be construed [in their unamended form] to require the entire process to be in real time or, on the other hand, if [it is] determined that's not the case and it doesn't have to be in real time, that those portions of the specification wouldn't be enough to support from a [§] 112 standpoint the new real time limitations [Patent Owner is] seeking to add by amendment.

Tr. 56:6–15; *see id.* at 56:16 ("Yes, I agree with that."), 56:19–20 (confirming understanding the question and confirming agreement).

In addition to concluding that the intrinsic evidence does not support a construction that requires all of the "connecting," "transmitting," and "blocking" steps to be performed in real time, we conclude that the amendments that seek to add such a requirement lack sufficient support in the Specification and other intrinsic evidence. Accordingly, except for the cancellation of claims 32–35, we deny the Motions to Amend.

III. ORDER

It is

ORDERED that, based on a preponderance of the evidence, claims 1–5, 7–12, 14, and 15 of U.S. Patent No. RE42,196 E are held to be unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Amend in IPR2016-00216 is *granted* as to its request to cancel claims 32–35 of U.S. Patent No. RE42,196 E;

FURTHER ORDERED that Patent Owner's Motions to Amend are otherwise *denied*; and

FURTHER ORDERED that, because this is a final written decision, parties to this proceeding seeking judicial review of our decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

James F. Valentine
jvalentine@perkinscoie.com

Ryan J. McBrayer
RMcBrayer@perkinscoie.com

PERKINS COIE LLP

PATENT OWNER:

Keith E. Kline
kkline@carrferrell.com

CARR & FERRELL LLP

Bruce J. Wecker
bwecker@hausfeld.com

HAUSFELD LLP