UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case IPR2018-01505
Patent 9,137,205 B2

Before BRIAN J. McNAMARA, STACEY G. WHITE, and
JOHN P. PINKERTON, *Administrative Patent Judges.*

McNAMARA, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314
37 C.F.R. § 42.4(a)

BACKGROUND

Cisco systems Inc. ("Petitioner") filed a Petition, Paper 2 ("Pet."), to institute an *inter partes* review of claims 49, 52–53, 55, 58–60, 63, 66–67, 69, 72–74, 77, 80–81, 83, and 86–88 (the "challenged claims") of U.S. Patent No. 9,137,205 B2 ("the '205 patent"). 35 U.S.C. § 311. Centripetal Networks, Inc. ("Patent Owner") timely filed a Preliminary Response, Paper 6 ("Prelim. Resp."), contending that the petition should be denied as to all challenged claims. We have jurisdiction under 37 C.F.R. § 42.4(a) and 35 U.S.C. § 314, which provide that an *inter partes* review may not be instituted unless the information presented in the Petition "shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Having considered the arguments and the associated evidence presented in the Petition and the Preliminary Response, for the reasons described below, we decline to institute *inter partes* review.

REAL PARTIES IN INTEREST

The Petition identifies itself as the sole real party-in-interest. Pet. 3. Patent Owner identifies itself as the real party-in-interest. Paper 3, 1.

RELATED PROCEEDINGS

The Petition states that the '205 patent is asserted in the following proceedings:

Centripetal Networks, Inc. v. Cisco Systems, Inc., 2:18-cv-00094-MSD-LDL, E.D. Va., filed Feb. 13, 2018;

Centripetal Networks, Inc. v. Keysight Techs. Inc. and Ixia, 2:17-cv-00383-HCM-LRL, E.D. Va. Filed July 20, 2017;

Cisco Systems, Inc. v. Centripetal Networks, Inc., IPR2018-01443 and IPR2018-01444, PTAN, filed July 27, 2018. Pet. 3.

THE '205 PATENT (EXHIBIT 1001)

The '205 patent discloses methods and systems for protecting a secured network. Ex. 1001, Abstract. Figure 1 of the '205 patent is shown below:

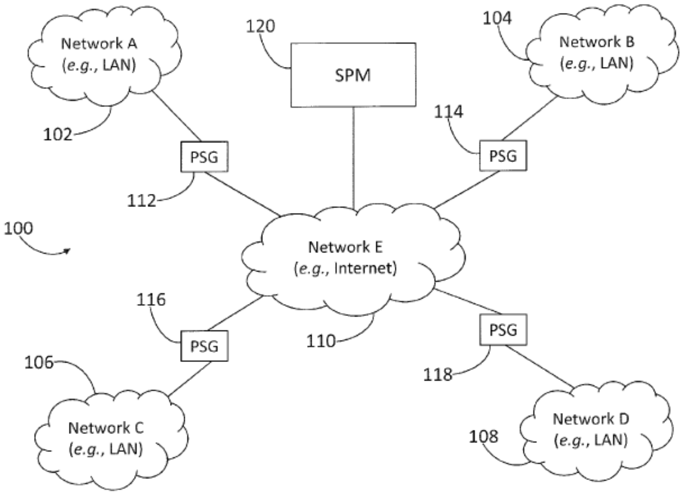

FIG. 1

Figure 1 illustrates a network environment that includes packet security gateways (PSGs) situated between networks and a security policy management server (SPMS) that communicates dynamic security policies to the PSGs. *Id.* at 4:53–55, 5:5–15, Fig. 1. The PSGs may operate in a network transparent manner, sending and receiving traffic at a link layer using an interface that is not addressed at the network layer, and simultaneously performing packet transformation functions at the network layer. *Id.* at 3:1–6. The PSG may include a management interface having a network layer address accessible at the application layer. *Id.* at 3:7–10.

The PSGs perform packet transformation functions on received packets according to rules in a dynamic security policy that specifies one or more packet transformation functions that should be performed on packets associated with specific criteria. *Id.* at 5:15–25, 6:59–62.

> The specified criteria may take the form of a five-tuple of values selected from packet header information, specifying a protocol type of the data section of the IP packet (e.g., TCP, UDP, ICMP, or any other protocol), one or more source IP addresses, one or more source port values, one or more destination IP addresses, and one or more destination ports.

Ex. 1001, 6:62–67, Fig. 3.

The ’205 patent states that packet transformation functions may forward packets into or out of the network protected by the PSG (e.g., Ex. 1001, 2:47–51) or drop all packets associated with network addresses outside a specified set (*id*. at 1:65–2:4, 2:54–56). Multiple dynamic security policies also may be received from the security policy management server. *Id.* at 2:12–24. For example, rules in a dynamic security policy may specify a transformation function that routes or switches packets to a network address corresponding to a monitoring device by encapsulating the packet with a header that corresponds to the network address of the monitoring device. *Id.* at 15:1–7. The monitoring device strips the header and copies the packets, or data within the packets, for subsequent review before forwarding the packets to the destination address. *Id.* at 15:7–17.

Various combinations of rules may implement services, such as a blocklist service within a network environment that may include one or more rules specifying criteria for which associated packets should be blocked or denied, and at least one rule specifying that all packets outside the blocked sets should be forwarded, accepted, or allowed. *Id.* at 7:55–8:6.

ILLUSTRATIVE CLAIM

Independent claim 49, reproduced below, is illustrative of the subject matter of the challenged claims:

> 49. A method, comprising:
>
> at each of one or more packet security gateways associated with a security policy management server:
>
> receiving, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI):
>
> receiving packets associated with a network protected by the packet security gateway; and
>
> performing, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy, wherein performing the at least one packet transformation function comprises:
>
> encapsulating at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a network device configured to copy information contained in the at least one packet and to forward the at least one packet to the destination network address; and
>
> routing, based on the header, the at least one packet to the network address that is different from the destination network address.

Ex. 1001, 27:47–28:6.

ART CITED IN PETITIONER’S CHALLENGES

Petitioner cites the following references in its challenges to patentability:

Reference	Designation	Exhibit No.
U.S. Patent Appl. Publ. No. 2007/0262741 A1	Jungck	Ex. 1010
Ingate Firewall/SIParator SIP Best Practice, Sept. 2, 2008	Ingate	Ex. 1012
C. Perkins, IP Encapsulation within IP, Network Working Group Request for Comment 2003, October 1996	RFC 2003	Ex. 1016
T. Ylonen, The Secure Shell (SSH) Transport Layer Protocol, Network Working Group, Request for Comments: 4253 (C. Lonvick ed., January 2006)	RFC 4253	Ex. 1013

CHALLENGES ASSERTED IN PETITION

Claims	Statutory Basis	Challenge
49, 52, 53, 55, 58, 60, 63, 66, 67, 69, 72, 74, 77, 80, 81, 83, 86, and 88	35 U.S.C. § 103(a)	Obvious over Jungck in view of Ingate and RFC 2003
57, 73, and 87	35 U.S.C. § 103(a)	Obvious over Jungck in view of Ingate and RFC 2003, and RFC 4253

ORDINARY SKILL IN THE ART

Noting that relevant experience and education can substitute for each other, Petitioner states that a person of ordinary skill in the relevant art on April 16, 2014 (the filing date of the application that matured in the ’205 patent), would have had a bachelor's degree in computer science, computer engineering, or an equivalent, four years of professional experience, and a working knowledge of packet-switched networking, firewalls, security policies, communication protocols and layers, and the use of customized rules to address cyber-attack. Pet. 18 (citing Ex. 1006, Declaration of Dr. Kevin Jeffay ("Jeffay Decl.") ¶¶ 24–26). Petitioner's definition of a person of ordinary skill, which Patent Owner does not dispute at this stage, appears appropriate for the technology addressed by this proceeding.

CLAIM CONSTRUCTION

The Petition has been accorded a filing date of July 26, 2018. For petitions accorded a filing date before November 13, 2018, we interpret 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) (2018); *Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016). In applying a broadest reasonable construction, claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Any special definition for a claim term must be set forth in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

Petitioner proposes the following claim constructions (Patent Owner does not propose constructions for any other terms):

Dynamic security policy. Petitioner proposes that "dynamic security policy" be construed to mean "any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria." Pet. 13 (citing Ex. 1001, 4:44–47; Ex. 1006, Jeffay Decl. ¶¶ 148–150).

Patent Owner argues that Petitioner's proposed construction improperly reads the term "dynamic" out of the claim and is inconsistent with the construction adopted by the district court in the Keysight litigation. Prelim. Resp. 11. Patent Owner proposes that "dynamic security policy" be construed to mean "a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets." *Id.* at 10.

We addressed the construction of this term in our Decision to Institute in *Cisco Systems, Inc. v. Centripetal Networks, Inc.,* Case IPR2018-01386, slip op. at 7–8 (PTAB Jan. 24, 2019)(Paper 8) ("the '1386 IPR"), which concerned challenges to certain claims of related U.S. Patent 9,565,213 B2 (the "'213 patent"), and in *Cisco Systems, Inc. v. Centripetal Networks, Inc.,* Case IPR2018-01443, slip. op at 8 (PTAB Feb. 12, 2019) (Paper 7), which also concerned the '205 patent. As in the '1386 IPR, the language proposed by Petitioner in this case follows exactly the disclosure in the '205 Specification (and the '213 Specification) that states "[a]s used herein, a dynamic security policy includes [Petitioner's proposed construction]." Ex. 1001, 4:43–47. We also note the '205 Specification (and the '213 Specification) states "[o]ptionally, a dynamic security policy may further specify one or more additional parameters as described herein." *Id.* at 4:48–49. Patent Owner points to no disclosure in the '205 Specification that gives any meaning to the term "non-static" in its proposed construction. Nothing in Petitioner's proposed construction precludes a "dynamic security policy" from changing at any time.

In view of the disclosure in the '205 Specification, and consistent with the '205 Specification (and the '213 Specification), we construe "dynamic security policy" to mean *any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria.*

Rule/rules. Petitioner proposes that the term "rule/rules" be construed to mean "part of a dynamic security policy" that "may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria." Pet. 13 (citing Ex. 1001, 6:59–67, 7:64–65; Ex. 1006, Jeffay Decl. ¶¶ 151–153). Patent Owner argues that Petitioner's construction is ambiguous because it introduces criteria and packet transformation functions into the construction. Prelim. Resp. 11–12. Patent Owner proposes that we apply the same construction the district court applied in the Keysight litigation, i.e., "a condition or set of conditions that when satisfied cause a specific function to occur." *Id.* at 11 (citing Ex. 2001, 21–22). Although "rule" is used throughout the '205 Specification, "rule" is not defined. The exemplary dynamic security policy of Figure 3 is illustrative of how "rule" is used in the '205 patent. Figure 3 shows Rules 1–5, each of which causes an action, i.e., a packet transformation (e.g., accepting, denying, or forwarding packets to a monitoring device), in response to a specific set of conditions specified by a five-tuple (e.g., protocol, source address, source port, destination address and port address).

It is not necessary to define “rule/rules” as part of a dynamic security policy because all the challenged claims recite that receiving a dynamic security policy comprises receiving one or more rules. Having considered the ’205 Specification and the evidence currently of record, we adopt the construction used in the Keysight litigation and construe “rule/rules” to mean *a condition or set of conditions that when satisfied causes a specific function to occur*.

Security policy management server (SPM server or SPMS). Petitioner cites the ’205 patent as stating that an SPM server “includes ‘any computing device configured to communicate a dynamic security policy to a packet security gateway.’” Pet. 14 (citing Ex. 1001, 4:38–40). Patent Owner proposes the same construction, except that Patent Owner proposes to substitute the word “server” for “any computing device,” as proposed by Petitioner. Prelim. Resp. 12 (citing Pet. 13–14, which acknowledges that the ’205 patent discloses a server). Petitioner acknowledges that Patent Owner’s proposed construction was applied in the Keysight litigation and the Petition applies Patent Owner’s proposed construction. Pet. 14. We agree with Patent Owner. The term “any computing device” is so broad in this context that it has no clear meaning. We note, however, that the ’205 patent states that it does not use term “server” in the same context as used in a client-server architecture, where a server responds to requests from a client. Ex. 1001, 12:53–58. Instead, “server” in the context of the ’205 patent (and the related ’213 patent) refers to a computing device that performs the functions described in the ’205 patent, but not necessarily in the response to client computer requests. Recognizing that the ’205 patent discloses any such computing device be configured as a server, we construe “security policy management server" to mean *a server configured to communicate a dynamic security policy to a packet gateway*.

Packet security gateway (PSG). Petitioner proposes that we construe "packet security gateway (PSG)" to mean "a gateway computer configured to receive packets and perform a packet transformation function on the packets," stating that this construction is consistent with that agreed to by Patent Owner in the Keysight litigation. Pet. 14. Petitioner cites the '205 patent as stating that a "packet security gateway" "includes 'any computing device configured to receive packets and perform a packet transformation function on the packets.'" *Id.* (citing Ex. 1001, 4:33–35). Patent Owner does not oppose Petitioner's proposed construction. Prelim. Resp. 12. As the proposed construction appears consistent with the use of the term in the '205 patent, we construe "packet security gateway" to mean *a gateway computer configured to receive packets and perform a packet transformation function on the packets.*

Packet transformation function. Petitioner proposes that we construe "packet transformation function" to mean "an action taken upon a packet." Pet. 14–15. Petitioner notes that the '205 patent does not define this term explicitly, but describes a packet transformation function as an action taken on a packet, such as forwarding, dropping, routing, and queuing packets. *Id.* (citing Ex. 1001, 2:37–56, 7:34–36, 9:25–26; Ex. 1006, Jeffay Decl. ¶¶ 158–164). Patent Owner contends Petitioner's proposed construction inappropriately removes any act of "transformation." Prelim. Resp. 12. Patent Owner proposes that we construe this term to mean a "function that transforms one or more packets from one state to another." *Id.* at 13.

Patent Owner’s proposed construction of “packet transformation function” as a “function that transforms one or more packets from one state to another” uses a variation of the operative term “transform” to define itself. *Id.* Patent Owner does not cite to any discussion in the ’205 patent about the state of a packet or what it means to transform a packet from one state to another. Thus, we are not persuaded that Patent Owner’s proposed construction provides a meaningful construction of the term.

The ’205 Specification states that a dynamic security policy includes any rule that specifies packet criteria “identifies a packet transformation function to be performed on packets corresponding to the specified criteria.” Ex. 1001, 4:43–46. Above, we construed the term “rule” to mean “a condition or set of conditions that when satisfied causes a specific function to occur.” Consistent with that construction of rule, we note that the ’205 Specification refers to “a packet transformation function specified by one of the rules” (Ex. 1001, 1:57–58) or “by the rule on the packet” (*id.* at 11:65–66). *See also id.* at 19:30–32. The ’205 patent also describes “[t]he packet transformation function specified by the dynamic security policy.” *Id.* at 2:36–37, 5:10–12, 5:19–20, 19:17–19. The ’205 Specification states that a dynamic security policy may include a rule that forwards a packet to a packet transformation function (e.g., *id.* at 5:65–6:2) and that the packet transformation function may perform a number of operations, such as: forwarding packets to the network or an IPsec stack; dropping packets or sending them to an infinite sink (e.g., *id.* at 6:5–14); routing packets to a network address corresponding to a monitoring device whose address may be different from the packet’s destination network address; and encapsulating packets with an IP header specifying the address corresponding to the monitoring device (*id*. at 15:1–15). Thus, dynamic security policies and rules identify conditions that cause packet transformation functions to carry out specific operations that may differ depending upon the policy or rule that applies to detected packet conditions.

In consideration of the above, we construe the term “packet transformation function” to mean *operations performed on a packet*.

PRINTED PUBICATION STATUS OF INGATE

Introduction

Petitioner cites Ingate in each of its challenges to patentability. The lower left corner of each page of the Ingate reference states “Ingate – Partner Information Guide.” The Ingate reference as filed in this proceeding does not include a copyright notice or state that it was published in any particular place. A date on the cover page of the Ingate reference, September 2, 2008, is earlier than the October 22, 2012 filing date of the ’205 patent. *See* Ex. 1012. As discussed below, Petitioner cites the Ingate reference as a document available on a website operated by Ingate. Patent Owner argues that Petitioner failed to establish the Ingate reference qualifies as a prior art printed publication because Petitioner did not demonstrate the Ingate reference was accessible to the public before the priority date of the ’205 patent. Prelim. Resp. 22–26. .

The party seeking to introduce the reference “should produce sufficient proof of its dissemination or that it has otherwise been available and accessible to persons concerned with the art to which the document relates and thus most likely to avail themselves of its contents.” *In re Wyer*, 655 F.2d 221, 227 (CCPA 1981). In this case, the burden is on Petitioner to demonstrate that Ingate is a prior art reference. *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018) (petitioner has the burden of proving a reference is a printed publication).

The Petition states only that the Ingate reference "is a printed publication that published on September 2, 2008, and was publicly available more than one year before the October 22, 2012 priority date of the '205 patent." Pet. 16. As support for this assertion, Petitioner cites the Declaration of Scott Beer (Ex. 1023, Beer Decl.) and the Declaration of attorney Christopher Davis (Ex. 1021, Davis Decl.). *Id.*

The Beer Declaration (Ex. 1023)

Mr. Beer testifies that he worked for Ingate from January 2008 through September 2013 writing articles explaining and teaching aspects of VoIP technology. Ex. 1023, Beer Decl. ¶ 3. Mr. Beer states that he authored the Ingate reference and that he did not revise it after he completed the first draft on September 2, 2008. *Id.* ¶ 4. Mr. Beer further testified that Ingate published papers as soon as possible after they were written, that he recalls the Ingate reference was published to the Ingate website and was publically available on or around September 2, 2008, and that the Ingate reference was supplied to potential customers via the website. *Id.* ¶¶ 4–6.

Patent Owner responds that Mr. Beer's testimony demonstrates that "his role at Ingate was limited to writing articles and explaining and teaching," but that Mr. Beer "does not even claim to have been the one to publish the paper on the website." *Id.* at 24.

Patent Owner also notes that the website at the address specified in Mr. Beer's declaration, http://www.ingate.com/appnotes/Ingate_Security_Best_Practices.pdf (the

Link), could not be located on the Wayback machine, a well-known website archiving tool. *Id.* at 23 (citing Ex. 2003, stating "Wayback Machine doesn't have that page archived"). Thus, Patent Owner argues that Petitioner fails to offer any evidence that the Ingate reference actually was available to an interested member of the public in the relevant time frame or how such a person could locate the Ingate reference. *Id.*

The Davis Declaration (Ex. 1021)

Mr. Davis testifies that, when preparing the Petition, an attorney at Merchant & Gould, P.C. accessed the website at the Link and retrieved the Ingate reference. Ex. 1021 ¶ 3. According to Mr. Davis, metadata in the Adobe Acrobat file containing the Ingate reference indicates that the reference was created using Microsoft Word 2007 at 9:32 AM on September 2, 2008. *Id.* ¶ 4 (citing Document Properties viewed on July 18, 2018).

Patent Owner responds that this evidence merely demonstrates the date the document was created, but provides no information about whether or when the document became accessible to the public at the Link. Prelim. Resp. 25.

Mr. Davis also testifies he located an article by K.V.N.R. Sai Krishna titled Safety Dimensions of Session Initiation Protocol published in the August 2013 *Journal of Computer Science and Mobile Computing* that cites the Ingate reference in footnote 32. Footnote 32 includes a parenthetical stating that the author accessed the Ingate reference on April 4, 2012 using the Link. Ex. 1021 ¶ 5 (citing Ex. 1022 n.32) ("the Krishna Article").

Patent Owner contends that the Krishna article demonstrates only that "the author had a direct link to Ingate," but "does not establish that Ingate was disseminated to the public, or that a person interested in the art would have been able to locate the reference." Prelim. Resp. 25.

Analysis

"The statutory phrase 'printed publication' has been interpreted to mean that before the critical date the reference must have been sufficiently accessible to the public interested in the art; dissemination and public accessibility are the keys to the legal determination whether a prior art reference was 'published.'" *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1568 (Fed. Cir. 1988). Whether a reference qualifies as a "printed publication" involves a case-by-case inquiry into the facts and circumstances surrounding the reference's disclosure to members of the public. *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004). The key inquiry is whether the reference was made "sufficiently accessible to the public interested in the art" before the critical date. *In re Lister*, 583 F.3d 1307, 1311 (Fed. Cir. 2009) (quoting *In re Cronyn*, 890 F.2d 1158, 1161 (Fed. Cir. 1989)). A reference is considered "publicly accessible" upon a satisfactory showing that the document has been "disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence[] can locate it." *Kyocera Wireless Corp. v. ITC*, 545 F.3d 1340, 1350 (Fed. Cir. 2008) (citation and internal quotation marks omitted).

Often, the determination of public accessibility turns on whether a reference is indexed and catalogued in a meaningful way. For example, a dissertation shelved in the stacks and indexed in the catalog at a university library was found to be a printed publication. *In re Hall*, 781 F.2d 897, 898–99 (Fed. Cir. 1986). However, indexing and cataloging must be prepared in a "meaningful" way, e.g., in relationship to the subject matter of the references, to allow an interested researcher exercising reasonable diligence to locate the prior art. *See Cronyn*, 890 F.2d at 1161. Accessibility goes to the issue of whether interested members of the relevant public could obtain the information. If accessibility is proved, there is no requirement to show that particular members of the public actually received the information. *Constant*, 848 F.2d at 1568–69.

We consider Mr. Beer's testimony, recognizing that evidence of a routine business practice can be sufficient to prove that a reference was made accessible before a critical date. *See* Hall, 781 F.2d at 899. Although Mr. Beer states that he has "personal knowledge regarding the content and publishing of the Ingate reference," Mr. Beer does not assert that, except for his authorship, he had any role in publishing the Ingate reference. Ex. 1012, Beer Dec. ¶¶ 3–6. Mr. Beer does not state that he personally placed the Ingate reference on Ingate's publically accessible website. *Id*. Mr. Beer offers no testimony as to what the legend "Ingate – Partner Information Guide" means or how the Ingate reference would have been published on the website, such that it would have been accessible to the public in the relevant time frame. *Id.* Mr. Beer provides no information about Ingate's procedures for reviewing and approving articles prior to publication on Ingate's website. Mr. Beer also does not describe how such articles were posted to the website, e.g., Mr. Beer does not describe procedures Ingate followed to load the reference to a publically accessible location, to assign a link to that location, who was responsible for carrying out such procedures, how long such procedures would have taken, how the reference would have been identified or indexed on the website, how the existence of the reference would have been made known to the public, or how an interested person would search for the Ingate reference. Although it is not determinative, in the absence of an Internet archive record, there is no evidence that corroborates Mr. Beer's assertions that it was Ingate's business practice to publish papers after they were written. *Id.*

Mr. Beer's Declaration also fails to address how, or if, the Ingate reference was indexed, or who was responsible for such indexing, such that interested members of the relevant public could obtain the information. For example, Mr. Beer's declaration is silent about whether the website included any search feature or how keywords or other indicia would have been assigned to the Ingate reference to facilitate its identification by an interested person.

Mr. Beer testifies that the Ingate reference is "still available" at: http://www.ingate.com/appnotes/Ingate_Security_Best_Practices.pdf. ("the Link"). Mr. Beer does not state explicitly if "still available" means the Link is the same website address that hosted the Ingate reference before the filing date of the application for the '205 patent. Although the Ingate reference appears to be available by clicking on the Link, Petitioner does not identify any index through which the Link could be found or explain how a person of ordinary skill would become aware of or locate the Link at any time between September 2, 2008 and the present.

Thus, we are not persuaded that Mr. Beer's testimony is sufficient to support the proposition that the Ingate reference was accessible to interested members of the public prior to the priority date of the '205 patent.

As to the Davis Declaration, we agree with Patent Owner that even if the Ingate reference metadata accessed on July 18, 2018 by an attorney preparing the Petition indicates that the Ingate reference is authentic and was created on September 2, 2008, the metadata does not provide sufficient evidence to conclude that the Ingate reference was accessible to the public on any particular date. As discussed above, Mr. Beer's testimony is inadequate to establish public accessibility.

The Krishna Article was published months after the October 22, 2012 filing date of the '205 patent and cannot be relied upon to establish facts concerning the availability of Ingate to interested persons prior to the Krishna article's publication. Footnote 32 of the Krishna article is, at best, circumstantial evidence that the author successfully accessed Ingate at the Link several months before the priority date of the '205 patent. In the absence of testimony from the author of the Krishna article, there is no evidence addressing how the author obtained or located the Link or if Ingate was "**meaningfully** indexed such that an interested artisan exercising reasonable diligence would have found it." *Acceleration Bay*, 908 F.3d at 774 (emphasis in original).

Having considered the testimony of Mr. Beer and Mr. Davis, both alone and together, we find that Petitioner has presented insufficient evidence of public dissemination of the Ingate reference prior to the filing date of the '205 patent, and insufficient evidence that Ingate reference was indexed in a meaningful way. Thus, we conclude that, for purposes of institution, Petitioner has failed to establish that Ingate is a prior art reference.[1]

[1] Nothing in this Decision is inconsistent with our decision in a related case concerning the '205 patent where we instituted trial on Petitioner's challenges to dependent claims 8, 24, and 40 that cite the Ingate reference in combination with other references. *See Cisco v. Centripetal Networks, Inc.*,

ANALYSIS OF PETITIONER'S PRIOR ART CHALLENGES

All of Petitioner's challenges rely on Ingate. As discussed above, Petitioner has failed to demonstrate that Ingate qualifies as a prior art reference. In view of the circumstances, Petitioner has failed to demonstrate a reasonable likelihood it will succeed on any of the challenges presented in the Petition.

ORDER

In consideration of the foregoing, we decline to institute *inter partes* review.

Case IPR2018-01444, slip op. 6, 45 (PTAB Feb. 12, 2019) (Paper 7). In IPR2018-01444 Patent Owner did not challenge the printed publication status of the Ingate reference, opting instead to argue that Petitioner failed to establish that the other references disclose limitations of the claims from which claims 8, 24, and 40 depend. *Id.*

PETITIONER:

Daniel W. McDonald
Jeffrey D. Blake
Kathleen E. Ott
Michael S. Wagner
Christopher C. Davis
MERCHANT & GOULD P.C.
dmcdonald@merchantgould.com
jblake@merchantgould.com
kott@merchantgould.com
mwagner@merchantgould.com
cdavis@merchantgould.com

PATENT OWNER:

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

Bradley C. Wright
BANNER & WITCOFF, LTD.
bwright@bannerwitcoff.com

kis