

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORCEPOINT LLC,
Petitioner,

v.

OPEN TEXT INC.,
Patent Owner.

IPR2023-00784
Patent 8,438,386 B2

Before JUSTIN T. ARBES, BARBARA A. PARVIS, and
MICHELLE N. WORMMEESTER, *Administrative Patent Judges*.

PARVIS, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. *Background*

Forcepoint LLC (“Petitioner”) filed a Petition (Paper 2 (“Pet.”)) requesting an *inter partes* review of claims 1–13, 15, 16, and 18 (“challenged claims”) of U.S. Patent No. 8,438,386 B2 (Ex. 1001, “the ’386 patent”) pursuant to 35 U.S.C. §§ 311–319, along with a supporting Declaration of Michael T. Goodrich, Ph.D. (Ex. 1002). Open Text Inc. (“Patent Owner”) filed a Preliminary Response (Paper 6 (“Prelim. Resp.”)), along with the supporting Declaration of Alessandro Orso, Ph.D. (Ex. 2001).

We have authority to determine whether to institute review under 35 U.S.C. § 314 and 37 C.F.R. § 42.4. We may institute an *inter partes* review if “the information presented in the petition . . . and any response . . . 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.” 35 U.S.C. § 314(a). For the reasons provided below, we determine that Petitioner has not demonstrated a reasonable likelihood that it will prevail in showing the unpatentability of at least one challenged claim. Accordingly, we do not institute *inter partes* review.

B. *Real Parties-in-Interest*

Petitioner identifies itself, Forcepoint LLC, as the real party-in-interest. Pet. 1, 75.

Patent Owner identifies itself, Open Text Inc., and Webroot LLC as the real parties-in-interest. Paper 4, 1. Patent Owner also states “[o]ut of an abundance of caution, Patent Owner further identifies the following affiliates: Carbonite, LLC; Open Text Corporation; and Open Text Holdings, Inc.” *Id.*

C. Related Matters

The parties indicate that the '386 patent is the subject of *Webroot, Inc. v. Forcepoint LLC*, No. 6:22-cv-00342 (W.D. Tex.), which has been consolidated with *Webroot, Inc. v. AO Kaspersky Lab*, No. 6:22-cv-00243 (W.D. Tex.) (“the district court case”). *See* Pet. 75; Paper 4, 1. Patent Owner also cites various other *inter partes* review proceedings involving unrelated patents at issue in the district court case. Paper 4, 1–2. Petitioner filed a petition challenging an unrelated patent in IPR2023-00786.

D. The '386 Patent

The '386 patent is titled “System and Method for Developing a Risk Profile for an Internet Service.” Ex. 1001, code (54). The '386 patent relates to “developing a risk profile for an Internet resource by generating a reputation index, based on attributes of the resource collectively referred to as the reputation vector of the resource.” *Id.* at 1:23–28.

System 20 for controlling access to an Internet service is shown in Figure 1, reproduced below. Ex. 1001, 10:1–2.

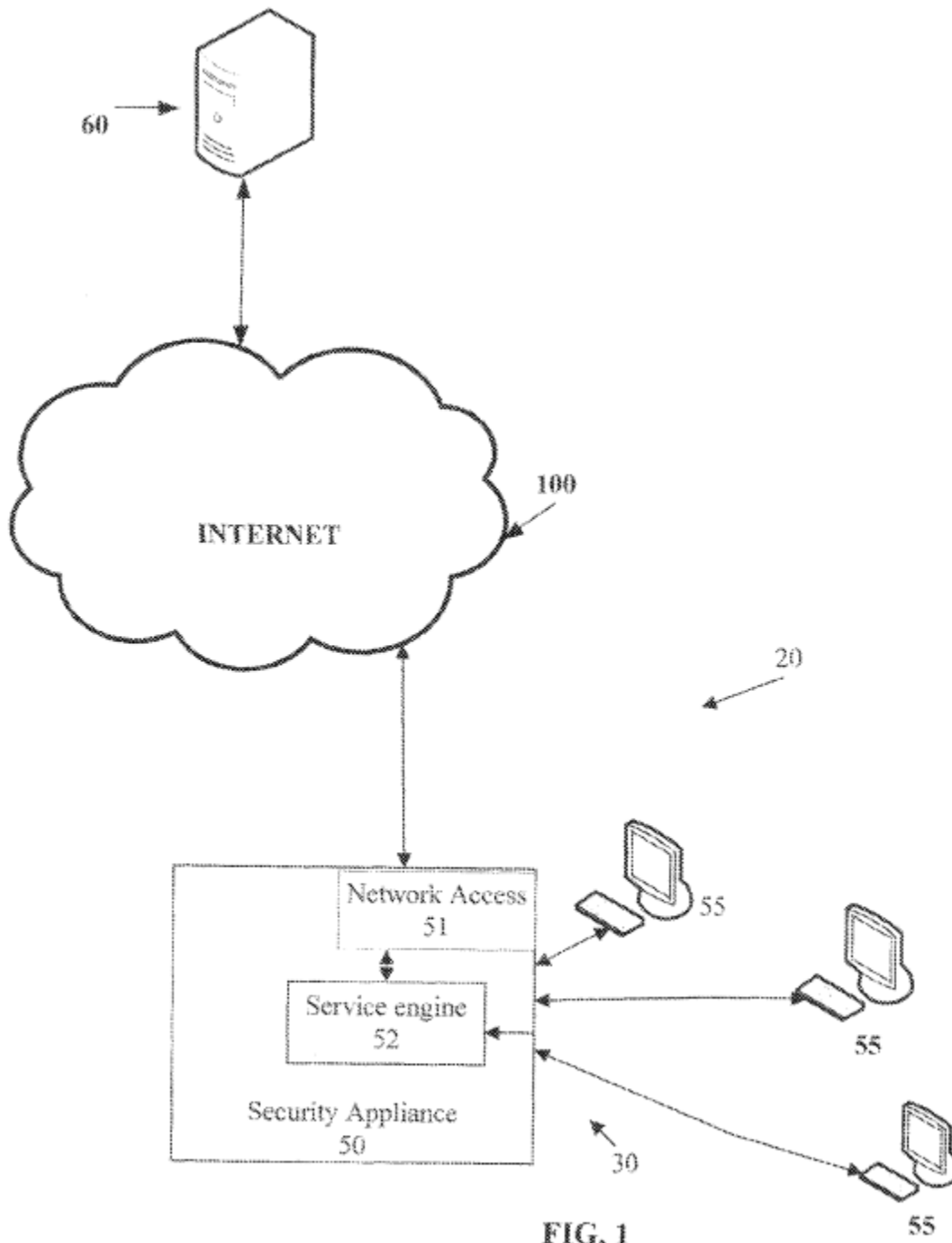


FIG. 1

Figure 1, above, shows local area network 30, Internet 100, and an Internet resource located at remote server 60. Ex. 1001, 4:34–38, 10:1–4. The Internet resource is preferably a Web site. *Id.* at 10:4–5. Network 30 comprises security appliance 50 and plurality of client-side devices 55. *Id.* at

10:5–7. Security appliance 50 comprises network access 51 for permitting access to Internet 100 from local area network 30, and service engine 52 for determining if a requested Web site has a reputation index that meets a threshold established for local area network 30. *Id.* at 10:12–16.

A reputation index is calculated from a reputation vector which preferably includes a plurality of factors for the Web site. *Id.* at 10:23–25. If the reputation index is not above a threshold, then access to the Web site is denied. *Id.* at 10:33–35. If the reputation index for the Web site is above the threshold, then access to the Web site by the client-side device is permitted by the security appliance. *Id.* at 10:37–41.

E. Illustrative Claim

Petitioner challenges claims 1–13, 15, 16, and 18 of the '386 patent. Pet. 1. Claims 1, 7, 11, and 13 are independent claims. Independent claim 1, reproduced below, is illustrative of the claimed subject matter.

1. [1[P]] A method for controlling access to an Internet resource, the method comprising:

[1[a]] transmitting a request for an Internet resource from an Internet-enabled client application from a client-side device of a local area network, the Internet resource residing at a first server;

[1[b]] receiving the request for the Internet resource at a security appliance of the local area network prior to transmission of the request over the Internet;

[1[c1]] determining if a reputation index for the Internet resource is at or above a threshold value established for the local area network, [1[c2]] the reputation index generated from a reputation vector for the Internet resource, the reputation vector comprising a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location, [1[c3]] wherein the location factor of the plurality of factors for the reputation vector comprises

two or more of: country of domain registration, country of service hosting and country of an internet protocol address block, [1[c4]] wherein the legitimacy factor of the plurality of factors for the reputation vector comprises two or more of: age of a domain registration, popularity rank, internet protocol address, number of hosts, top-level domain, and [1[c5]] wherein the behavior factor of the plurality of factors for the reputation vector comprises at least one of: plurality of run-time behaviors, script block count, picture count, immediate redirect and response latency; and

[1[d]] transmitting a decision transmission to the Internet-enabled client application of the client-side device, the decision transmission allowing or denying access to the Internet resource.

Ex. 1001, 15:65–16:30.¹

F. Evidence

Petitioner relies on the references summarized in the table below.

Pet. 3.

Name	Reference	Exhibit
Hubbard-495	U.S. Patent No. 9,654,495 B2, filed Feb. 28, 2007, issued May 16, 2017	1004
Hubbard-174	U.S. Patent No. 8,015,174 B2, filed Feb. 28, 2007, issued Sept. 6, 2011	1005
Alperovitch	U.S. Patent Application Publication No. 2008/0175266 A1, filed Jan. 24, 2007, published July 24, 2008	1006

G. Asserted Grounds

Petitioner asserts that the challenged claims are unpatentable on the following grounds (Pet. 3):

¹ We include bracketed annotations provided by Petitioner for ease of analysis. *See* Pet. 18–35.

Claims Challenged	35 U.S.C. §	References/Basis
1–13, 15, 16, 18	§ 103(a) ²	Hubbard-495, Hubbard-174
1–13, 15, 16, 18	§ 103(a)	Hubbard-495, Hubbard-174, Alperovitch

II. ANALYSIS

A. *Legal Standards*

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) (quoting 35 U.S.C. § 103(a) (2006)). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of nonobviousness, i.e., secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. *Level of Ordinary Skill in the Art*

Petitioner argues that at the time of the ’386 patent, a person of ordinary skill in the art would have had “at least a four-year undergraduate

² The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. § 103. Because the challenged claims of the ’386 patent have an effective filing date before the effective date of the applicable AIA amendment, we refer to the pre-AIA version of 35 U.S.C. § 103. Pet. 3; Ex. 1001, code (22). Our analysis would not change under the AIA version of § 103.

degree in computer science or a closely related field and at least two years of experience in the field of computer and network security,” where “[a]dditional education could substitute for professional experience and vice versa.” Pet. 6–7 (citing Ex. 1002 ¶¶ 22–25). Patent Owner argues that a person of ordinary skill in the art instead would have had “a bachelor’s degree in an accredited program of electrical engineering, computer engineering, or computer science, or a similar discipline, and have [had] 2–3 years of practical work experience in the general fields of electrical engineering, computer science, networking, communications, and/or device and network security,” where “[m]ore advanced degrees and/or training in a related discipline can compensate for shorter work experience.” Prelim. Resp. 28; *see* Ex. 2001 ¶ 50. The parties’ proposed definitions have only minor differences (e.g., at least two years of work experience versus 2–3 years). For purposes of this Decision, we adopt Petitioner’s proposed definition of the level of ordinary skill in the art, except that we eliminate the term “at least” to eliminate vagueness as to the amount of education and practical experience. We note, however, that our conclusions herein would be the same regardless of which party’s definition is used.

C. Claim Construction

We interpret the challenged claims

using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

37 C.F.R. § 42.100(b). Under this standard, the words of a claim generally are given their “ordinary and customary meaning,” which is the meaning the

term would have to a person of ordinary skill at the time of the invention, in the context of the entire patent including the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc).

Petitioner does not propose express constructions for any claim terms. Pet. 7. Patent Owner proposes a construction for the term “security history.” Prelim. Resp. 26–28. More specifically, Patent Owner argues “[c]onsistent with its plain and ordinary meaning, ‘security history’ refers to ‘a history of security events for an internet resource.’” *Id.* at 27.

“In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).³ We begin with the claim language. Independent claims 1, 7, and 13 each recite “the reputation vector comprising a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location.” Claim 11 includes a similar recitation.

The dispute between the parties turns on whether the term “security history” is a factor distinct from other factors including “legitimacy” and “behavior.” Prelim. Resp. 39 (arguing that prior art teachings “at most, relate to ‘legitimacy’ of an internet resource, which *all challenged claims recite as a factor distinct from* the ‘security history’ factor” (emphasis added)), 44 (arguing that prior art teachings “at best might have suggested the ‘behavior’ factor for assessing reputation, but not the *separate* ‘security history’ factor”

³ Neither party directs us to the prosecution history of the ’386 patent with respect to interpreting “security history.”

(emphasis added)). We recognize that “[d]ifferent claim terms are presumed to have different meanings.” *SimpleAir, Inc. v. Sony Ericsson Mobile Commc’ns*, 820 F.3d 419, 431 (Fed. Cir. 2016); *Phillips*, 415 F.3d at 1314. The challenged claims recite “a plurality of factors” that includes “security history” in a list with the “legitimacy” and “behavior” factors. Each of “security history,” “legitimacy,” and “behavior” are different words. We discern nothing in the claim language suggesting that the presumption that these different words carry different meanings is overcome.

Additionally, each of the independent claims uses the term “comprising.” For instance, independent claims 1, 7, and 13 each recite “the reputation vector comprising a plurality of factors for the Internet resource *comprising* security history, legitimacy, behavior, associations and location” (emphasis added). Claim 11 includes a similar recitation. “Comprising” is a term of art used in claim language, which means that the named elements are essential, but other elements also may be included to constitute additional components within the scope of the claim. *Genentech, Inc. v. Chiron Corp.*, 112 F.3d 495, 501 (Fed. Cir. 1997). We find on the current record that “security history” is a named element that is essential.

The ’386 patent Specification also supports Patent Owner’s position that the term “security history” is a factor distinct from other factors including “legitimacy” and “behavior.” Prelim. Resp. 39, 44. In particular, the ’386 patent Specification describes the following:

The reputation of an Internet resource is preferably determined by security, legitimacy, behavior, geographic location, associations and additional factors. Legitimacy is determined by the top-level domain, the investment in the Internet resource (virtual hosting with non-affiliated sites, multiple hosting and SSL security), the traffic volume, the

category age and the popularity rank. Legitimacy is also preferably determined by any or all of the following: the consistency between the registering and hosting city region or country; and city, region or country associated with the IP address. Behaviors include the use of popup ads, browser hijacking and the use of auto-redirecting. Associations include the number of sites linking into the site, the reputations of the linked in sites and the reputations of the linked-to sites. The geographic location includes the hosting country, the registration country, the region and the city. The geographic location also preferably includes the consistency between the registering and hosting country and the country associated with the IP address.

Ex. 1001, 9:8–27.

Similar to the claim language, the '386 patent Specification lists “security” as separate from “legitimacy, behavior, geographic location, associations and additional factors.” *Id.* at 9:8–11. As is discussed below, the '386 patent describes an exemplary security event as a “security breach” (*id.* at 8:63–65) and describes security trends as a number of “malware infections” (*id.* at 12:8–9). The '386 patent provides different examples of the other factors, such as “legitimacy” and “behavior” showing the other factors are distinct. *Id.* at 9:8–27. For instance, in the portion of the '386 patent reproduced above, “legitimacy” is described as being determined based on “SSL security” and “behavior” is described as including “the use of popup ads, browser hijacking and the use of auto-redirecting.” *Id.* at 9:10–20.

Although the parties' dispute turns on the discussion above, as an additional reason for our determinations herein, the intrinsic record supports Patent Owner's proposed construction. For instance, Patent Owner's proposal that “security history” refers to “a history of security events . . .” is supported by the language in the term itself, specifically that the term

“security history” recites “security” and “history.” Patent Owner’s proposal that the “security history” is “for an internet resource” is supported by the requirement in independent claims 1, 7, and 13 that “the reputation vector” comprises “a plurality of factors for the *Internet resource*” (emphasis added). Claim 11 similarly recites “a reputation vector for the Internet resource comprising security history” and other factors.

The Specification also supports Patent Owner’s position. Patent Owner’s proposal that “security history” refers to “a history of security events” is supported by description in the ’386 patent Specification that “reputation is built up *over time*” and that “[r]eputation can be lost, or become ‘bad’, *over a period of time*.” Ex. 1001, 8:58–61 (emphases added) (quoted in Prelim. Resp. 27). Patent Owner’s proposal also is supported by description in the ’386 patent Specification that reputation is lowered “with repeated security events.” *Id.* at 8:61–62 (quoted in Prelim. Resp. 27); *see also id.* at 8:63–67 (quoted in Prelim. Resp. 27) (describing that a “single security breach” does not “dramatically lower the reputation of a site,” but “[r]epeated occurrences over time” will “destroy the reputation of the site”). The ’386 patent describes an exemplary security event as a “security breach (the site gets hacked and is a danger to visitors).” *Id.* at 8:63–65. The ’386 patent also describes that a “Security Trend” is the “[n]umber of malware infections in past 12 months” and that “Total Security” is the “[t]otal number of malware infections known.” *Id.* at 12:8–9.

Patent Owner’s proposal that the “security history” is “for an internet resource” is supported by description in the ’386 patent Specification that its invention “focuses on the reputation of a Web site, or *any Internet-based service or resource*.” *Id.* at 4:36–38 (emphases added). Consistently, the

'386 patent further describes that the “reputation incorporates many factors that are relevant to the overall safety of *visiting a site*.” *Id.* at 4:38–39 (emphasis added).

For the reasons given, we determine “security history” means “a history of security events for an internet resource,” consistent with Patent Owner’s proposed construction. Prelim. Resp. 27–28. We further determine that the term “security history” is a factor distinct from other factors including “legitimacy” and “behavior.” We need not make further determinations regarding claim construction to resolve the disputes between the parties. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. Asserted Obviousness of Claims 1–13, 15, 16, and 18

Petitioner argues that claims 1–13, 15, 16, and 18 are unpatentable as obvious over Hubbard-495 and Hubbard-174 or, alternatively, Hubbard-495, Hubbard-174, and Alperovitch. Pet. 13–75.

1. Overview of Hubbard-495 (Ex. 1004)

Hubbard-495 is titled “System and Method of Analyzing Web Addresses.” Ex. 1004, code (54). Hubbard-495 describes “a method of controlling access to web content.” *Id.* at 2:33–34. Figure 1, reproduced below, provides a top-level illustration of an exemplary system for controlling access to web content. *Id.* at 2:33–34, 4:38–49.

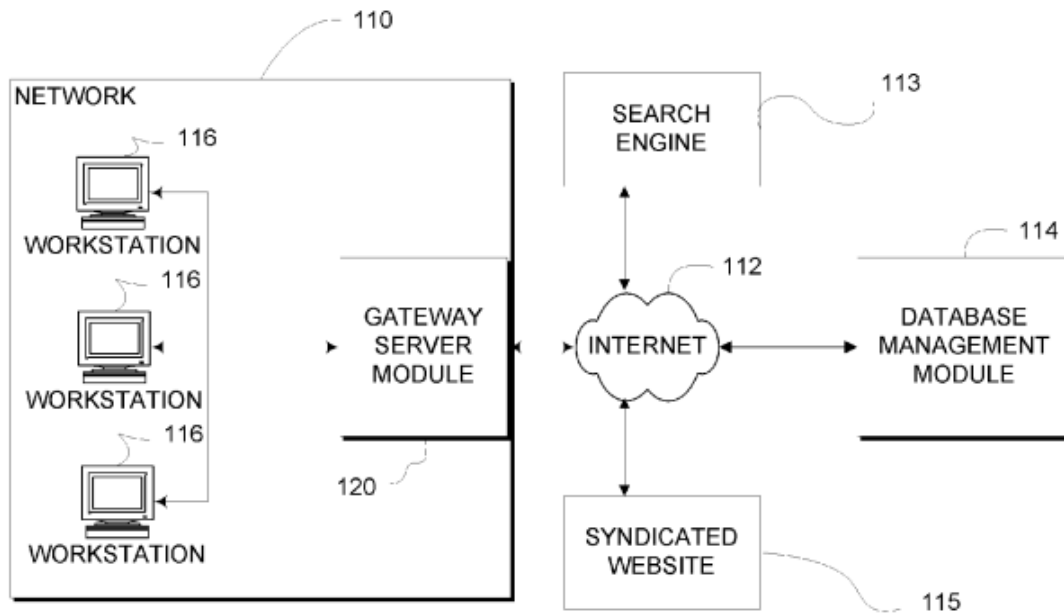


Figure 1 shows a system including network 110 and Internet 112. Ex. 1004, 4:38, 4:51–54, Fig. 1. Network 110 includes workstations 116 that are in communication with gateway server module 120. *Id.* at 4:41–42, 4:50–51. Workstations 116 are client computers that are loaded with operating systems that allow them to use the network through various software modules such as web browsers. *Id.* at 4:42–49. Gateway server module 120 is at the edge of network 110 so that traffic sent to and from Internet 112 may pass through it on its way into or out of network 110. *Id.* at 4:50–54. Workstations 116 are in communication with one or more search engines 113 and/or one or more syndicated web sites 115 via Internet 112. *Id.* at 5:1–10.

Gateway server module 120 comprises URL analysis module 149. Ex. 1004, 8:15–16. URL analysis module 149 comprises a reputation scoring module that generates a score or other data representative of a reputation of a URL. *Id.* at 9:29–33. URL analysis module 149 provides its score to policy

module 142 that implements different policies depending on the score. *Id.* at 11:26–29.

2. *Overview of Hubbard-174 (Ex. 1005)*

Hubbard-174 is titled “System and Method of Controlling Access to the Internet.” Ex. 1005, code (54). Hubbard-174 describes gateway server module 120 that includes content filtering module 149. *Id.* at 6:49–50. Content filtering module 149 filters portions of search results returned in response to a network request. *Id.* at 6:50–53. A page returned by search engine 113 to one of client workstations 116 may be intercepted by gateway server module 120 and analyzed by content filtering module 149. *Id.* at 6:59–62.

3. *Overview of Alperovitch (Ex. 1006)*

Alperovitch is titled “Multi-dimensional Reputation Scoring.” Ex. 1006, code (54). Alperovitch describes reputation engines assisting in identifying malicious communication and legitimate communication. *Id.* ¶ 34. Alperovitch describes that reputation can be assigned based in part of behavioral patterns. *Id.* ¶ 45. Alperovitch describes that a number of behavioral attributes for a particular type of behavior can be combined to derive a behavioral profile. *Id.* ¶ 48. “Examples of behavioral profiles relevant to messaging security might include, ‘Spammer’, ‘Scammer’, and ‘Legitimate Sender’.” *Id.* Alperovitch further discloses:

Events and/or evidentiary attributes relevant to each profile define appropriate entities to which a profile should be assigned. This may include a specific set of sending patterns, blacklist events, or specific attributes of the evidentiary data. Some examples include: Sender/Receiver Identification; Time Interval and sending patterns; Severity and disposition of payload;

Message construction; Message quality; Protocols and related signatures; Communications medium.

Id.

4. *Independent Claim 1*

Our determinations herein turn on the parties' dispute as to whether the asserted prior art combinations teach element 1[c2], which requires that a reputation index is "generated from a reputation vector for the Internet resource, the reputation vector comprising a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location." In particular, Patent Owner argues that the asserted prior art combinations do not teach a reputation vector comprising *security history*. Prelim. Resp. 35. We discuss the parties' dispute in connection with each of the two grounds in turn.

a) *Ground 1: Obviousness of Claim 1 over Hubbard-495 and Hubbard-174*

Petitioner argues that "Hubbard-495 discloses the plurality of factors for the Internet resource." Pet. 25. With respect to "security history," Petitioner, more specifically, argues the following:

Security History. Hubbard-495 discloses that "scoring criteria" for the Internet resource may include security history. Ex.1002, ¶82. Hubbard-495 discusses "historical data associated with the IP address of the URL host." Ex.1004, 18:61–19:4. Hubbard-495 explains that this "historical data" could include historical security data, such as "certificate details associated with the URL (e.g., for secure (such as HTTPS) access schemes)," "active content previously identified with reference to the host, the hosts' domain, or the URL path," and "a fingerprint (e.g., a digest or hash) associated with the content of the URL for comparison to such data of previously categorized URLs (and to generate reputation data depending on whether

URLs with the same fingerprint had targeted content).” *Id.*, 19:2-17; *see* Ex.1002, ¶82.

Pet. 25–26.

Patent Owner disagrees and argues:

Hubbard-495 does not disclose any of the . . . claim requirements for the “security history” factor. (Petition 25). Petitioner points to a general list of “criteria” in Hubbard-495. (Petition 25 (*citing* EX-1004 18:61–19:4).) This list does not disclose anything a POSITA would have understood to be a “security history” of an internet resource. (EX-2001 ¶72) Although Petitioner emphasizes Hubbard-495’s use of the term “historical data” (Petition 25), Hubbard uses this phrase only to refer to an IP address history (*see* EX-1004 18:61–19:20; 19:67–20:3.), not a “security history.” Petitioner does not explain, and a POSITA would not understand, how historical data of an IP address teaches the use of a “security history” factor in a reputation vector to adjust a reputation score based on, for example, the frequency of malware infections over time. (EX-2001 ¶72)

Prelim. Resp. 38.

Based on the record before us, we agree with Patent Owner. Hubbard-495’s list of criteria relied on by Petitioner includes “historical data associated with the IP address of the URL host” in a list of “information” that Hubbard-495’s reputation scoring module uses to generate scores. Ex. 1004, 18:58–19:22. We find that Petitioner’s argument that “Hubbard-495 explains that this ‘historical data’ could include historical security data,” such as HTTPS certificate details, active content, and a fingerprint (Pet. 25) is not consistent with the description in Hubbard-495. Hubbard-495 merely describes “historical data associated with the IP address of the URL host” in a list of information, without indicating that any other information in that list comprises “historical data.” Ex. 1004, 18:58–19:22. We also agree with

Patent Owner (Prelim. Resp. 38) that the phrase “historical data associated with the IP address of the URL host” (Ex. 1004, 19:3–4) does not indicate that the data relates to security events and Petitioner does not identify disclosure in Hubbard-495 that remedies the deficiency.

Patent Owner further argues the following:

Petitioner suggests that three other criteria in the Hubbard-495 list teach the “security history” factor recited in the challenged claims: “certificate details associated with the URL (e.g., for secure (such as HTTPS) access schemes),” “active content previously identified with reference to the host, the hosts’ domain, or the URL path,” and “a fingerprint (e.g., a digest or hash) associated with the content of the URL for comparison to such data of previously categorized URLs (and to generate reputation data depending on whether URLs with the same fingerprint had targeted content).” (Petition 25–26.) As discussed below, none of these three criteria discloses or renders obvious the claimed “security history” factor.

Prelim. Resp. 39.

Patent Owner argues that Petitioner “suggests” that the other criteria teach “security history.” *Id.* To the extent Patent Owner argues the Petition includes insufficient explanation, we agree. We find that the Petition simply lists the other criteria and does not provide sufficient explanation as to why those criteria teach the “security history” factor. Pet. 25–26. Dr. Goodrich’s testimony is similar in providing only the same listing and conclusory statements that the other criteria require historical information. Ex. 1002 ¶ 82. Dr. Goodrich’s testimony does not cite supporting evidence, except Dr. Goodrich testifies “as of this writing, the certificate associated with the uci.edu domain for use with the HTTP protocol” includes historical data and his testimony includes an undated snapshot of a certificate viewer for that Web site. *Id.* A snapshot of a Certificate Viewer for a current Web site (*id.*)

taken on the date near or on the date of signing of Dr. Goodrich's Declaration, which is March 31, 2023 (*id.* ¶ 222), does not provide evidence of the understanding of a person of ordinary skill in the art at the time of the invention claimed in the challenged patent. Because Dr. Goodrich's testimony on this point does not disclose supporting evidence, we give Dr. Goodrich's testimony little to no weight. *See* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

Patent Owner provides additional argument and evidence in support of its position that the other criteria listed in the Petition do not teach the "security history" factor. We first address Patent Owner's additional arguments regarding Hubbard-495's "certificate details associated with the URL (e.g., for secure (such as HTTPS) access schemes)" relied on by Petitioner. Pet. 25 (citing Ex. 1004, 18:53–19:22). Relying on the testimony of Dr. Orso, Patent Owner argues "[t]hese criteria do not teach the claimed 'security history' factor and, at most, relate to 'legitimacy' of an internet resource, which all challenged claims recite as a factor distinct from the 'security history' factor." Prelim. Resp. 39 (citing Ex. 2001 ¶ 73). Dr. Orso's testimony relied on by Patent Owner (Ex. 2001 ¶ 73) is supported by the '386 patent's disclosure that "[l]egitimacy is determined by . . . the investment in the Internet resource (virtual hosting with non-affiliated sites, multiple hosting and *SSL security*)." Ex. 1001, 9:10–15. For the reasons discussed with respect to claim construction (*see* § II.C), we determine that the term "security history" is a factor distinct from other factors including "legitimacy" and "behavior."

Also, for reasons discussed with respect to claim construction (*see* § II.C), we determine “security history” means “a history of security events for an internet resource.” We do not discern disclosure in Hubbard-495 supporting that “certificate details associated with the URL (e.g., for secure (such as HTTPS) access schemes)” relied on by Petitioner (Pet. 25 (citing Ex. 1004, 18:53–19:22)) teaches a history of security events, such as breaches or malware infections.

As discussed above, Petitioner simply lists “certificate details associated with the URL (e.g., for secure (such as HTTPS) access schemes)” and does not provide sufficient explanation supporting that this disclosure teaches “security history.” Dr. Goodrich’s testimony is conclusory and does not include citations to supporting evidence, whereas Patent Owner’s arguments and Dr. Orso’s testimony are consistent with the disclosure of Hubbard-495 and our claim construction above. We find that Hubbard-495’s “certificate details associated with the URL (e.g., for secure (such as HTTPS) access schemes)” do not teach using “security history” as required by claim 1.

Second, we turn to Hubbard-495’s “active content previously identified with reference to the host, the hosts’ domain, or the URL path,” relied on by Petitioner. Pet. 25 (citing Ex. 1004, 18:53–19:22). Patent Owner argues “[a]ccording to Hubbard-495, ‘[a]ctive content’ is simply content in a webpage that provides interactive or dynamic qualities to the website.” Prelim. Resp. 40 (citing Ex. 1004, 1:34–52). Also, Patent Owner relies on Dr. Orso’s testimony that Hubbard-495’s active content disclosure “relates to the ‘behavior’ factor” and is “not inherently malicious.” Ex. 2001 ¶¶ 74–75 (cited in Prelim. Resp. 40–41). We do not discern disclosure in Hubbard-

495 supporting that Hubbard-495’s description of active content teaches a history of security events, such as breaches or malware infections. Also, Dr. Orso’s testimony is supported by the ’386 patent’s disclosure of examining *content* for “known patterns” (that is, behaviors) that represent a security threat. Ex. 1001, 1:41–44. Indeed, claim 1 recites that “the behavior factor” “comprises at least one of: plurality of run-time behaviors, script block count, picture count, immediate redirect and response latency,” some of which pertain to examining active content.

As discussed above, Petitioner simply lists Hubbard-495’s “active content previously identified with reference to the host, the hosts’ domain, or the URL path” and does not provide sufficient explanation supporting that this disclosure teaches “security history.” Dr. Goodrich’s testimony is conclusory and does not include citations to supporting evidence, whereas Patent Owner’s arguments and Dr. Orso’s testimony are consistent with the disclosure of Hubbard-495 and our claim construction above. We find that Hubbard-495’s “active content previously identified with reference to the host, the hosts’ domain, or the URL path” does not teach using “security history” as required by claim 1.

Third, we turn to Hubbard-495’s “fingerprint (e.g., a digest or hash) associated with the content of the URL for comparison to such data of previously categorized URLs (and to generate reputation data depending on whether URLs with the same fingerprint had targeted content),” relied on by Petitioner. Pet. 25–26 (citing Ex. 1004, 18:53–19:22). Relying on the testimony of Dr. Orso, Patent Owner argues Hubbard-495’s fingerprint does not teach a history of security events, such as breaches or malware infections. Prelim. Resp. 41 (citing, e.g., Ex. 2001 ¶ 77). Dr. Orso testifies “a

fingerprint would fit within the ‘behavior’ factor, as it involves actively analyzing the content of an internet resource and comparing that content against a database of content that can be identified as malicious.” Ex. 2001 ¶ 77. Dr. Orso’s testimony is supported by the ’386 patent’s disclosure of examining content for known “signatures” that represent a security threat. Ex. 1001, 1:41–44.

As discussed above, Petitioner simply lists Hubbard-495’s “fingerprint (e.g., a digest or hash) associated with the content of the URL” and does not provide sufficient explanation supporting that this disclosure teaches “security history.” Dr. Goodrich’s testimony is conclusory and does not include citations to supporting evidence, whereas Patent Owner’s arguments and Dr. Orso’s testimony are consistent with the disclosure of Hubbard-495 and our claim construction above. We find that Hubbard-495’s “fingerprint (e.g., a digest or hash) associated with the content of the URL” does not teach using “security history” as required by claim 1.

Petitioner relies on only the disclosures discussed above in Hubbard-495. Petitioner does not rely on Hubbard-174 for teaching element 1[c2]. For the reasons given, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that independent claim 1 is unpatentable as obvious over Hubbard-495 and Hubbard-174.

b) Ground 2: Obviousness of Claim 1 over Hubbard-495, Hubbard-174, and Alperovitch

For Ground 2, Petitioner argues that Alperovitch discloses “the reputation vector comprising a plurality of factors for the Internet resource comprising security history.” Pet. 73. Petitioner, more specifically, argues the following:

Alperovitch discloses using behavioral attributes to derive a “behavioral profile” that includes “behavioral events relevant to defining the disposition of an entity matching the profile,” which “include, ‘Spammer’, ‘Scammer’, and ‘Legitimate Sender.’” Ex.1006, [0048]. “Events and/or evidentiary attributes relevant to each profile define appropriate entities to which a profile should be assigned.” *Id.* This may include a “*specific set of sending patterns, blacklist events*, or specific attributes of the evidentiary data.” *Id.* A POSITA would understand that blacklist events would be previous security events that would flag a site for placement on the “blacklist” or a list of entities that are blocked from communicating with or logging into a computer, site, or network, and that “a specific set of sending patterns” would reference historical data about the entity’s prior communications. Ex.1002, ¶215. A POSITA would accordingly understand that Alperovitch discloses historical events that flag security risks, e.g., a “security history” factor. Ex.1002, ¶215.

Id. at 73–74.

Patent Owner disputes Petitioner’s arguments. Prelim. Resp. 42–45.

For instance, Patent Owner argues the following:

First, Petitioner states that Alperovitch discloses that its “behavioral profile” may include “a specific set of sending patterns” and “blacklist events.” Petition at 73. Neither discloses or renders obvious the claimed “security history” factor. (EX-2001 ¶81) For example, “sending patterns” and “blacklist events” are, at most, only part of a larger “behavioral profile.” Alperovitch’s “behavioral profile” is not even limited to historical data and does not describe a history [of] security events [sic]. (EX-2001 ¶82; EX-1006 [0048])

...

Second, Petitioner’s reliance on Alperovitch’s reference to a “behavioral profile” conflates two separate factors of the claimed reputation vector. As discussed above, the challenged claims of the ’386 patent all require a reputation vector that includes five specific factors—“security history, legitimacy, *behavior*, associations and location.” (See Section IV.B, *supra*; EX-2001 ¶84.) Petitioner’s reliance on Alperovitch’s

“behavioral profile” and “behavioral events relevant to defining the disposition of an entity matching the profile” at best might have suggested the “behavior” factor for assessing reputation, but not the separate “security history” factor. (EX-1001 9:8-27.)

Indeed, while Petitioner speculates that Alperovitch’s “behavioral profile” may include “blacklist events” and “a specific set of sending patterns” (Petition 73), Alperovitch refers to both of these as behavioral information. (EX-1006 [0048]) In particular, Petitioner cites a “specific set of sending patterns,” but this reference is to a specific set of sending patterns by a source of electronic communications (*e.g.*, someone sending emails). (EX-2001 ¶86) Alperovitch does not disclose any relationship between these sending patterns and an internet resource’s (*e.g.*, a website’s) reputation for having vulnerabilities exploited, being caught exploiting vulnerabilities, or how often these exploits occur. (EX-2001 ¶85.) Rather, a specific set of sending patterns pertains to behavior of the individual or entity sending the messages, particularly behavioral patterns. (EX-2001 ¶85.)

Prelim. Resp. 43–45.

For the reasons discussed with respect to claim construction (*see* § II.C), we determine that the term “security history” is a factor distinct from other factors including “legitimacy” and “behavior.” We find that Patent Owner’s arguments are supported by Alperovitch. For instance, Alperovitch describes the disclosures relied on by Petitioner as “*behavioral* attributes” that “can be combined to derive a *behavioral* profile.” Ex. 1006 ¶ 48 (emphasis added).

Also, for reasons discussed with respect to claim construction (*see* § II.C), we determine “security history” means “a history of security events for an internet resource.” We do not discern disclosure in Alperovitch of use of a history of security events or sufficient explanation by Petitioner as to how Alperovitch teaches a history of security events.

Petitioner does not provide sufficient explanation supporting that Alperovitch's disclosure teaches "security history." Dr. Goodrich's testimony is conclusory and does not include citations to supporting evidence, whereas Patent Owner's arguments and Dr. Orso's testimony are consistent with the disclosure of Alperovitch and our claim construction above. We find that Alperovitch's disclosure does not teach using "security history" as required by claim 1.

Petitioner does not identify additional disclosures in Hubbard-495 or Hubbard-174 in connection with its second ground and element 1[c2]. For the reasons given, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that independent claim 1 is unpatentable as obvious over Hubbard-495, Hubbard-174, and Alperovitch.

5. Independent Claims 7, 11, and 13

Independent claims 7, 11, and 13 recite elements 7[e3], 11[c2], and 13[c2] that are similar to element 1[c2] discussed above with respect to claim 1 requiring that a reputation vector comprises a plurality of factors including "security history." For elements 7[e3], 11[c2], and 13[c2], Petitioner relies on its earlier analysis regarding element 1[c2] without supplementation. Pet. 52, 58, 64, 73–74. Accordingly, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that independent claims 7, 11, and 13 are unpatentable.

6. Dependent Claims 2–6, 8–10, 12, 15, 16, and 18

Each of dependent claims 2–6, 8–10, 12, 15, 16, and 18 depends, directly or indirectly, from one of claims 1, 7, 11 or 13. Petitioner's arguments and evidence for dependent claims 2–6, 8–10, 12, 15, 16, and 18

do not remedy the deficiencies discussed with respect to the independent claims. *See* Pet. 38–70, 74–75.

Accordingly, we conclude that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 2–6, 8–10, 12, 15, 16, and 18 are unpatentable.

III. CONCLUSION

Based on the arguments and evidence presented by the parties, we conclude that Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to at least one claim of the '386 patent challenged in the Petition. Therefore, we do not institute an *inter partes* review.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is denied and no *inter partes* review is instituted.

IPR2023-00784
Patent 8,438,386 B2

FOR PETITIONER:

Kat Li
KIRKLAND & ELLIS LLP
kat.li@kirkland.com

FOR PATENT OWNER:

Brian Eutermoser
Russell E. Blythe
Mikaela Stone
KING & SPALDING LLP
beutermoser@kslaw.com
rblythe@kslaw.com
mikaela.stone@kslaw.com