Paper No. 9
Entered: March 18, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SYMANTEC CORP.,
Petitioner,

v.

FINJAN, INC.,
Patent Owner.

Case IPR2015-01892
Patent 8,677,494 B2

Before JAMES B. ARPIN, ZHENYU YANG, and
CHARLES J. BOUDREAU, *Administrative Patent Judges*.

BOUDREAU, *Administrative Patent Judge.*

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

I. INTRODUCTION

Symantec Corp. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting *inter partes* review pursuant to 35 U.S.C. § 311 of claims 1, 2, 5, 6, 10, 11, 14, and 15 of U.S. Patent No. 8,677,494 B2 to Edery et al. (Ex. 1001, "the '494 patent"). Pet. 1. Finjan, Inc. ("Patent Owner") filed a Preliminary Response. Paper 7 ("Prelim. Resp."). We review the Petition under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a).

For the reasons that follow and on this record, we are persuaded that Petitioner demonstrates a reasonable likelihood of prevailing in showing the unpatentability of each of the challenged claims. Accordingly, we institute an *inter partes* review as to those claims.

A. The '494 Patent

The '494 patent, entitled "Malicious Mobile Code Runtime Monitoring System and Methods," issued March 18, 2014, from U.S. Patent Application No. 13/290,708 ("the '708 application"), filed November 7, 2011. Ex. 1001, [21], [22], [45], [54]. On its face, the '494 patent purports to claim priority from nine earlier applications, of which the earliest-filed is U.S. Provisional Application No. 60/030,639, filed November 8, 1996 (Ex. 1002, "the '639 application"). We need not make a determination on this record whether or not the challenged claims are entitled to the benefit of the filing dates of any of those earlier applications.

The ’494 patent describes protection systems and methods “capable of protecting a personal computer (‘PC’) or other persistently or even intermittently network accessible devices or processes from harmful, undesirable, suspicious or other ‘malicious’ operations that might otherwise be effectuated by remotely operable code.” *Id.* at 2:51–56. “Remotely operable code that is protectable against can include,” for example, “downloadable application programs, Trojan horses and program code groupings, as well as software ‘components’, such as Java™ applets, ActiveX™ controls, JavaScript™/Visual Basic scripts, add-ins, etc., among others.” *Id.* at 2:59–64.

B. Related Proceedings

The ’494 patent is the subject of a district court action between the parties, *Finjan, Inc. v. Symantec Corp.*, 3:14-cv-02998 (N.D. Cal. 2014), and has also been asserted in three other district court actions*, Finjan, Inc. v. Sophos, Inc.*, 3:14-cv-01197 (N.D. Cal. 2014)*, Finjan, Inc. v. Palo Alto Networks, Inc.*, 3:14-cv-04908 (N.D. Cal. 2014), and *Finjan, Inc. v. Blue Coat Systems, Inc.*, 5:15-cv-03295 (N.D. Cal. 2015). Pet. 1; Paper 5, 1.

Petitioner also filed another petition seeking *inter partes* review of the ’494 patent (Case IPR 2015-01897), a petition seeking *inter partes* review of related U.S. Patent No. 6,154,844 (Case IPR2015-01894), and two petitions seeking *inter partes* review of related U.S. Patent No. 7,613,926 (Cases IPR2015-01893 and IPR2015-01895). Pet. 1. Each of those petitions has been denied (Case IPR2015-01893, Paper 8; Case IPR2014-01894, Paper 7; Case IPR2015-01895, Paper 7; Case IPR2015-01897, Paper 7). Additionally, a petition filed by Sophos Inc. seeking *inter partes* review of the ’494 patent was denied on September 24, 2015 (Case IPR2015-01022, Paper 7), and a petition filed by Palo Alto Networks, Inc. seeking *inter partes* review of the ’494 patent is pending currently (Case IPR2016-00159, Paper 1).

C. Illustrative Claims

Of the challenged claims, claims 1 and 10 are independent. Those claims are illustrative and are reproduced below:

> 1. A computer-based method, comprising the steps of:
>
> receiving an incoming Downloadable;
>
> deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and
>
> storing the Downloadable security profile data in a database.
>
> 10. A system for managing Downloadables, comprising:
>
> a receiver for receiving an incoming Downloadable;
>
> a Downloadable scanner coupled with said receiver, for deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and
>
> a database manager coupled with said Downloadable scanner, for storing the Downloadable security profile data in a database.

Ex. 1001, 21:19–25, 22:7–16. Each of challenged claims 2, 5, and 6 depends directly from claim 1; and each of challenged claims 11, 14, and 15 depends directly from claim 10. *Id.* at 21:26–28, 21:33–37, 22:17–20, 22:26–30.

D. References Relied Upon

Petitioner relies on the following references:

Exhibit	Reference
1003	US 5,313,616, issued May 17, 1994 (“Cline”)
1004	Stephanie Forrest et al., *A Sense of Self for Unix Processes*, PROC. 1996 IEEE SYMPOSIUM ON SEC. & PRIVACY 120 (1996) (“Forrest”)[1]
1005	Morton Swimmer et al., *Dynamic Detection and Classification of Computer Viruses Using General Behaviour Patterns*, VIRUS BULL. CONF. 75 (Sept. 1995) (“Swimmer”)[2]
1012	US 5,623,600, issued Apr. 22, 1997 (filed Sept. 26, 1995) (“Ji”)

Pet. 3–5. Petitioner also relies on declarations of Sylvia Hall-Ellis, Ph.D. (Ex. 1006) and Jack W. Davidson, Ph.D. (Ex. 1018).

[1] Petitioner adduces evidence that Forrest was available to the public as of June 21, 1996. Pet. 4 (citing Ex. 1006, 7–8, 11–12, 15–17; Ex. 1008; Ex. 1009).

[2] Petitioner adduces evidence that Swimmer was available to the public as of December 1, 1995. Pet. 4–5 (citing Ex. 1006, 7–8, 11–12, 18–20; Ex. 1010; Ex. 1011).

E. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of the challenged claims on the following grounds:

Reference(s)	**Basis**	**Claims Challenged**
Swimmer	§ 102(b)	1, 2, 6, 10, 11, and 15
Swimmer	§ 103(a)	5 and 14
Swimmer	§ 103(a)	1, 2, 5, 6, 10, 11, 14, and 15
Cline and Ji	§ 103(a)	1, 2, 5, 6, 10, 11, 14, and 15
Forrest and Ji	§ 103(a)	1, 2, 5, 6, 10, 11, 14, and 15

Pet. 5.

In determining whether to institute an *inter partes* review of a patent, the Board, in its discretion, may "deny some or all grounds for unpatentability for some or all of the challenged claims." 37 C.F.R. § 42.108(b). Because Petitioner alternatively challenges claims 1, 2, 6, 10, 11, and 15 as either anticipated by Swimmer or as rendered obvious over Swimmer (Pet. 12–25), we exercise our discretion and decline to reach the anticipation challenge. 37 C.F.R. § 42.108(a).

II. DISCUSSION

A. Claim Interpretation

In an *inter partes* review proceeding, claims of an unexpired patent are given their broadest reasonable interpretation in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012); *In re*

Cuozzo Speed Techs., LLC, 793 F.3d 1268, 1275–79 (Fed. Cir. 2015), *cert. granted sub nom. Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 890 (2016). Under this standard, we interpret claim terms using "the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in the applicant's specification." *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997). We presume that claim terms have their ordinary and customary meaning. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007) ("The ordinary and customary meaning is the meaning that the term would have to a person of ordinary skill in the art in question.") (internal quotation marks omitted).

"Database"

The term "database" is recited in each of independent claims 1 and 10, as well as in dependent claims 2 and 11. Petitioner asserts that the broadest reasonable interpretation of the term "database" is "an organized collection of data." Pet. 10–11. Citing definitions from three dictionaries and Dr. Davidson's declaration for support, Petitioner contends this construction is consistent with the plain and ordinary meaning of the term to a person of ordinary skill in the art at the time of the '494 patent. *Id.* at 11 (citing RANDOM HOUSE WEBSTER'S COLLEGE DICTIONARY, 339 (2nd ed. 1999) (Ex. 1014, 3); WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY, 325 (1991) (Ex. 1015, 4); WEBSTER'S NEW WORLD DICTIONARY OF COMPUTER TERMS, 95 (4th ed. 1992) (Ex. 1016, 3); Ex. 1018 ¶¶ 84–85). Moreover, according to Petitioner, "neither the specification, nor the challenged claims, say anything about the form or structure of the claimed 'database,'" but "merely describe the type of data that is stored in the database (*e.g.*, [Downloadable security profile ('DSP')] data)." *Id.* (citing Ex. 1001, 3:47–50, 4:14–18, 9:52–55, Fig. 2, Fig. 3, claim 1). Petitioner contends that this construction is also consistent with Petitioner's position concerning the proper construction of this term in the related district court proceeding. *Id.* at 11–12 (citing *Finjan, Inc. v. Symantec Corp.*, 3:14-cv-2998 (N.D. Cal. 2014), Joint Claim Construction and Pre-Hearing Statement at 4 (Ex. 1017, 4)). According to Petitioner:

> [I]n the district court, Patent Owner agreed that a "database" is a collection of organized data. Ex. 1017, p. 4. Patent Owner argued, however, that the claimed "database" further requires the data to be organized "according to a database schema" and must "serve one or more applications." *See* Ex. 1017, p. 4. Patent Owner's proposed construction adds limitations that are unnecessary, confusing and, more importantly, have no support whatsoever in the intrinsic record. This appears to be nothing more than attempt to salvage the challenged claims by excluding certain types of databases described in the prior art, such as log files. *See* Ex. 1017, p. 4. Significantly, in the district court proceeding, Patent Owner and its expert acknowledged that, even under Patent Owner's proposed construction, at least some types of log files are "databases."

Id. at 12.

Patent Owner responds that the proper construction of "database" is instead "a collection of interrelated data organized according to a database schema to serve one or more applications." Prelim. Resp. 9. As Patent Owner points out (*id.*), this construction previously was adopted by the district court in Patent Owner's litigation with Sophos, Inc. concerning the '494 patent (*see Finjan, Inc. v. Sophos, Inc.*, No. 14-cv-01197 (N.D. Cal. 2014), Claim Construction Order at 7 (Ex. 2002, 7)), and also has been applied by the Board in two previous *inter partes* review proceedings. *See Sophos, Inc. v. Finjan, Inc.*, Case IPR2015-00907, slip op. at 8–10 (Paper 8) (Ex. 2003) (concerning related U.S. Patent No. 7,613,926); *Sophos, Inc. v. Finjan, Inc.*, Case IPR2015-01022, slip op. at 9–10 (Paper 7) (Ex. 2004) (concerning the ’494 patent).

Patent Owner asserts that its proposed construction in the concurrent district court litigation is “exactly the construction proposed herein,” and, therefore, Petitioner’s claim that “Patent Owner agreed that a database is a collection of organized data” (Pet. 12) “blatantly misrepresents Patent Owner’s position taken in the concurrent district court litigation.” Prelim. Resp. 11. Patent Owner contends that “[t]he goal of Petitioner’s construction is to broaden the term database beyond the specification so that it reads upon the techniques described in the cited prior art (e.g., a log file).” *Id.* at 10. Patent Owner further contends that Figure 3 of related U.S. Patent No. 6,092,194 (Ex. 3001, “the ’194 patent”)[3] “clearly illustrates that the security database 240 that stores DSP data 310 is completely different than a simple log file (i.e., Event Log 245).”[4]

[3] The ’194 patent is incorporated by reference in the ’494 patent. *See* Ex. 1001, 1:35–38.

[4] Patent Owner also contends that “Petitioner neglects to mention one of the passages of the ’494 Patent specifically relied upon by both the district court [in] *Finjan, Inc. v. Sophos, Inc.* as well as the Board in *Sophos, Inc. v. Finjan, Inc.*, Case Nos. IPR2015-00907 . . . and IPR2015-01022, that led both bodies to the conclusion that the claimed database could not be equated with a simple log file.” *Id.* at 10–11. Patent Owner then provides a quotation from a footnote in the district court’s claim construction order, stating in part that “[t]he fact that a database is listed along with more simple files ***does not mean that the database includes or is equated with these types of files***” and that “[i]n fact, one could argue that this list serves to

On this record, we agree with Patent Owner that the district court's construction in the litigation between Patent Owner and Sophos, as previously applied by the Board, represents the broadest reasonable construction of "database" in light of the claim language and the specification of the '494 patent. *See Morris*, 127 F.3d at 1054; *see also Power Integrations, Inc. v. Lee*, 797 F.3d 1318, 1326–27 (Fed. Cir. 2015) ("The fact that the board is not generally bound by a previous judicial interpretation of a disputed claim term does not mean . . . that it has no obligation to acknowledge that interpretation or to assess whether it is consistent with the broadest reasonable construction of the term."). As explained by the district court, the '494 patent does not define the term "database"; there is no evidence that Patent Owner disavowed the full scope of that term either in the Specification or during prosecution; and Patent Owner's definition appears to reflect both the context of the patent, as well as a well-accepted definition of the term. Ex. 2002, 5–7; *see also* IBM DICTIONARY OF COMPUTING, 165 (10th ed. 1993) (Ex. 2001, 3).

further differentiate a database from simpler files" (*id.* at 11 (quoting Ex. 2002, 5 n.1 (emphasis added by Patent Owner))), and cites certain pages of the Board's decisions (*id.* (citing Ex. 2003, 9; Ex. 2004, 9–10)). Patent Owner, however, does not identify the "one of the passages of the '494 Patent" upon which it alleges the court and the Board "specifically relied." Indeed, neither the quoted portion of Exhibit 2002 nor the cited portions of Exhibits 2003 and 2004 explicitly rely upon any passages of the '494 patent in reaching their respective conclusions. Exhibit 2002 does refer to column 9, lines 54–55 of related U.S. Patent No. 7,613,926, but it is unclear to us what relevance Patent Owner would intend us to ascribe to that citation.

Accordingly, on this record and for purposes of this Decision, we construe “database” to mean “a collection of interrelated data organized according to a database schema to serve one or more applications.”

B. Asserted Grounds of Unpatentability

Petitioner argues that claims 1, 2, 5, 6, 10, 11, 14, and 15 of the ’494 patent are rendered obvious under 35 U.S.C. § 103 by the references described above. *See supra* Sec. I.E. 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 skill in the art[5]; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

We analyze the asserted grounds with the principles identified above in mind.

[5] Petitioner proposes a definition for a person of ordinary skill in the art. Pet. 9–10; *see* Ex. 1018 ¶ 30. Patent Owner does not challenge this definition. For purposes of this Decision and to the extent necessary, we adopt Petitioner’s definition.

1. Obviousness over Swimmer

a. Overview of Swimmer

Swimmer is generally directed to a system, referred to as the "Virus Intrusion Detection Expert System" ("VIDES"), described as "a prototype for an automatic analysis system for computer viruses." Ex. 1005, 1. In Swimmer's system, an emulator is used to monitor the system activity of a virtual computer. *Id.* Sets of rules are used to detect viruses and extract details of their behavior. *Id.* The emulator collects system activity data and creates a set of audit record attributes that identify, among other things, disk operating system ("DOS") functions requested by the program, the register/memory values used in calls to the DOS functions, and register/memory values returned by the function calls. *Id.* at 1, 7, 9. The emulator provides the resulting audit trail in a canonical format as an activity data record for further analysis by a tool referred to as "Advanced Security audit trial Analysis on uniX" ("ASAX"). *Id.* at 9–12. ASAX analyzes the activity data collected by the emulator and detects viruses by employing rules that model typical virus behavior, using a rule-based language ("RUles-baSed Sequence Evaluation Language," or "RUSSEL") to identify the virus attack. *Id.* at 2, 4–5, 10–13. Swimmer discloses that ASAX also can pipe its output as a Normalized Audit Data Format ("NADF") file for further processing. *Id.* at 7, 12. Swimmer also states that "VIDES could conceivably be used outside the virus lab to detect viruses in a real environment" and that "[o]ne possibility is to use it as a type of firewall for programs entering a protected network." *Id.* at 13.

b. Discussion

Petitioner contends that Swimmer teaches or suggests all of the limitations of each of the challenged claims. Pet. 12–25.

First, Petitioner contends that Swimmer discloses both a "computer-based method," as recited in the preamble of claim 1, as well as a "system for managing Downloadables," as recited in the preamble of claim 10. *Id.* at 13–14. In particular, Petitioner contends, "Swimmer explains that its VIDES system is used to detect viruses in application programs and program code by monitoring and analyzing the functions and operations these programs attempt to invoke." *Id.* at 14 (citing Ex. 1005, 7; Ex. 1018 ¶ 89). "These application programs can include 'programs entering a protected network' (*i.e.*, executable code being downloaded over a network)." *Id.* (citing Ex. 1005, 13).

Second, according to Petitioner, because Swimmer "explains that the VIDES system can be used in a networked environment as part of a firewall for a protected network," Swimmer explicitly discloses that an incoming Downloadable is received over a network, as recited in claim 1. *Id.* at 15 (citing Ex. 1005, 13; Ex. 1018 ¶¶ 92–93 (explaining that firewalls are security devices or software located between an outside network, such as the Internet, and an internal network, such as an intranet that connects client computers)).

Relying on the testimony of Dr. Davidson, Petitioner further contends that, "in order for VIDES to be used at a firewall for 'programs entering a protected network' (*i.e.*, receive and analyze incoming Downloadables), a [person of ordinary skill in the art] would have understood that the system necessarily included a 'receiver' (i.e., networking components) for receiving these Downloadables." *Id.* at 16 (citing Ex. 1018 ¶ 94). Petitioner, accordingly, asserts that "Swimmer also discloses that the VIDES system includes a 'receiver' for receiving the Downloadable," as recited in claim 10. *Id.* Petitioner also argues, in the alternative, that this feature would have been obvious based on the teachings in Swimmer. *Id.* at 23–24. In particular, according to Petitioner, it would have been obvious that Swimmer's VIDES "could be used at a network device, such as a gateway or [file transfer protocol ("FTP")] or Web server in order to intercept incoming Downloadables and analyze them before they are sent to a destination computer," and "[o]ne of ordinary skill in the art would have been motivated to do so for a number of reasons, such as to improve the efficiency when checking incoming Downloadables." *Id.* at 23–24. Petitioner contends that, "[f]or one of ordinary skill in the art, this would have involved nothing more than combining well-known prior art elements (i.e., a gateway with Swimmer's VIDES system) according to well-known software programming techniques in order to yield a predictable result (i.e., a gateway scanner that receives Downloadables and analyzes their behavior)." *Id.* at 24 (citing Ex. 1018 ¶ 95).

Third, Petitioner contends, "Swimmer discloses [a Downloadable scanner coupled with said receiver for] deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable," as recited in claims 1 and 10. *Id.* at 16 (alteration in original) (boldface omitted). In particular, Petitioner alleges, to generate system activity data, Swimmer's emulator "accepts the entire instruction set of a processor as input, and interprets the binary code as the original processor would." *Id.* (quoting Ex. 1005, 8). Swimmer discloses that the "audit record attributes of records as collected by the PC emulator have the following meaning . . . [t]he final format for an MS-DOS audit record is as follows: <code segment, RecType[,] StartTime, EndTime, function number, [arg(…), ret(…)]>." *Id.* at 17 (quoting Ex. 1005, 9) (italics omitted by Petitioner). "In other words, the audit system and/or emulator generates audit records for the Downloadables (i.e., Downloadable security profile data) that identifies and lists functions (*i.e.*, operations) that the Downloadables attempt to invoke." *Id.* (citing Ex. 1005, Fig. 3 (illustrating an exemplary audit record listing identified operations); Ex. 1018 ¶¶ 98–99). Petitioner further contends:

> Swimmer explains that audit records generated by the audit system include a field, called "function number," which is the "number of the DOS function requested by the program." [Ex. 1005,] 9. As explained by Dr. Davidson, in DOS, function numbers are assigned to "INT 21h" functions, which include various types of system operations. [*Id.* at] 7 ("Primarily, interrupt 0x21 is used"); [Ex. 1018] ¶ 100. For example, function numbers 0, 49, 76 are program termination operations. Function numbers 15 are file operations (open, close). Functions 72-74, and 88 are memory operations. Function numbers 68, 94, and 95 are network operations. [*Id.* at] ¶ 101. Significantly, these operations identified by Swimmer's audit system are the very same types of operations referred to by the applications related to the '494 patent as examples of "suspicious operations." [Ex. 1002, 18:9-13] (DSP data "includes the fundamental computer operations," in a Downloadable such as "file management operations, system management operations, memory management operations and CPU allocation operations."). Thus, Swimmer discloses deriving security profile data (*e.g.*, audit records) that includes a list of suspicious operations that the Downloadable may attempt to invoke (*e.g.*, INT 21h system functions). [Ex. 1018] ¶ 102.

Id. at 17–18.

Additionally, Petitioner contends, "Swimmer discloses that this Downloadable security profile data is derived by a Downloadable scanner (*e.g.*, an emulator and/or audit system)." *Id.* at 18 (citing Ex. 1005, 8 (stating that the emulator is "a program which accepts the entire instruction set of a processor as input, and interprets the binary code as the original processor would"); Ex. 1018 ¶¶ 103–105 (explaining that identification and recordation of DOS function call numbers in Swimmer determines and identifies suspicious operations in the same manner as the code scanner described in the '194 patent)). Petitioner contends that the Downloadable scanner also is coupled to the receiver (e.g., the network components at the firewall). *Id.*

Lastly, Petitioner argues that Swimmer discloses that the audit records (i.e., Downloadable security profile data) are stored in a database, and that, accordingly, "Swimmer discloses [a database manager coupled with said Downloadable scanner, for] storing the Downloadable security profile data is a database," as recited in claims 1 and 10. *Id.* at 18–19 (alteration in original) (boldface omitted). Petitioner contends, in particular, that Figure 3 of Swimmer shows that "the audit record includes a list of suspicious operations identified by the audit system that are organized according to a clearly defined structure with various fields (*i.e.*, an organized collection of data that is organized based on a particular schema)." *Id.* at 19. Petitioner equates Swimmer's "audit system or a portion thereof" with the "database manager" recited in claim 10, and contends that "the database manager is coupled to the Downloadable scanner (*e.g.*, emulator)," as "both components are located on the same computer system (*e.g.*, a firewall) and would be stored together in memory (*e.g.*, RAM)." *Id.* at 20. Moreover, Petitioner contends, “to the extent Patent Owner argues that the claimed ‘database’ must ‘serve one or more applications,’ Swimmer . . . discloses that the audit records stored in the database are used by other processes.” *Id.* at 19–20. “For example, the database is used by an expert system (*e.g.*, application) to analyze program behavior using virus behavior rules.” *Id.* at 20 (citing Ex. 1005, 1, 2).

Petitioner also argues, in the alternative, that “the claimed [database manager for] storing the DSP data in a database would have been obvious based on the teachings in Swimmer.” *Id.* at 24–25 (alteration in original). In particular, according to Petitioner, “it would have been obvious to one of ordinary skill in the art that the security profile data in Swimmer could have been stored in any suitable format or structure, such as a relational database.” *Id.* (citing Ex. 1018 ¶ 111). “One of ordinary skill in the art would have been motivated to use such a database for a number of reasons,” Petitioner contends, including “to improve the organization, efficiency and speed when storing and retrieving this data.” *Id.* at 25 (citing Ex. 1018 ¶ 111). “Additionally, one of ordinary skill in the art would have also found it obvious to use a database manager with these types of databases.” *Id.* (citing Ex. 1018 ¶¶ 112–113).

With respect to dependent claims 2 and 11, which depend from claims 1 and 10, respectively, and further recite “stor[ing] a date & time when the Downloadable security profile data was derived [by said Downloadable scanner], in the database,” Petitioner points to Swimmer’s disclosure that each audit record entry includes “StartTime” and “EndTime” fields that indicate when the audit record was generated by the emulator and/or audit system. *Id.* at 20–21 (citing Ex. 1005, 9, 10, Fig. 3; Ex. 1018 ¶¶ 115–116).

With respect to claims 5 and 14, which depend from claims 1 and 10, respectively, and recite that the Downloadable "includes program script," Petitioner points to Swimmer's disclosure that VIDES can be used to derive security profile data for application programs and code, including programs received at a firewall, and argues that "[a]lthough Swimmer does not explicitly state that the Downloadables that are received and analyzed include 'program scripts,' this would have been obvious" to a person of ordinary skill in the art. *Id.* at 22 (citing Ex. 1005, Abst., 13; Ex. 1018 ¶¶ 121–122). Petitioner also points out that the '494 patent admits that various kinds of program scripts, including scripts received over a network, were well-known and disclosed in the prior art. *Id.* (citing Ex. 1001, 2:22–27). Thus, Petitioner contends, for a person of ordinary skill in the art, "this would have merely involved applying the same techniques to another well-known form of executable code (*e.g.*, receiving program scripts at a firewall and using the emulator to identify and record suspicious operations in the script)," and a person of ordinary skill in the art "would have been motivated to do so for a number of reasons, including to improve the effectiveness of the virus detection system taught by Swimmer by enabling use with a wider range of Downloadables." *Id.* at 23 (citing Ex. 1018 ¶¶ 124–125).

With respect to dependent claims 6 and 15, which depend from claims 1 and 10, respectively, and further recite that the suspicious computer operations "include calls made to an operating system, a file system, a network system, and to memory," Petitioner contends that "Swimmer discloses that the emulator and/or audit system identifies and records DOS system calls (*i.e.*, suspicious operations) that a Downloadable attempts to invoke." *Id.* at 21 (citing Ex. 1005, Fig. 3). Citing Dr. Davidson's testimony that different function numbers are assigned to the different types of system calls, including function numbers for file system operations, network system operations, and memory operations, Petitioner contends a person of ordinary skill in the art would have considered all of the system calls to be "operating system operations." *Id.* Petitioner additionally contends that certain other function numbers correspond to operating system operations for terminating a program, which, Petitioner points out, is an example of an operating system operation explicitly discussed in the '194 patent. *Id.* at 21–22 (citing Ex. 1005, Fig. 3; Ex. 1018 ¶¶ 119–120; Ex. 3001, 5:66–6:3).

Patent Owner raises a number of arguments in response to Petitioner's contentions, including that "Swimmer is not enabling and cannot, therefore, anticipate the '494 patent"; that Swimmer does not disclose "receiving an incoming Downloadable" or "a receiver for receiving an incoming Downloadable"; that Petitioner has not met its burden to demonstrate that Swimmer teaches the claimed "security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable"; that "Swimmer does not teach storing Downloadable security profile data in a database because it does not teach the derivation of the claimed Downloadable security profile data"; and that, "additionally, Petitioner does not identify any element disclosed in Swimmer that could be considered a 'database.'" Prelim. Resp. 13–22. With respect to claims 6 and 15, Patent Owner contends that, "even under its own theory, Petitioner has not met its burden to demonstrate that Swimmer discloses suspicious operations for all four distinct systems (i.e., 'an operating system, a file system, a network system, and to memory') recited in the claim language." *Id.* at 23. And with respect to claims 5 and 14, Patent Owner argues "Petitioner does not provide any evidence that Swimmer's emulator could analyze a Downloadable that included program script or even how a system could operate," and "[t]hus, Petitioner has failed to meet its burden that the '494 Patent is invalid because Swimmer's does not disclose this element and it is not enabled to processes scripts." *Id.* at 24.

We are persuaded on this record that Petitioner has demonstrated a reasonable likelihood that it would prevail at trial in showing that the subject matter of each of the challenged claims is unpatentable over Swimmer under 35 U.S.C. § 103. We are satisfied at this stage of the proceeding that Petitioner adequately accounts for all limitations of each claim, and we are not persuaded by Patent Owner's contention that "Swimmer is not enabled."

Although, as Patent Owner points out, Swimmer states that "[t]he present version of VIDES is only of interest to virus researchers; it is not designed to be a practical system for the end-user" (Ex. 1005, 2), it does not follow necessarily that Swimmer "cannot teach one of skill in the art how to make and use such a system without 'undue experimentation,'" as argued by Patent Owner. Prelim. Resp. 14 (quoting *Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1334 (Fed. Cir. 2003)). Petitioner has proposed that the person of ordinary skill in the art relevant to the '494 patent would have, for example, "a Master's degree in computer science, computer engineering, or a similar field, or a Bachelor's degree in computer science, computer engineering, or a similar field, with approximately two years of industry experience relating to computer security" and that "significant experience in the field of computer programming and malicious code might substitute for formal education." Pet. 9–10. Patent Owner has not challenged that definition, and, on this record, we regard that definition as appropriate to the subject matter of the challenged claims. *See supra* note 5. Importantly, we also observe that that definition much more closely approximates the skill level of a "[computer] virus researcher" than the skill level of an "end user." Moreover, although enablement is a threshold issue with respect to anticipation, *Amgen*, 314 F.3d at 1354, "a non-enabling reference may qualify as prior art for the purpose of determining obviousness under § 103." *Symbol Techs. Inc. v. Opticon Inc.*, 935 F.2d 1569, 1578 (Fed., Cir. 1991). In the context of § 103, "[e]ven if a reference discloses an inoperative device, it is prior art for all that it teaches." *Beckman Instruments Inc. v. LKB Produkter AB,* 892 F.2d 1547, 1551 (Fed. Cir. 1989).

Regarding Patent Owner's argument that Swimmer does not disclose "receiving an incoming Downloadable" or "a receiver for receiving an incoming Downloadable" (Prelim. Resp. 15), we are satisfied that those limitations are suggested by Swimmer's disclosure that "VIDES could conceivably be used outside the virus lab to detect viruses in a real environment" and that "[o]ne possibility is to use it as a type of firewall for programs *entering* a protected network" (Ex. 1005, 13 (emphasis added)). Contrary to Patent Owner's argument that "Swimmer acknowledges that . . . it is unclear how such a system would operate" (Prelim. Resp. 16), Swimmer specifies that "[f]or such a system to be accepted, it must not cause false positives," that "[a] concept for this is currently under development," and that "a virtual 8086 machine will be the basis for this" (Ex. 1005, 13).

We find that Petitioner has met its burden to demonstrate that Swimmer teaches the claimed "security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable." As Petitioner points out, Swimmer's audit trail includes a field entitled "function number" that identifies and lists numbers corresponding to DOS functions requested by an analyzed program. Pet. 17. Petitioner provides evidence that such function numbers were known in the prior art to correspond to, among other functions, the same four types of operations that are recited as "suspicious computer operations" in challenged dependent claims 6 and 15. Pet. 17–18, 21–22 (citing Ex. 1018 ¶¶ 117–120 (citing Duncan, "Advanced MS-DOS," Microsoft Press (1986) at 272–82 (Ex. 1020, 3–13) (listing function numbers corresponding to, *inter alia*, calls made to an operating system (e.g., function numbers 0, 49, 76), a file system (15, 19), a network system (68, 94, 95), and to memory (72, 73, 74, 88)))). Although Swimmer does not use the terms "security profile data" or "suspicious computer operations" to refer to such functions, Swimmer indicates that the audit records are based on a slight modification of a pattern "representing the program behaviour in general, and virus activity in particular." Ex. 1005, 9. Moreover, although the challenged claims require that the DSP data "includ[e] a list of suspicious computer operations that may be attempted by the Downloadable" (*see, e.g.*, claims 1, 10), the claims do *not* require that the list consist *only of* suspicious operations. Accordingly, we are not persuaded by Patent Owner's contention that "to find the claims anticipated by Swimmer's audit trail . . . would improperly read the limitation 'suspicious' out of the claim language." Prelim. Resp. 18.

We also are not persuaded by Patent Owner's argument that "Petitioner does not identify any element disclosed in Swimmer that could be considered a 'database.'" *Id.* at 19. Whereas Patent Owner contends that Swimmer's audit record is "a log of program activity, not a database," we disagree. As explained by Swimmer, the audit record includes records collected by Swimmer's VIDES system, organized with a specific "canonical format" to serve the ASAX tool. Ex. 1005, 9–10. We are persuaded on this record that the audit record is a database as that term is construed herein as "a collection of interrelated data organized according to a database schema to serve one or more applications." *See* Section II.A, *supra*.

We, accordingly, conclude that Petitioner has identified sufficient evidence to establish a reasonable likelihood of showing at trial that Swimmer teaches or suggests the subject matter of each of claims 1, 2, 5, 6, 10, 11, 14, and 15 of the '494 patent and that those claims are unpatentable under 35 U.S.C. § 103.

2. Obviousness over Cline and Ji

a. Overview of Cline

Cline describes a method for certifying the portability of software between computer systems, including certification tests to ensure that application programs will run on any conforming computer system regardless of the vendor. Ex. 1003, 2:66–3:5. The certification tests include a static analysis, in which the object code of an application program is analyzed against a "conformance database" of allowable external calls to determine whether any illegal or erroneous calls are being made, and a dynamic analysis, in which the application program is analyzed as it is being run to determine any runtime errors in the calls. *Id.* at 3:6–16. If no errors are detected in either analysis, the application program then is certified to be compatible and transportable without change between all certified compatible computer systems. *Id.* at 3:16–21.

b. Overview of Ji

Ji describes a system for detecting and eliminating viruses on a computer network, wherein a File Transfer Protocol ("FTP") proxy server is used to scan incoming and outgoing files for viruses and to transfer those files if they do not contain viruses. Ex. 1012, Abst. According to Ji, "[w]ith the advent of the Internet and its increased popularity, there are no prior art methods that have been able to successfully scan connections . . . such as those utilized by a gateway node in communicating with other networks," and, therefore, "there is a need for a system and method that can detect and eliminate viruses in networks attached to other information systems by way of gateways or the Internet." *Id.* at 2:19–22, 33–35. Ji discloses a method for processing a file before transmission into or from a network, including the steps of receiving a data transfer command and file name; transferring the file to a proxy server or system node; performing virus detection on the file; and determining whether the file contains any viruses. *Id.* at Abst., 3:4–11. If the file does not contain any viruses, the file is transferred from the system to a recipient node. *Id.* at Abst., 3:11–12. If the file does contain a virus, the file is deleted or some other preset action is performed. *Id.* at Abst., 3:13–14.

c. Discussion

Petitioner generally relies on Cline for teaching all limitations of independent claims 1 and 10 (Pet. 27–41), but additionally contends that, to the extent Cline does not expressly teach "receiving an incoming Downloadable," that limitation is taught by Ji (*id.* at 30). Petitioner also contends that "Ji explicitly teaches that its techniques can be used to scan files and messages including program code that are received or downloaded over a network," and, "[a]ccordingly, Ji teaches receiving and scanning incoming files and messages that include program code (*i.e.*, Downloadables)." *Id.* at 31. According to Petitioner, it would have been obvious for a person of ordinary skill in the art to combine the teachings of Cline and Ji, because both references are generally directed to scanning/analyzing executable programs and code, and a person of ordinary skill in the art would have been motivated to combine these teachings "for a number of reasons, including to verify that incoming Downloadables conform to certain rules before allowing computers on a network (*e.g.*, an Intranet) to download and execute the Downloadables." *Id.* at 31–32.

In response to Petitioner's contentions, Patent Owner argues, *inter alia*, that Cline is not analogous art to the '494 patent and that Petitioner has not demonstrated that the combination of Cline and Ji discloses "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable" and "storing the Downloadable security profile data in a database," as required by each of the challenged claims. Prelim. Resp. 28–42.

As an initial matter, we are not persuaded, on this record, by Patent Owner's assertions that Cline is not analogous art to the '494 patent. *Id.* at

28–31. Although Cline is concerned with interoperability, rather than security per se, we decline Patent Owner's invitation to define the field of endeavor so narrowly. Both Cline and the '494 patent fundamentally are concerned with the analysis of computer code, even if their intended applications differ. Moreover, we are not prepared, on this record, to say that methods that may be employed in determining compatibility are not reasonably pertinent to identifying security threats. *See In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011) ("A reference is reasonably pertinent if, even though it may be in a different field from that of the inventor's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering his problem.").

Nonetheless, we are persuaded by Patent Owner's substantive arguments that Petitioner has not demonstrated on this record that the combination of Cline and Ji teaches or suggests "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable" and "storing the Downloadable security profile data in a database." *Id.* at 31–42. Although Cline monitors and records system and procedure calls made by an application being tested, we are not persuaded, on this record, that Cline derives "security profile data," as that term is used in the challenged claims. Unlike Swimmer, discussed in Section II.B.2, *supra*, Cline does not relate records of such system and procedure calls to virus activity, but instead relates those calls with compliance testing. *Compare* Ex. 1005, 9, *with* Ex. 1003, 3:6–21. We agree with Patent Owner that Cline's dynamic and static analyses do not derive security profile data. Prelim. Resp. 32–39. And as

Patent Owner further points out (Prelim. Resp. 31), Petitioner has not cited Ji in connection with these limitations, except as allegedly teaching, in combination with Cline, that Cline's dynamic analyzer "would be coupled to the network components that receive incoming Downloadables" (Pet. 36).

On this record, Petitioner has not identified sufficient evidence that the combination of the teachings of Cline and Ji teaches or suggests all of the limitations recited in independent claims 1 and 10, and, in particular, "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable" and "storing the Downloadable security profile data in a database." Consequently, we are not persuaded that Petitioner demonstrates a reasonable likelihood that it would prevail at trial in showing that the subject matter of those claims or of dependent claims 2, 5, 6, 11, 14, or 15 would have been obvious over Cline and Ji.

3. Obviousness over Forrest and Ji

a. Overview of Forrest

Forrest is directed generally to "anomaly intrusion detection," wherein "it is assumed that the nature of [an] intrusion is unknown, but that the intrusion will result in behavior different from that normally seen in the system." Ex. 1004, 2. According to Forrest, because anomaly intrusion detection relies on detecting behavior that is different from what is considered normal, it is important to define normal behavior. *Id.* at 1 ("An important prerequisite of such a system is an appropriate definition of self, which is the subject of this paper."). Forrest, thus, discloses systems that are used to develop a database of normal program behavior of executable programs and to analyze such programs for subsequent anomalous behavior characterized by Forrest as intrusions. *Id.* at Abst., 1, 3. Forrest "defines normal behavior in terms of short sequences of system calls in a running process." *Id.* at 2. These sequences of system calls are stored in a database associated with a particular process. *Id.* ("The overall idea is to build up a separate database of normal behavior for each process of interest."); *id.* at 3 ("[W]e scan traces of normal behavior and build up a database of characteristic normal patterns (observed sequences of system calls)."). To generate the pattern of normal behavior, the program is run and data is collected using a utility referred to as "strace." *Id.* at 4. Deviations from the normal behavior sequences are detected as potential intrusions. *Id.* at 8 ("If a program enters an unusual error state during an attempted break-in, and if this error condition executes a sequence of system calls that is not already covered by our normal database, we are likely to notice the attack."). Additionally, Forrest teaches its techniques can be "implemented as an online system, in which the kernel checked each system call . . . [and] each site would generate its own normal database, based on the local software/hardware configuration and usage patterns." *Id.* at 7.

b. Discussion

Petitioner generally relies on Forrest as teaching each limitation of independent claims 1 and 10. Pet. 48–57. Petitioner equates Forrest's "anomaly intrusion detection" system with the "computer-based method" of claim 1 and the "system for managing Downloadables" of claim 10. *Id.* at 48–49. Petitioner contends that a person of ordinary skill in the art would have understood that the Sun SPARCstations on which Forrest disclosed its systems to run "would have typically included I/O hardware such as network cards, telephone modems, parallel ports, [and] serial ports, which would be capable of receiving 'incoming Downloadables.'" *Id.* at 49. Furthermore, Petitioner contends, "Forrest explains that these systems are capable of running applications such as sendmail[,] . . . a well-known email transfer utility," and "it also was well-known that generally any type of file (including executable programs) could be attached to e-mails, thus allowing a computer system running sendmail to receive and transfer these attachments to an ultimate destination (*e.g.*, a client)." *Id.* Still further, however, Petitioner contends that, "[t]o the extent Forrest does not expressly teach 'receiving an incoming Downloadable,' this feature is clearly disclosed by Ji," which "recognized that with the proliferation of the Internet, there was a need to scan and verify incoming executables at the connection points between networks (*e.g.*, gateways)." *Id.* at 50 (citing Ex. 1012, 2:13–29). According to Petitioner, it would have been obvious for a person of ordinary skill in the art to combine the teachings of Forrest and Ji, because both references "are directed to scanning/analyzing executable software (*i.e.*, Downloadables)," specifically, "anomaly intrusion detection" in Forrest, and "behavior detection" in Ji. *Id.* at 51–52 (citing Ex. 1018 ¶¶ 200–202). Petitioner argues that, "based on the teachings of Ji, it would have been obvious for Forrest['s] 'anomaly intrusion detection' system to receive 'Downloadables' and to determine/verify their behavior." *Id.* at 52 (citing Ex. 1018 ¶ 203).

With respect to the claimed "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable," Petitioner points, *inter alia*, to Forrest's disclosure that "we scan traces of normal behavior and build up a database of characteristic normal patterns (observed sequences of system calls)" and contends that "these traces represent 'operations that may be attempted by the Downloadable.'" *Id.* at 54 (citing Ex. 1004, 2–4; Ex. 1018 ¶¶ 207–209). Petitioner further contends that a person of ordinary skill in the art "would have understood that system calls correspond closely the types of 'suspicious operations' provided by the '639 provisional (which is incorporated by reference by the '494 patent)." *Id.* at 54–55 (citing Ex. 1002, 18:9–13; Ex. 1018 ¶¶ 210–212. Further, according to Petitioner, "Forrest teaches that the system calls (*i.e.* suspicious operations) are maintained in a list." *Id.* at 55 (citing Ex. 1003, 3).

Lastly, with respect to the claimed "storing the Downloadable security profile data in a database," Petitioner again points to Forrest's disclosure that a database is built up of "characteristic normal patterns (observed sequences of system calls)," as well as disclosure in Forrest that "[t]he overall idea is to build up a separate database of normal behavior for each process of interest." *Id.* at 56 (quoting Ex. 1003, 2–3). Further, Petitioner contends, "[t]o the extent [Patent Owner] argues that a database must 'serve one or more applications,' Forrest discloses that the database is used by further processes. More specifically, the database is used to analyze program behavior based upon newly captured traces of a program's execution in order to detect anomalies." *Id.* (citing Ex. 1003, 2–3, 7; Ex. 1018 ¶¶ 217–219).

Patent Owner responds that Petitioner has not demonstrated that the combination of Forrest and Ji discloses "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable" and "storing the Downloadable security profile data in a database," as required by each of the challenged claims.

Prelim. Resp. 43–48. With respect to the first of those limitations, in particular, Patent Owner argues, “Petitioner completely omits any explanation as to how the references teach the recited ‘deriving security profile data for the Downloadable,” and “[a]dditionally, Petitioner fails to demonstrate that Forrest in view of Ji discloses ‘a list of . . . suspicious computer operations that may be attempted by the Downloadable.’” *Id.* at 44. According to Patent Owner, whereas “Petitioner attempts to equate ‘traced normal behavior’ with ‘operations that may be attempted by the Downloadable,’” Forrest instead explains that “a trace ‘build[s] up a database of characteristic normal patterns (observed sequences of system calls)’” and “[o]nce these sequences are saved in a database Forrest discloses ‘check[ing] new traces against it using the same method.’” *Id.* at 44–45 (quoting Ex. 1004, 3). “Accordingly, what Forrest generates and stores in this database is neither a security profile for a Downloadable nor a list of suspicious operations; rather Forest generates a database including ***sequences of calls*** that a process performs during normal operations.” *Id.* at 45. “Second, the sequences of calls that are written to the database define a process’s ***normal behavior***,” and “Petitioner fails to explain how calls that are explicitly designated as normal could be considered ‘suspicious computer operations.’” *Id.* Patent Owner contends that, whereas Petitioner asserts that a person of ordinary skill in the art “would have understood that system calls correspond closely the types of ‘suspicious operations’ provided by the ’639 provisional,” the cited portion of the ’639 provisional “does not state or imply that all system calls are suspicious and all other computer operations are benign as implied in the Petition and cannot therefore cure Forrest’s deficiencies.” *Id.* at 45–46 (citing Pet. 54–55; Ex. 1002, 18:9–13).

We agree with Patent Owner that Petitioner has not demonstrated on this record that the combination of Forrest and Ji teaches or suggests "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable" and "storing the Downloadable security profile data in a database." *Id.* at 43–48. As Patent Owner points out (*id.* at 44–45), whereas Petitioner equates Forrest's "traced normal behavior" with the claimed "operations that may be attempted by the Downloadable" (Pet. 54), Forrest discloses instead that that traced normal behavior is used to build up a database of characteristic normal patterns against which new traces may be checked. *Id.* at 44–45; Ex. 1004, 3. Further, despite Petitioner's citation to the '639 provisional as providing exemplary "suspicious operations," we also agree with Patent Owner that Petitioner fails to provide any persuasive explanation as to how calls that are explicitly designated as "normal" could be considered 'suspicious computer operations.'" Prelim. Resp. at 45. Indeed, to the extent Forrest suggests that any operations at all might be suspicious, those would be *abnormal* operations, rather than the "normal operations" included in Forrest's database.

On this record, Petitioner has not identified sufficient evidence that the combination of the teachings of Forrest and Ji teaches or suggests all of the limitations recited in independent claims 1 and 10, and, in particular, "deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable" and "storing the Downloadable security profile data in a database." Consequently, we are not persuaded that Petitioner demonstrates a reasonable likelihood that it would prevail at trial in showing that the subject matter of those claims or of dependent claims 2, 5, 6, 11, 14, or 15 would have been obvious over Forrest and Ji.

C. Secondary Considerations

Patent Owner contends that Petitioner ignored evidence of secondary considerations that Patent Owner asserted in litigation with Petitioner, allegedly including evidence of "industry praise; licensing of Finjan's patent portfolio, including the '494 patent, to several technology companies, including McAfee, Inc./Intel Corporation, Websense, Inc., Webroot Inc., Trustwave Holdings, Inc., M86 Security and Microsoft; copying by competitors; and commercial success" (Prelim. Resp. 48–51). Thus far, however, Patent Owner has provided only a copy of an interrogatory response that provides insufficient detail for us to evaluate the strength of its evidence. Ex. 2005, 10–13. The interrogatory response alleges the existence and dates of agreements with the above-identified companies, but does not establish any nexus between the recitations of the challenged claims and the licenses themselves. *Id.* at 12. The licenses are not part of the record, and Patent Owner provides no evidence showing that the licensing program was successful either because of the recitations of the challenged claims or because they were entered into as business decisions to avoid litigation, because of prior business relationships, or for other economic reasons. "Without a showing of nexus, 'the mere existence of . . . licenses is insufficient to overcome the conclusion of obviousness.'" *Iron Grip Barbell Co. v. USA Sports, Inc.*, 392 F.3d 1317, 1324 (Fed. Cir. 2004) (quoting *SIBIA Neurosciences, Inc. v. Cadus Pharm. Corp.*, 255 F.3d 1349, 1358 (Fed. Cir. 2000)); *see also In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995). Patent Owner's interrogatory response also cites praise for its products, provides sales figures from the 2004–06 time period with a statement that "[t]hese sales were primarily the result of the Finjan platform, specifically the Vital Security suite," and alleges that versions of that product "in or about 2004 and later versions incorporated technology of claims 1, 7, 11, 15, 16, 41, and 43 of the '844 Patent," but Patent Owner has not made any evidence supporting this allegation of record in this proceeding. Ex. 2005, 11–12. On this record, the relatively weak evidence of secondary considerations does not overcome the relatively strong evidence of obviousness.

III. CONCLUSION

On this record, we conclude that Petitioner has demonstrated a reasonable likelihood that it would prevail at trial in demonstrating that claims 1, 2, 5, 6, 10, 11, 14, and 15 of the '494 patent are unpatentable over Swimmer.

At this stage of the proceeding, the Board has not made a final determination as to the patentability of any challenged claim or the construction of any claim term.

IV. ORDER

Upon consideration of the record before us, it is, therefore,

ORDERED that, pursuant to 35 U.S.C. § 314, an *inter partes* review is instituted as to claims 1, 2, 5, 6, 10, 11, 14, and 15 of the '494 patent under 35 U.S.C. § 103(a) as unpatentable over Swimmer;

FURTHER ORDERED that no other ground of unpatentability alleged in the Petition for any claim is authorized for this *inter partes* review; and

FURTHER ORDERED that, 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 commencing on the entry date of this Decision.

For PETITIONER:

Joseph J. Richetti
Daniel A. Crowe
BRYAN CAVE LLP
joe.richetti@bryancave.com
dacrowe@bryancave.com

For PATENT OWNER:

James Hannah
Jeffrey H. Price
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com

Michael Kim
FINJAN, INC.
mkim@finjan.com