UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SYMANTEC CORP.,
Petitioner,

v.

FINJAN, INC.,
Patent Owner.

Case IPR2015-01549
Patent 7,930,299 B2

Before THOMAS L. GIANNETTI, RICHARD E. RICE, and
MIRIAM L. QUINN, *Administrative Patent Judges.*

RICE, *Administrative Patent Judge*.

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

I. INTRODUCTION

Petitioner Symantec Corporation filed a Petition (Paper 1, "Pet.") requesting an *inter partes* review of claims 13–18 and 20 ("the challenged claims") of U.S. Patent No. 7,930,299 B2 (Ex. 1001, "the '299 Patent"). Patent Owner Finjan Inc. filed a Preliminary Response (Paper 8, "Prelim.

Resp.”). We have jurisdiction 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). As Petitioner has not shown a reasonable likelihood that it would prevail with respect to at least one of the challenged claims, we do not institute an *inter partes* review with respect to the ’299 Patent.

A. Related Proceedings

We are informed that Petitioner is named as a defendant in a federal district court case involving the ’299 Patent (*Finjan, Inc. v. Symantec Corp.*, Case No. 3:14-cv-02998-RS (N.D. CA)). Pet. 1. We also are informed that Petitioner has filed petitions requesting *inter partes* review of U.S. Patent Nos. 8,141,154 (IPR2015-01547); 8,015,182 (IPR2015-01548); 7,757,289 (IPR2015-01552), and 7,756,996 (IPR2015-01545 and IPR2015-01546). *See id.*

B. The ’299 Patent

The ’299 Patent, titled “System and Method for Appending Security Information to Search Engine Results,” issued April 19, 2011 from U.S. Application No. 11/606,663, filed November 29, 2006, and claims the benefit of U.S. Provisional Application No. 60/740,663, filed November 30, 2005. Ex. 1001, at (54), (45), (21), (22). The ’299 Patent is directed “to a system and method for combining operation of a search engine with operation of a content security filter, so as to provide security assessments for web pages or media content (collectively, web content) located by the search engine.” *Id.* at 2:12–16. The system, according to the Specification, “can integrate [1] a client computer with a web browser, [2] a search engine with a web server, and [3] a content security scanner, *to append* security assessments to search engine results." *Id.* at 2:28–31 (emphasis added). The Specification describes "appending" as follows:

> As used herein, appending refers to inclusion in any way as a part of search engine results, including, for example, in-line with individual search results or at the end of a group of results. This can be embodied in a wide variety of architectures that couple these components in different ways. In some embodiments of the present invention, a database manager can be used to store content inspection results in a database indexed by web page references, such as URLs. In these embodiments, security assessments can be retrieved directly from the database. Use of a database for storing security assessments enables content security scanning to be performed asynchronously, and not necessarily in real-time. Use of a database for storing security assessments also enables content security scanning to be performed pro-actively, and not necessarily reactively.

Id. at 2:32–46.

In an embodiment, the search engine sends the results of a search to the client computer before the search engine receives security assessments of the search results from the content scanner. *Id.* at 7:16–20. After the search engine receives the security assessments from the content scanner, the search engine sends modified search results, with the security assessments appended, to the client computer. *Id.* at 7:20–23. The Specification asserts that this embodiment "eliminates the latency of scanning content in the located web pages and media" by "enabl[ing] a user of the client computer to access the located web pages and media immediately after the search engine locates these pages and pieces of media content, and before the security assessments are available, albeit at the user's risk." *Id.* at 7:28–31. The Specification further states:

> During the stage when the client computer displays the unmodified search results before receiving the security assessments, the client computer may display a notice indicating to the user that the client computer is awaiting the security assessments. Such a notice may be of the form "(Checking for malicious content . . .)."

Id. at 7:32–37.

C. Illustrative Claim

Claims 13 and 20 are independent. Claims 14–18 depend directly or indirectly from claim 13. Claim 13 is illustrative of the claimed subject matter, and is reproduced below:

> 13. A system for appending security information to search engine results, comprising:
>
> a client computer
>
> (i) that issues to a search engine a search request for web content having at least one designated search term,
>
> (ii) that receives from the search engine search results identifying web content that includes the at least one designated search term,
>
> (iii) that generates a search results summary that presents the identified web content,
>
> (iv) that issues to a content scanner a request for assessment of potential security risks of at least a portion of the identified web content,
>
> (v) that receives from the content scanner assessments of potential security risks of the at least a portion of the identified web content,
>
> (vi) that dynamically generates a combined search and security results summary that presents the at least a portion of the identified web content, while some of the assessments of potential security risks have not yet been received from the content scanner,
>
> (vii) *that dynamically updates the combined search and security results summary, by presenting potential security*

> *risks of the presented web content, after the assessments of potential security risks are received from the content scanner*, and
>
> (viii) that displays a warning of potential risk, subsequent to presenting the at least a portion of the identified web content and prior to dynamically updating the combined search and security results summary; and
>
> a content scanner communicatively coupled with the client computer that receives and responds to the issued request to assess potential security risks of the at least a portion of the identified web content.

Id. at 13:60–14:22 (emphasis added).

D. The Asserted Grounds

Petitioner challenges claims 13–18 and 20 of the ’299 Patent on the following grounds (Pet. 4):

References	**Basis**	**Claims Challenged**
Dixon[1]	§ 102	13–18 and 20
Rowan[2] and Dixon	§ 103(a)	13–18 and 20

In addition to Dixon and Rowan, Petitioner relies on the Declaration of

[1] U.S. Patent No. 8,296,664 B2 (Ex. 1004) issued October 23, 2012, from U.S. Patent Application 11/837,067 filed August 10, 2007, which is a continuation of U.S. Patent Application No. 11/342,250 filed January 26, 2006, and claims the benefit of U.S. Provisional Patent Applications Nos. 60/677,786 filed May 3, 2005 (Ex. 1005) and 60/691,349 filed June 16, 2005 (Ex. 1006).

[2] U.S. Patent No. 7,694,135 B2 (Ex. 1007) issued April 6, 2010, from U.S. Patent Application No. 11/184,049 filed July 18, 2005, and claims the benefit of U.S. Provisional Patent Applications Nos. 60/588,570 filed July 16, 2004 and 60/633,464 filed December 6, 2004.

Somesh Jha, Ph.D. Ex. 1002.

II. ANALYSIS

We turn now to Petitioner's asserted grounds of unpatentability to determine whether Petitioner has met the threshold standard of 35 U.S.C. § 314(a) for instituting review.

A. Claim Construction

In an *inter partes* review, the Board gives claim terms in an unexpired patent their broadest reasonable interpretation in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *see also In re Cuozzo Speed Techs., LLC,* 793 F.3d 1268, 1278, 1279 (Fed. Cir. 2015). Under the broadest reasonable interpretation standard, and absent any special definition, claim terms 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. *In re Translogic Tech., Inc.,* 504 F.3d 1249, 1257 (Fed. Cir. 2007). Any special definition for a claim term must be set forth with reasonable clarity, deliberateness, and precision. *In re Paulsen,* 30 F.3d 1475, 1480 (Fed. Cir. 1994).

In this case, Petitioner proposes an express claim construction for the phrase "dynamically updates the combined search and security results summary." Pet. 11–15. Patent Owner opposes Petitioner's proposed claim construction, but itself does not propose an express construction. Prelim. Resp. 9–10. We do not resolve this claim construction dispute between the parties, however, because none of our determinations regarding Petitioner's proposed grounds of unpatentability requires us to interpret expressly the phrase "dynamically updates the combined search and security results summary," or any other claim term.

B. Asserted Anticipation by Dixon

1. Introduction

In an *inter partes* review, anticipation must be based on prior art consisting of patents or printed publications. 35 U.S.C. § 311(b). Anticipation requires all features of a claim to be disclosed within a single reference. *Finisar Corp. v. DirecTV Group, Inc.*, 523 F.3d 1323, 1334 (Fed. Cir. 2008) (holding that, for anticipation, "a single prior art reference must expressly or inherently disclose each claim limitation").

In arguing that claims 13–18 and 20 are anticipated by Dixon (Ex. 1004), Petitioner asserts that certain limitations of independent claim 20 overlap the corresponding limitations of independent claim 13, including the following limitation, which Petitioner designates as "13[H]": "that dynamically updates the combined search and security results summary, by presenting potential security risks of the presented web content, after the assessments of potential security risks are received from the content scanner." *See* Pet. 7–10, 23–27, 34. Below, we focus our anticipation analysis on limitation 13[H].

2. Overview of Dixon

Dixon relates to systems and methods for providing Web reputational services. Ex. 1004, 1:63–64. Figure 4 of Dixon, reproduced below, illustrates reputation information process 400 involving Internet requests 402. *Id.* at 17:61–62.

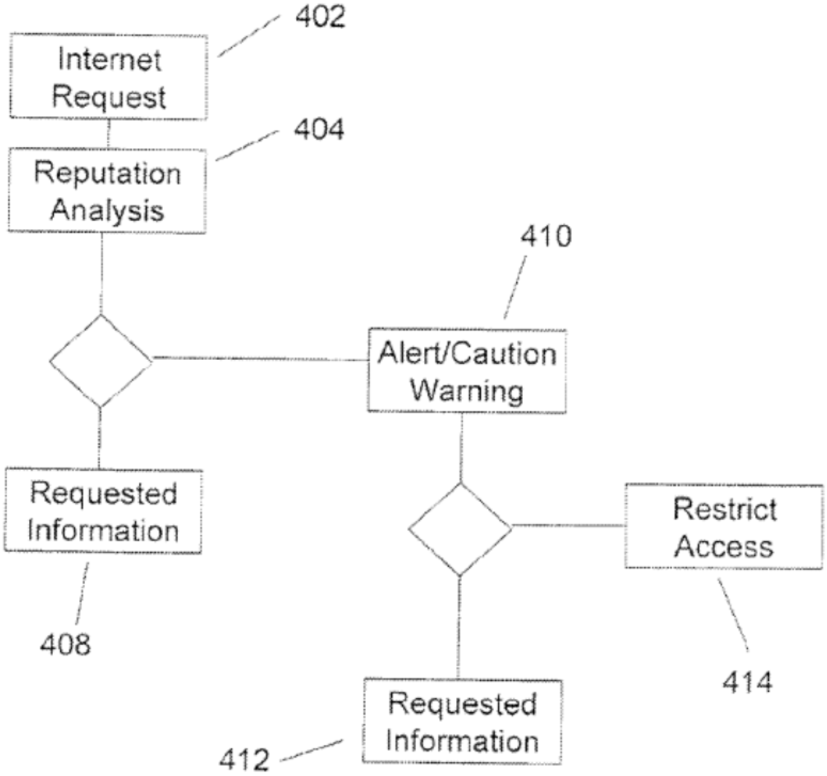

Fig. 4

As shown in Figure 4, reputation analyis 404 is performed in connection with Internet request 402 (e.g., a search request or URL address request). *Id.* at 17:62–66. If Internet request 402 involves a search term or search phrase, for example, reputation analysis 404 may be performed on the results produced. *Id.* at 18:3–5. After the reputation analysis is conducted, a decision may be made either to provide the search results (requested information 408) and/or "to provide an alert, caution, warning, recommendation, or other reputation service" (alert/caution warning 410). *Id.* at 18:6–25. Following the alert/caution warning, the user may be presented with an option to receive the requested information, or access to the information may be restricted. *Id.* at 18:25–29. As disclosed in Dixon, "[a] Web reputation service may involve a real-time database query interface for looking up the reputation of Web sites, programs, Web forms, and other such content." *Id.* at 20:14–16.

3. Analysis

Petitioner contends that Dixon discloses all limitations of claim 13, including 13[H], which requires "dynamically updat[ing] the combined search and security results summary, by presenting potential security risks of the presented web content, after the assessments of potential security risks are received from the content scanner." Pet. 17–29. With respect to this dynamically updating requirement, Petitioner argues that "Dixon's reputation service can 'iteratively update' reputations for sites that 'did not otherwise have a known reputation,'" based on the known reputations of other sites to which they are linked. *Id.* at 24 (citing Ex. 1004, 44:41–52). Petitioner cites Dixon's disclosure that each site is represented by a node in a graph, and each site/node's reputation can be adjusted using then-existing graph theory algorithms. *Id.* (citing Ex. 1004, 44:41–44, 46–50).

Petitioner further argues that "the combined search and security results summary initially generated by Dixon is dynamically updated given that Dixon discloses such iterative updating of site reputations." *Id.* (citing Ex. 1002 ¶¶ 78–79). And, "[a]s these additional reputation assessments are received from the reputation host (*i.e.*, content scanner), the potential security risks for the corresponding sites are presented *at the client computer*." *Id.* (emphasis added; citing Ex. 1002 ¶ 80 and Ex. 1004, Abstract).

We are not persuaded, however, that merely receiving additional reputation assessments at the client computer, as disclosed in Dixon, meets the claim requirement for "dynamically updat[ing] the combined search and security results summary, *by presenting potential security risks of the presented web content, after the assessments of potential security risks are received from the content scanner*." *See* Ex. 1001, 14:10–14 (emphasis added). The language of this limitation, itself, distinguishes "presenting" potential security risks from "receiv[ing]" assessments of potential security risks, by reciting that "presenting" occurs after the assessments are "received." *See id.* Petitioner has not shown sufficiently that Dixon discloses "presenting" potential security risks after the assessments of potential security risks are received, as required by the claims. Accordingly, we agree with Patent Owner that "[i]t simply does not follow from Dixon's disclosure of iteratively updating nodes based on neighboring nodes' reputations that Dixon teaches dynamically updating a combined search and results summary." Prelim. Resp. 15.

We also agree with Patent Owner that presenting search results, in real-time utilizing a database query, is different from updating an initial summary of search and security results by presenting newly-assessed, potential security risks:

> In fact the *only* evidence relied upon in the Petition to support this conclusion is the Abstract's disclosure that "an indicia of risk associated with the search results is presented, in real-time, within the graphical user interface." *See* Petition at 24. However, . . . this only means that disclosing Dixon's "search engine may return search results that are augmented with the reputation of URLs appearing in the results based on a *real time database query*." Dixon at 20:7–10. That is, if there is a reputation entry in the database for a particular URL, it will be included in the search results in real time. It does not mean that the presentation of the search results will ever be dynamically updated.

Id. at 15. As Patent Owner argues, the reference in Dixon's Abstract to a graphical user interface for presenting an indicia of risk in real-time is described more fully in Dixon as a real-time database query interface for looking up the reputation of Web sites, programs, Web forms, and other such content. Ex. 1004, Abstract, 20:14–16. Petitioner has not shown sufficiently that Dixon discloses utilizing the real-time database query interface, or any other means, for dynamically updating a combined search and security results summary, as required by the claims.

Moreover, we are not persuaded by Dr. Jha's testimony that a POSITA would have understood Dixon to disclose the dynamically updating requirement. *See* Ex. 1002 ¶¶ 78–83. Dr. Jha testifies, for example, that "once an 'Unknown' site has been iteratively updated to indicate whether it is safe or not, it will be provided to the client computer so as to be added in the presentation of the search results and reputation information." *Id.* ¶ 78. Dr. Jha does not explain, however, where Dixon discloses "presenting" the potential security risks after the new risk assessments are received, as required by the claims. Apparently recognizing this weakness, Dr. Jha further opines that a POSITA "would have clearly recognized that Dixon's disclosure requires the reputation information to be updated in order to ensure that a user can safely interact with the Internet." *Id.* This testimony is conclusory, in particular, because it does not explain sufficiently what in Dixon's disclosure would support that conclusion.

Also unpersuasive is Dr. Jha's assessment of the disclosure in Dixons's provisional applications (Exhibits 2005 and 2006). *See* Ex. 1002 ¶ 78. The applications, at best, support the contention that Dixon's database is updated in the background to include previously-unassessed sites in the search request results. *See id.* ¶¶ 76 (citing, in footnote 13, Exhibits 1005 and 1006), 78. That is, the updates are of the database reputation, but Dr. Jha has not shown sufficiently that Dixon discloses updating an initial presentation of search and security results to reflect the new reputation assessment performed in the background. For example, Exhibit 1006 teaches that "[p]erformance of loading and viewing web pages must not be affected by the background operation of checking each URL against the InfiniTrust database." Ex. 1006, 34:2–3.

For these reasons, we determine that Petitioner has *not* demonstrated a reasonable likelihood of prevailing with respect to its challenge to claim 13 and dependent claims 14–18 as anticipated by Dixon. As Petitioner asserts that independent claim 20, like independent claim 13, requires limitation [H] (*see* Pet. 34), we also determine that Petitioner has *not* demonstrated a reasonable likelihood of prevailing with respect to its challenge to claim 20 as anticipated by Dixon.

C. Asserted Obviousness over Rowan and Dixon

1. Introduction

In an *inter partes* review, obviousness must be based on prior art consisting of patents or printed publications. 35 U.S.C. § 311(b). A claim is unpatentable for obviousness under 35 U.S.C. § 103(a) if the differences between the subject matter sought to be patented 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 ("POSA") to which the subject matter pertains. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). A patent claim composed of several elements, however, is not proved obvious merely by demonstrating that each of its elements was known, independently, in the prior art. *Id.* at 418. In analyzing the obviousness of a combination of prior art elements, it can be important to identify a reason that would have prompted one of skill in the art to combine the elements in the way the claimed invention does. *Id.* A precise teaching directed to the specific subject matter of a challenged claim is not necessary to establish obviousness. *Id.* Rather, "any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *Id.* at 420. The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations, when in evidence. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Here, Petitioner defines the level of skill in the art as follows:

> A [person of ordinary skill in the art ("POSITA")] at the time of the alleged invention of the '299 patent would generally have 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 experience in the fields of web-related technologies, computer security or equivalent work experience. Additional graduate education might substitute for experience, while significant experience in the field of computer programming, web-related technologies, and/or malicious code might substitute for formal education. Jha, ¶26. This person would have been capable of understanding the '299 patent and applying the prior art references discussed herein. Jha, ¶27.

Pet. 10–11. Patent Owner does not dispute Petitioner's definition of the level of skill in the art, with which we agree, and we adopt it for purposes of our Decision.

Petitioner challenges claims 13–18 and 20 as obvious over Rowan and Dixon. Below, we focus our analysis of Petitioner's obviousness challenge on limitation [H], which, as discussed above and asserted by Petitioner, all of the challenged claims require.

2. *Overview of Rowan*

Rowan relates to a service or system that allows a user to perform a search on an address and to establish a report on the trustworthiness of the address. Ex. 1007, 2:38–46. As disclosed in Rowan:

> The system can provide trustworthiness report information to users while viewing search results within a standard search engine format. The user can access the trustworthiness report information and backup information directly in the search results and does not have to travel to the actual link.

Id. at 3:4–9.

Rowan discloses, in reference to the embodiment depicted in Figures 9(a)–9(c), that a search engine could be used to provide results in response to a query, such as links on a search results page, and the service could provide, automatically, a trustworthiness report or summary report for each of the addresses that are on the search page. *Id.* at 6:10–16. The summary report "could take the form of an icon next to each link provided by the search to indicate that the location is verified, not verified (as in FIG. 9(c)), questionable, or some other indication." *Id.* at 6:17–20.

Rowan also discloses a toolbar embodiment that can use the service. *Id.* at 9:9. The toolbar can display an indicator, such as a "green" indicator indicating the location is trustworthy, a yellow indicator indicating that the location should be accessed with caution, and a red indicator indicating that the location is untrustworthy. *Id.* at 9:11‒16. "A waiting indicator indicates that the source is trying to locate the site, and that the user should click on that location again." *Id.* at 9:16‒18. By clicking on the indicator, the user can obtain more information about the location's trust rating. *Id.* at 6:19–20.

Rowan additionally discloses that to reduce the number of accesses to the service and to provide greater efficiency, the trustworthiness level of the site can be cached on the user's computer. *Id.* at 11:7‒10. The service can provide information to the user indicating a trustworthiness level and a period of time for which the site may be considered to have that same level. *Id.* at 11:10–14. The period of time may vary depending on the site. For example, in the case of a site with significant safeguards, the period could be expressed in terms of a number of hours. *Id.* at 11:15–17. Rowan states: "The user is thus caching the verification status and the trustworthiness of the site for some period of time, and the period of time can be controlled or adjusted based on a set of rules." *Id.* at 11:25–28.

3. Analysis

Petitioner contends that the combination of Rowan and Dixon discloses limitation [H]. Pet. 46‒50. In support of its contention, Petitioner relies on Rowan's disclosure of updating a trustworthiness report for a site, after initially presenting a waiting indicator that advises the user to click again on that site at some unspecified future time. *Id.* For example, Petitioner argues:

> Indeed, Rowan's service initially computes a trustworthiness score such as a "'zero' or 'no trust' score," or even a "yellow not verified score." Rowan, 4:41–48. In such cases, Rowan will place "the location name . . . in a search queue and the service will access the site directly and *perform an updated trustworthiness report*" (emphasis added). Rowan, 7:64–66. Specifically, "if no match is found, the location name is placed in the search queue, and a waiting indicator is returned to the requesting application." Rowan, 8:3–8. Rowan's "waiting indicator indicates that the source is trying to locate the site, and the user should click on that location again [to obtain an updated trustworthiness report.]" Rowan, 9:16–18. As a result, the user "could check with the service with each access each time to get a score or indication of the trustworthiness of that site (*e.g.*, "Verified", "Not Verified," or "Warning")." Rowan, 11:1–3. Thus, once Rowan's service locates the site, it will dynamically update the presentation to the user such that the user will be provided with an updated trustworthiness report. Jha, ¶114.

Id. at 46–47. Petitioner also asserts that Rowan caches the trustworthiness levels for some period of time and that, once the period lapses, "the cache would be cleared and the service would provide an updated trustworthiness score to the user." *Id.* at 47 (citing Ex. 1002 ¶ 114). Petitioner combines the teachings of Rowan and Dixon (discussed *supra* in Section II.B.3) as follows:

> Because Rowan's service presents a waiting indicator (*e.g.*, Warning) to the user and, once a period of time lapses (and certain reputations for unknown [s]ites are computed by Dixon's service), an updated trustworthiness score for such sites is provided along with security assessments from Dixon's service, Rowan in view of Dixon discloses "dynamically updating the combined search and security results summary" as required by the claim.

Id. at 48 (citing Ex. 1002 ¶¶ 115–116).

We are not persuaded that the asserted combination of Rowan and Dixon ("Rowan/Dixon") teaches limitation [H]. This limitation recites "dynamically updat[ing] the combined search and security results summary, *by presenting potential security risks of the presented web content, after the assessments of potential security risks are received from the content scanner*." *See* Ex. 1001, 14:10–14 (emphasis added). As discussed above, the language of this limitation, itself, distinguishes "presenting" potential security risks from "receiv[ing]" the assessments of potential security risks, by reciting that "presenting" occurs after the assessments are "received." *See id.* Petitioner has not shown sufficiently that Rowan/Dixon teaches "presenting" potential security risks after the assessments of potential security risks are received, as required by the claims.

Although Rowan teaches that a new trustworthiness report may be retrieved by a user at some unspecified future time, we are not persuaded that such user intervention meets the "presenting" aspect of limitation [H]. For example, as Patent Owner points out, and we agree, when a "waiting indicator" is provided on Rowan's toolbar, the indicator "indicates that the source is trying to locate the site, and *the user should click on that location again*." Prelim. Resp. 18 (quoting Ex. 1007, 9:16–18). Although a new trustworthiness report may be retrieved if the user clicks on the location at a later time, Petitioner does not explain whether or how the user of Rowan's system would know either: (i) when to click again on the site; or (ii) what type of trustworthiness report would be retrieved by doing so. In particular, Petitioner has not cited any evidence to show that the "waiting indicator" changes or any other updating to the initial presentation occurs, once the new trustworthiness report becomes available.

Petitioner cites paragraph 114 of the Jha Declaration to support its contention that once Rowan's service updates the trustworthiness report or trustworthiness score, it will dynamically update the presentation to the user. Pet. 47 (citing Ex. 1002 ¶ 114). The cited paragraph in the Jha Declaration, however, provides no factual support for this contention. Accordingly, we are not persuaded by Dr. Jha's testimony that Rowan teaches "presenting" potential security risks after new risk assessments are received. Nor does Petitioner or Dr. Jha explain sufficiently how combining Dixon with Rowan would have remedied this deficiency in Rowan.[3] *See* Pet. 46–50; Ex. 1002 ¶¶ 114–119. Accordingly, we are not persuaded that Rowan/Dixon teaches "presenting" potential security risks after new risk assessments are received, as required by limitation [H].

For these reasons, we determine that Petitioner has *not* demonstrated a reasonable likelihood of prevailing with respect to its challenge to claims 13–18 and 20 as obvious over Rowan and Dixon.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner has not established a reasonable likelihood of prevailing on its challenges to claims 13–18 and 20 of the '299 Patent.

[3] Indeed, as discussed *supra* in Section II.B.3, we are not persuaded that Dixon, any more than Rowan, discloses "presenting" potential security risks after new risk assessments are received, as required by the claims.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that Petitioner's Petition for an *inter partes* review of claims 13–18 and 20 of U.S. Patent No. 7,930,299 B2 as (i) anticipated by Dixon and (ii) obvious over Rowan and Dixon is *denied*, and no *inter partes* review will be instituted pursuant to 35 U.S.C. § 314 as to any claim of that patent on any of the grounds of unpatentability alleged by Petitioner in the Petition.

PETITIONER:

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

PATENT OWNER:

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

Michael Kim
FINJAN INC.
mkim@finjan.com