Trials@uspto.gov
571-272-7822

Paper 14
Entered: March 8, 2016

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
Patent RE42,196 E[1]

---

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

BOUCHER, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Reviews
*37 C.F.R. § 42.108*

---

[1] We consolidate the proceedings under 35 U.S.C. § 314(d). The parties are directed to use a similar caption that identifies both proceedings in subsequently filed papers.

On September 2, 2015, McAfee, Inc. ("Petitioner") filed a Petition (IPR2015-01855, Paper 1 ("Pet. 1855")) pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1, 3, 5, 8, 10, and 12 of U.S. Patent No. RE42,196 E ("the '196 patent"). On September 4, 2015, Petitioner filed another Petition (IPR2015-01877, Paper 2 ("Pet. 1877")) to institute an *inter partes* review of claims 4 and 5 of the '196 patent. CAP Co., Ltd. ("Patent Owner") filed respective Preliminary Responses (IPR2015-01855, Paper 11 ("Prelim. Resp. 1855"); IPR2015-01877, Paper 10 ("Prelim. Resp. 1877")) on December 11, 2015. 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 consolidate the proceedings and institute *inter partes* review of claims 1, 3–5, 8, 10, and 12.

## 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,[2] 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

[2] Several exhibits have been filed in both proceedings. Unless otherwise noted, citations are to IPR2015-01855.

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

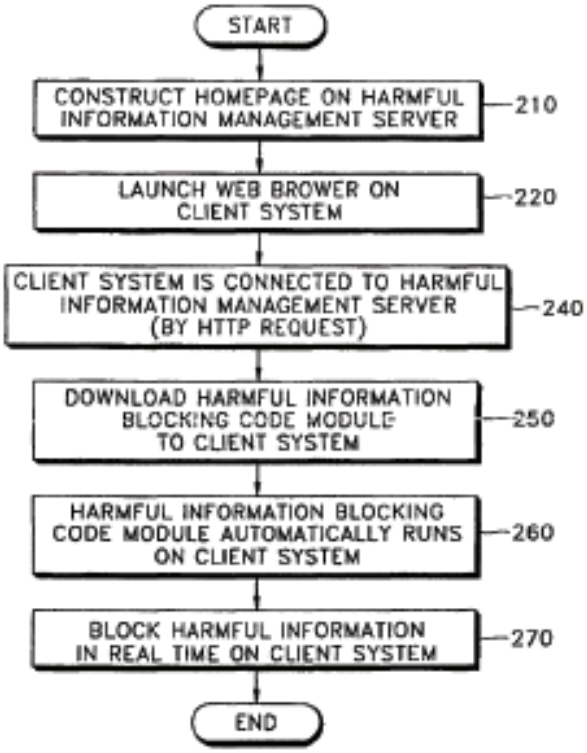


Figure 2A is a flowchart illustrating an online method of blocking harmful information. Ex. 1001, col. 4, ll. 32–34. After constructing a homepage on a server, launching a web browser on a client system, and connecting the client system to the server at blocks 210, 220, and 240, a harmful-information 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.

### *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, [64]. The '552 patent matured from the

national-stage entry of PCT/KR00/01374, which claimed priority to two Korean applications. *Id.* at [63], [30].

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 all 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 this proceeding 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.

### *B. References*

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")

### *C. Asserted Grounds of Unpatentability*

Petitioner challenges claims 1, 3, 5, 8, 10, and 12 in IPR2015-01855, and challenges claims 4 and 5 in IPR2015-01877, on the following grounds. Pet. 1855, 37; Pet. 1877, 38.

| References | Basis | Claim(s) Challenged |
|---|---|---|
| Hodges and Butt | § 103(a) | 1, 3, and 12 |
| Hodges, Butt, and Ször | § 103(a) | 5 |

| References | Basis | Claim(s) Challenged |
|---|---|---|
| Hodges, Butt, and Levergood | § 103(a) | 8 and 10 |
| Hodges, Butt, and Freund | § 103(a) | 4 and 5 |

### *D. 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 interprets claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *In re Cuozzo Speed Techs., LLC,* 793 F.3d 1268, 1278 (Fed. Cir. 2015) ("We conclude that Congress implicitly approved the broadest reasonable interpretation standard in enacting the AIA"), *cert. granted sub nom.*, *Cuozzo Speed Techs., LLC v. Lee*, 84 U.S.L.W. 3218 (U.S. Jan. 15, 2016) (No. 15-446); Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012).

#### *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 a 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.

Petitioner contends that the preambles are not entitled to patentable weight because "[t]he body of the 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. Petitioner specifically observes that the recitations "in real time" and "in a file to be executed" also appear in the bodies of the claims themselves. *Id.* at 11–12.

Patent Owner counters that "in real time" and "in a file to be executed" were "added to the preamble of the claims during prosecution to emphasize the real-time nature *of the entire method*, including the step of a web server transmitting a harmful information blocking code module to the client computer." Prelim. Resp. 1855, 11 (footnote omitted) (emphasis added). Addressing Petitioner's observation that similar recitations appear in the body of the claim, Patent Owner contends that "if the real time limitation in element (c) were entirely duplicative of the preamble, the patentee would have had no reason to add those words to the preamble in order to distinguish from Chen." *Id.* at 15.

Although we agree with Patent Owner that it is appropriate to consider the prosecution history, we are not persuaded on the present record that the preambles are limiting. *See Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1298 (Fed. Cir. 2015) ("The PTO should also consult the patent's prosecution history in proceedings in which the patent has been brought

back to the agency for a second review"). "[I]t 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). In this instance, the comments made by the applicant during prosecution draw two principal distinctions with Chen. First, the applicant distinguished the amended claims from Chen by arguing that Chen did not disclose certain limitations added in defining step "(c)" of the claim, i.e. that file input/output is inspected by "hooking up file I/O routines" or that execution of a file determined to be harmful is aborted. Ex. 2002, 101. Second, the applicant distinguished Chen by arguing that Chen "describes targeting all files to be treated," while the claims "block[] harmful information in a file to be executed in real time on a computer network." *Id.* at 100–01.

Notwithstanding Patent Owner's argument, it is not apparent from the prosecution history that the preamble amendments accomplish anything more than routine consistency with amendments made concurrently to the body of the claims. The applicant's comments do not identify clearly any aspect of Chen that is distinguished by the "in real time" language added to the preamble. And the "in a file to be executed" language appears merely to provide antecedent basis for the added recitation of "the file to be executed" in step (c2). Moreover, the resulting language of a method or system "for blocking in real time harmful information in a file to be executed" appears to recite no more than the purpose or intended use of the invention. Thus, "[t]he prosecution history fails to demonstrate 'clear reliance on the preamble during prosecution to distinguish the claimed invention from the

prior art.'" *Symantec,* 522 F.3d at 1289 (quoting *Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002)).

We have also considered Patent Owner's identification of certain passages in the Specification that Patent Owner characterizes as explaining "the real time nature of the entire method." Prelim. Resp. 1855, 18; *see id.* at 16–20 (citing Ex. 1001, col. 1, ll. 49–56, col. 1, l. 57–col. 2, l. 17, col. 4, ll. 42–47, col. 4, ll. 48–51, col. 4, ll. 58–60, col. 9, ll. 20–35, col. 8, ll. 27–44). Those portions of the Specification are not inconsistent with Patent Owner's position, but they do not express an unambiguous intention to limit the invention to a method or system with a globally real-time character.

Accordingly, on the present record and for purposes of this Decision, we do not afford patentable weight to the preambles of the challenged claims.

*2. "harmful information"*

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 (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. Other terms*

Petitioner proposes constructions for a number of other terms that appear in the claims. We do not find it necessary to construe such terms explicitly for purposes of this Decision, and accord the terms their ordinary and customary meaning.

## *B. Obviousness of Claims 1, 3, and 12 Over Hodges and Butt*

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.

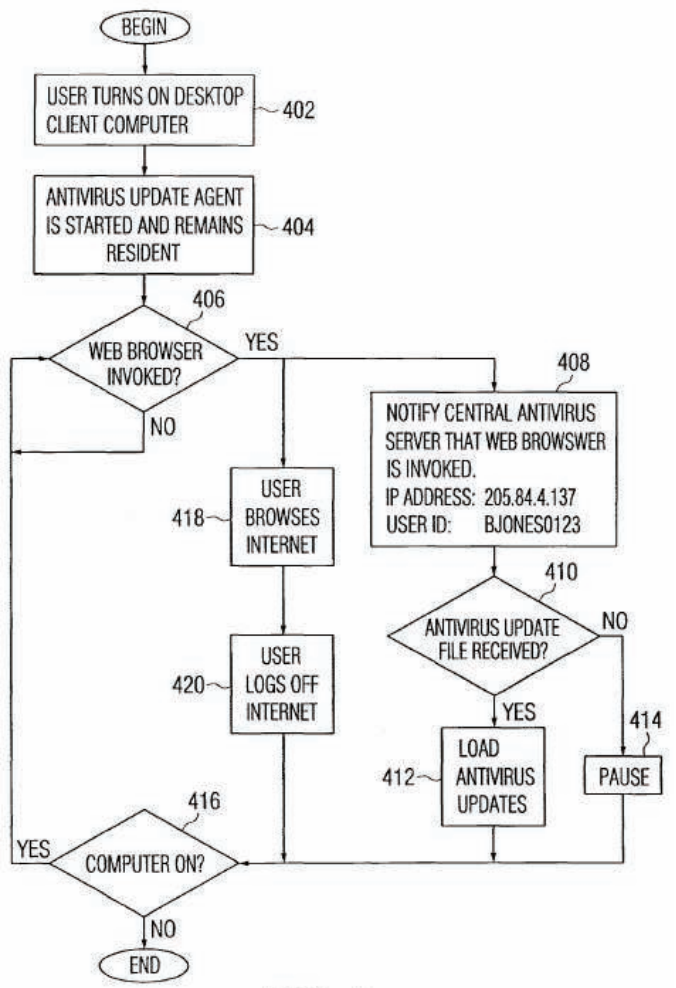


FIG. 4

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 these proceedings, 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. Petitioner's analysis draws a correspondence between the "harmful information blocking code module" recited in the claims and the antivirus software update pushed to the client computer. *Id.* at 41–42. Based on the record before us, we are persuaded that Petitioner has made a sufficient showing, including that the antivirus

software update described by Hodges "block[s] in real time harmful information including computer viruses," as recited in element (c) of independent claim 1. We are also persuaded that Petitioner has made a sufficient showing with respect to steps (c1)–(c3) of independent claim 1 by identifying Butt's disclosure of an interceptor function that scans files for viruses on access. *See id.* at 43–48. In considering Petitioner's argument directed at step (c3), we also credit the testimony of Petitioner's witness, Atul Prakash, Ph.D., that "even if Hodges does not explicitly state what happens to the infected file if it cannot be treated, a person of ordinary skill in the art would understand that a virus scanning engine would block the execution of an infected file if the file is unable to be treated." Ex. 1008 ¶ 271.

Furthermore, Petitioner provides sufficient reasoning at this stage 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).

After considering the arguments and evidence presented by the parties, we conclude that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenge of independent claims 1 and 12 as unpatentable under 35 U.S.C. § 103(a) over Hodges and Butt.

With respect to dependent claim 3, which 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." *Id.* at 48 (citing Ex. 1006, col. 2, ll. 46–47 (emphasis by Petitioner), col. 2, ll. 47–49). Petitioner has made a sufficient showing at this stage.

We conclude that Petitioner also has demonstrated a reasonable likelihood of prevailing on its challenge of dependent claim 3 as unpatentable under 35 U.S.C. § 103(a) over Hodges and Butt.

### *C. Obviousness of Claim 5 Over Hodges, Butt, and Ször*

Petitioner challenges dependent claim 5—which 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"—as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Ször. *Id.* at 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 a 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 further provides 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)) (clarifications by Petitioner). On this record, Petitioner's showing is sufficient at this stage of the case.

We conclude that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenge of dependent claim 5 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Ször.

### *D. Obviousness of Claims 8 and 10 Over Hodges, Butt, and Levergood*

Petitioner challenges independent claims 8 and 10 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Levergood. Independent

claims 8 and 10 are generally similar to independent claim 1, but encompass the embodiment of Fig. 2B of the '196 patent using a second server that provides information used in accessing a first server. *See* Ex. 1001, col. 6, ll. 1–28. Petitioner generally repeats 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 element." Pet. 1855, 51–52.

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.

In contending that one of ordinary skill in the art would have combined this multiserver architecture with Hodges and Butt, Petitioner observes that "Hodges specifically contemplated a multiserver architecture over the Internet," reasoning 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 Hodge'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); *see id.* at 55–57. Petitioner has made a sufficient showing at this stage.

We conclude that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenge of independent claims 8 and 10 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Levergood.

### *E. Obviousness of Claims 4 and 5 Over Hodges, Butt, and Freund*

In addition to challenging dependent claim 5 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Ször, Petitioner challenges dependent claims 4 and 5 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Freund. Pet. 1877, 48–59. Claim 4 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 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." Ex. 1007 (IPR2015-01877), 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 communication 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 Ex. 1007 (IPR2015-01877) at col. 13, ll. 57–65). Petitioner has made a sufficient showing at this stage.

We conclude that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenge of dependent claim 4 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Freund.

With respect to claim 5, Petitioner further contends that "Freund disclosed checking ongoing processes for harmfulness by checking their corresponding file activities." Pet. 1877, 57. Freund discloses "intercepting certain file activities and assigning them to the originating process" to "track files being created and changed by any process." Ex. 1007 (IPR2015-01877), 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. Petitioner has made a sufficient showing at this stage.

We conclude that Petitioner has demonstrated a reasonable likelihood of prevailing on its challenge of dependent claim 5 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Freund.

### *F. Consolidation*

There is considerable overlap in the issues involved in these two proceedings, which relate to the same patent. We exercise the discretion afforded by 35 U.S.C. § 315(d) to consolidate the proceedings.

## III. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that IPR2015-01855 and IPR2015-01877 are *consolidated*;

FURTHER ORDERED that *inter partes* review is *instituted* with respect to the following grounds of unpatentability:

(1) claims 1, 3, and 12 as unpatentable under 35 U.S.C. § 103(a) over Hodges and Butt;

(2) claim 5 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Ször;

(3) claims 8 and 10 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Levergood; and

(4) claims 4 and 5 as unpatentable under 35 U.S.C. § 103(a) over Hodges, Butt, and Freund;

FURTHER ORDERED that *inter partes* review is *not instituted* with respect to any other ground of unpatentability;

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(a), *inter partes* review of the '196 patent is hereby instituted commencing on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

PETITIONER

James F. Valentine
Ryan J. McBrayer
Jonathan Allred
PERKINS COIE LLP
JValentine@perkinscoie.com
RMcBrayer@perkinscoie.com
JAllred@perkinscoie.com

PATENT OWNER

Keith E. Kline, Esq.
CARR & FERRELL LLP
Bruce J. Wecker, Esq.
HAUSFELD LLP
kkline@carrferrell.com
bwecker@hausfeld.com