

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORCEPOINT LLC,
Petitioner

v.

WEBROOT, INC. AND OPEN TEXT, INC.,
Patent Owners.

IPR2023-00784
U.S. Patent No. 8,438,386

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,438,386 UNDER 37 C.F.R. § 42.101**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	RELIEF REQUESTED.....	2
A.	37 C.F.R. § 42.104(b)(1): Claims for Which Review Is Requested	2
B.	37 C.F.R. § 42.104(b)(2): Statutory Grounds for Challenge	2
III.	THE '386 PATENT	3
IV.	LEVEL OF ORDINARY SKILL.....	6
V.	CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3)	7
VI.	THE BOARD SHOULD NOT EXERCISE DISCRETION TO DENY INSTITUTION	7
A.	The Board Need Not Reach the <i>Fintiv</i> Factors Due to Compelling Evidence of Unpatentability.....	7
B.	The <i>Fintiv</i> Factors Favor Institution	8
C.	The <i>Becton Dickinson</i> Factors Favor Institution.....	10
VII.	BRIEF OVERVIEW OF PRIOR ART REFERENCES	13
A.	Hubbard-495.....	13
B.	Hubbard-174.....	14
C.	Alperovitch.....	14
VIII.	CLAIMS 1-13, 15, 16, AND 18 ARE UNPATENTABLE UNDER 37 C.F.R. § 42.104(B)(4)	15
A.	GROUND 1: HUBBARD-495 IN COMBINATION WITH HUBBARD-174 RENDERS OBVIOUS CLAIMS 1-13, 15, 16, and 18.	15
1.	Claim 1	15
2.	Claim 2.....	38

3.	Claim 3	39
4.	Claim 4	42
5.	Claim 5	42
6.	Claim 6	45
7.	Claim 7	46
8.	Claim 8	53
9.	Claim 9	53
10.	Claim 10	56
11.	Claim 11	57
12.	Claim 12	60
13.	Claim 13	61
14.	Claim 15	67
15.	Claim 16	68
16.	Claim 18	69
B.	GROUND 2: HUBBARD-495 IN COMBINATION WITH HUBBARD-174 and ALPEROVITCH RENDERS OBVIOUS CLAIMS 1-13, 15, 16, and 18.....	70
1.	Claims 1, 7, 11, and 13	70
2.	Claims 2, 3, 5, 6, 8, 9, 10, 12, 15, 16, and 18	74
3.	Claim 4	74
IX.	SECONDARY CONSIDERATIONS	75
X.	CERTIFICATION OF GROUNDS FOR STANDING UNDER 37 C.F.R. § 42.104	75
XI.	MANDATORY NOTICES	75

A.	Real Party-in-Interest Under 37 C.F.R. § 42.8(b)(1)	75
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	75
C.	Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)	76
D.	Service Information Under 37 C.F.R. § 42.8(b)(4).....	76
XII.	PAYMENT OF FEES UNDER 37 C.F.R. §42.103.....	76
XIII.	CONCLUSION	77

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH,</i> IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020).....	10, 12
<i>Apple Inc. v. Fintiv, Inc.,</i> IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020)	7, 8, 10
<i>Becton, Dickinson & Co. v. B. Braun Melsungen AG,</i> IPR2017-01586, Paper 8 (P.T.A.B. Dec. 15, 2017)	10
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.,</i> 868 F. 3d 1013 (Fed. Cir. 2017)	7
<i>Phillips v. AWH Corp.,</i> 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	7
<i>Fasteners for Retail, Inc. v. RTC Indus., Inc.,</i> IPR2019-00994, Paper 9 (PTAB Nov. 5, 2019).....	12
<i>Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.,</i> 200 F.3d 795 (Fed. Cir. 1999)	7
<i>Webroot Inc., et al. v. AO Kaspersky Lab, et al.,</i> No. 6:22-cv-243 (W.D. Tex.)	8
<i>Webroot, Inc. et al v. Forcepoint LLC,</i> No. 6:22-cv-342 (W.D. Tex.)	8, 75
<i>Whitewater West Indus., LTD v. Am. Wave Machs.,</i> IPR2022-01033, Paper 8 (P.T.A.B. Nov. 22, 2022).....	12
Statutes	
35 U.S.C. § 102.....	2, 3
35 U.S.C. § 103	3
35 U.S.C. § 311	2

35 U.S.C. § 314.....	8, 10
----------------------	-------

Other Authorities

37 C.F.R. § 1	15
---------------------	----

37 C.F.R. § 42	2, 7, 15, 75
----------------------	--------------

TABLE OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 8,438,386 to Hegli et al.
1002	Declaration of Dr. Michael T. Goodrich
1003	Curriculum Vitae of Dr. Michael T. Goodrich
1004	U.S. Patent No. 9,654,495 to Hubbard et al.
1005	U.S. Patent No. 8,015,174 to Hubbard
1006	U.S. Patent Publication No. 2008/0175266 to Alperovitch et al.
1007	Complaint, <i>Webroot, Inc. et al v. Forcepoint LLC</i> , No. 6:22-cv-342 (W.D. Tex.) (Mar. 31, 2022)
1008	Excerpt from Transcript of Motions Hearing in <i>Webroot, Inc., et al. v. AO Kaspersky Lab</i> , No. 6:22-cv-243 (W.D. Tex.) (Dec. 9, 2022)
1009	Patent File History of U.S. Patent No. 8,438,386
1010	LexMachina Summary of Cases filed by Webroot, Inc. in the Western District of Texas
1011	Periakaruppan, Ram & Nemeth, Evi, “GTrace—A Graphical Traceroute Tool,” <i>USENIX</i> (1999)
1012	Microsoft Computer Dictionary (5th ed., 2002)
1013	U.S. Patent Publication No. 2008/0082662 to Dandliker et al.

I. INTRODUCTION

Petitioner Forcepoint LLC (“Forcepoint” or “Petitioner”) requests *inter partes* review of claims 1-13, 15, 16, and 18 of U.S. Patent No. 8,438,386 (Ex.1001, the “’386 Patent”), purportedly assigned to Patent Owners Webroot, Inc. and Open Text, Inc. (collectively, “Patent Owners”).

The ’386 Patent describes “[a] method and system for controlling access to an Internet resource.” Ex.1001, Abstract. The patent sets forth “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.*, 1:24-28. “The reputation vector comprises a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location.” *Id.*, 6:44-46, 6:67-7:2. But as became apparent during prosecution, controlling access to an Internet resource by generating a reputation index, based on a plurality of the claimed factors, was already well-known in the art.

The applicants added limitations concerning the “plurality of factors for the Internet resource” that were not new and non-obvious. Having the location factor include “two or more of[] country of domain registration, country of service hosting and country of an internet protocol address block,” the legitimacy factor include “two or more of[] age of a domain registration, popularity rank, internet protocol address, number of hosts, top-level domain,” and the behavior factor include “at least

one of[] plurality of run-time behaviors, script block count, picture count, immediate redirect and response latency” were all taught by the prior art well before the ’386 Patent was filed. *See* Ex.1001, Cl. 1. As the prior art shows, it was well-known before the ’386 Patent’s priority date to use these factors and the other claimed limitations in developing a risk profile for an Internet resource to control access to the Internet resource.

II. RELIEF REQUESTED

A. 37 C.F.R. § 42.104(b)(1): Claims for Which Review Is Requested

Petitioner respectfully requests *inter partes* review under 35 U.S.C. § 311 of claims 1-13, 15, 16, and 18 of the ’386 Patent and the cancellation of those claims as unpatentable.

B. 37 C.F.R. § 42.104(b)(2): Statutory Grounds for Challenge

The ’386 Patent was filed February 21, 2010, and lists provisional applications filed April 21, 2009, and September 10, 2009, respectively, as related applications. Ex.1001. Even assuming the ’386 Patent is entitled to a priority date of April 21, 2009,¹ each asserted reference identified in the table is prior art to the ’386 Patent under at least pre-AIA 35 U.S.C. § 102(a) and/or (e).

¹ In the parallel district court proceedings, Plaintiffs asserted a priority date of April 21, 2009 for the ’386 Patent. Ex.1007, 16.

Prior Art References
Hubbard-495 (Ex.1004), U.S. Patent No. 9,654,495, filed February 28, 2007, published June 5, 2008, and issued May 16, 2017 (§§ 102(a), (e)).
Hubbard-174 (Ex.1005), U.S. Patent No. 8,015,174, filed February 28, 2007, published August 28, 2008, and issued September 6, 2011 (§§ 102(a), (e)).
Alperovitch (Ex.1006), U.S. Patent Application Publication No. 2008/0175266, filed January 24, 2007, and published July 24, 2008. (§§ 102(a), (e)).

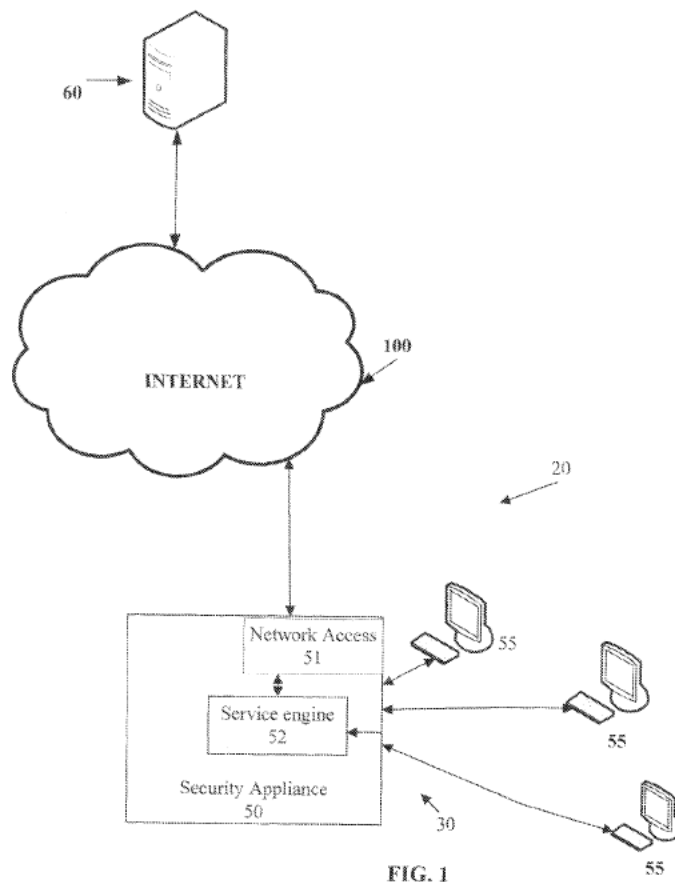
Claims 1-13, 15, 16, and 18 of the '386 Patent are unpatentable under pre-AIA 35 U.S.C. § 103 based on the following grounds:

No.	Grounds of Unpatentability	Basis
1	Hubbard-495 in view of Hubbard-174 renders obvious claims 1-13, 15, 16, and 18.	§ 103
2	Hubbard-495 in view of Hubbard-174 and further in view of Alperovitch renders obvious claims 1-13, 15, 16, and 18.	§ 103

III. THE '386 PATENT

The '386 Patent, titled "SYSTEM AND METHOD FOR DEVELOPING A RISK PROFILE FOR AN INTERNET SERVICE" issued on May 7, 2013, from U.S. Patent Application No. 12/709,504, filed on February 21, 2010.

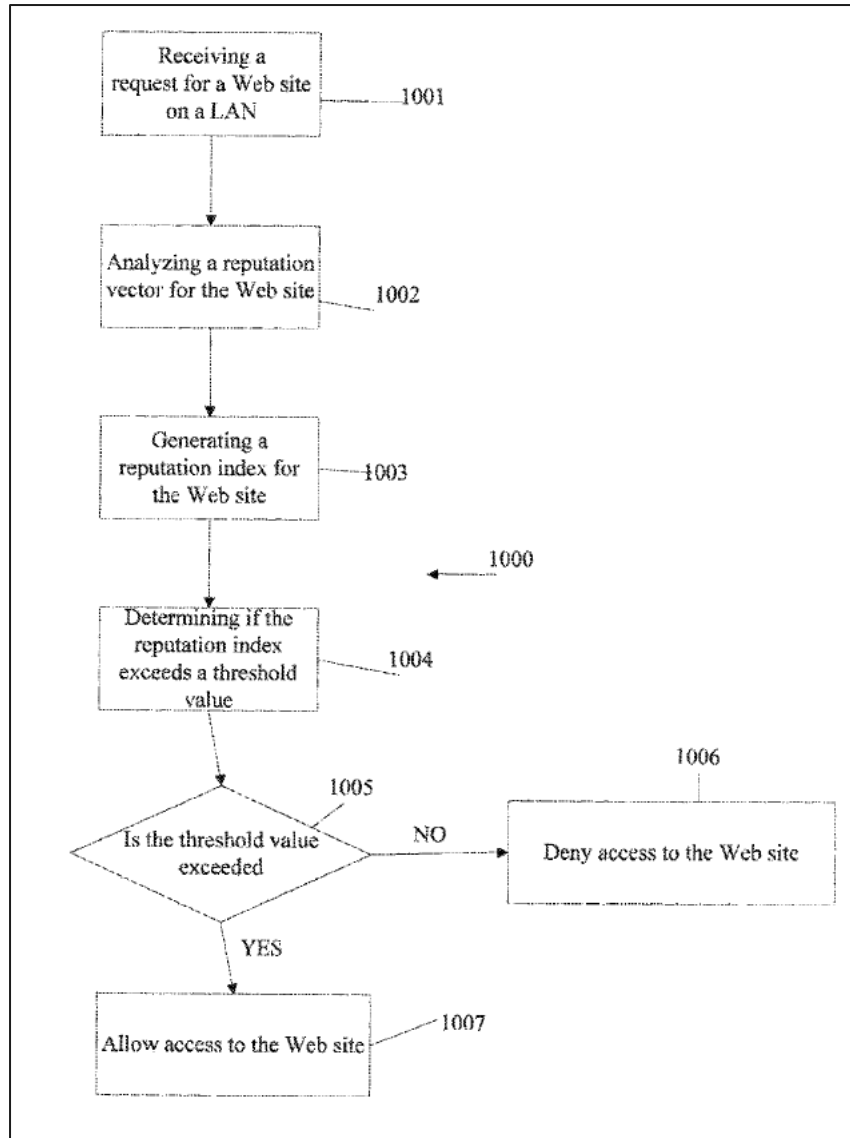
The system of the '386 Patent "comprises a local area network 30, the Internet 100 and an Internet service located at a remote server 60," where the local area network 30 "comprises a security appliance 50 and a plurality of client-side devices 55." Ex.1001, 10:2-7.



Ex.1001, Fig.1.

The '386 Patent discloses “transmitting a request for an Internet resource from an Internet-enabled client application from a client-side device of a local area network,” “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,” and “determining if a reputation index for the Internet resource is at or above a threshold value established for the local area network.” *Id.*, 6:32-42; *see id.*, 6:59-7:8. “The reputation index is calculated from a reputation vector which preferably includes a

plurality of factors for the Web site comprising country of domain registration, country of service hosting, country of an internet protocol address block, age of a domain registration, popularity rank, internet protocol address, number of hosts, to-level [*sic*] domain, a plurality of run-time behaviors, JavaScript block count, picture count, immediate redirect and response latency.” *Id.*, 10:23-31. In Figure 3, “if the reputation index is not above the threshold,” then “access to the Web site is denied and a transmission of the denial is sent to the client-side device” whereas if “the reputation index for the Web site is above the threshold, then the access to the Web site by the client-side device is permitted by the security appliance.” *Id.*, 10:33-41.



Ex.1001, Fig.3.

IV. LEVEL OF ORDINARY SKILL

A person having ordinary skill in the art (a “POSITA”) relative to the ’386 Patent would have at least a four-year undergraduate degree in computer science or a closely related field and at least two years of experience in the field of computer

and network security. Ex.1002, Declaration by Michael Goodrich, Ph.D., ¶¶22-25.

Additional education could substitute for professional experience and vice versa. *Id.*

V. CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3)

Claims only need to be construed “to the extent necessary to resolve the controversy.” *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). Here, no terms need construction because the claims read on the prior art under any construction consistent with *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

VI. THE BOARD SHOULD NOT EXERCISE DISCRETION TO DENY INSTITUTION

A. The Board Need Not Reach the *Fintiv* Factors Due to Compelling Evidence of Unpatentability

The USPTO Director stated that the Board “will not rely on the *Fintiv* factors to discretionarily deny institution...where a petition presents compelling evidence of unpatentability,” which “would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” USPTO Memorandum (June 21, 2022), https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf (“*Fintiv* Memorandum”), 2, 4. This Petition meets that criteria.

B. The *Fintiv* Factors Favor Institution

To the extent the Board finds it necessary to analyze the *Fintiv* factors, the relevant *Fintiv* factors demonstrate the Board should not exercise discretion to deny institution under 35 U.S.C. § 314(a) and *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, 2020 WL 2126495 (P.T.A.B. Mar. 20, 2020) (precedential).

Factor 1 (existence or likelihood of a stay):

The '386 Patent was asserted against Petitioner in *Webroot, Inc. et al v. Forcepoint LLC*, No. 6:22-cv-00342 (W.D. Tex.) (filed Mar. 31, 2022) (the “related litigation”).² See Ex.1007, ¶¶14-16. Where a stay on the basis of parallel IPR proceedings has been neither requested nor granted, “[t]his factor does not weigh for or against discretionary denial.” *Fintiv*, at *12. As a stay was neither requested nor granted in the related litigation, Factor 1 is neutral.

Factor 2 (proximity of trial date to statutory IPR deadline):

Pursuant to the District Court’s amended scheduling order on January 22, 2023 (Dkt. 160), trial in this case will not begin until August 19, 2024. Based on an 18-month IPR schedule, a Final Written Decision (“FWD”) would issue around October 2024. However, “scheduled trial dates are unreliable and often change.” *Fintiv* Memorandum, 8. “A court’s scheduled trial date, therefore, is not by itself a

² This case has been consolidated with four others as *Webroot Inc. and Open Text, Inc. v. AO Kaspersky Lab*, 6:22-cv-00243 (W.D. Tex.).

good indicator of whether the district court trial will occur before the statutory deadline for a [FWD].” *Id.* This is particularly true here, as the consolidated case consists of multiple patents asserted against multiple defendants (fifteen patents and five defendants). The District Court stated this case is “about as complicated as you’re going to get with patent cases,” Ex.1008, 53:7-8, and said it would be “amenable to adjusting the schedule” by “granting more time to address things,” *id.*, 53:22-23. The case against Forcepoint was filed last of the five cases, so any trial relating to this patent would likely occur after other defendants. Ex.1010, Summary of Webroot WDTX Cases. Thus, it is unlikely the District Court will resolve the dispute related to the ’386 Patent before a FWD arising from this petition. Thus, this factor weighs against discretionary denial.

Factor 3 (investment in parallel proceeding):

The District Court proceeding is still in the early stages, as fact discovery has not yet begun. Petitioner has committed significant resources to this IPR proceeding, which balances any resources invested in the related litigation, which would be lost without consideration on the merits. In addition, institution of this Petition would reduce the substantial expenses that would result from the related litigation. Given Petitioner’s diligence and significant investment in filing this Petition, especially this early in the litigation, this factor weighs against a discretionary denial.

Factor 4 (overlap between issues):

There should be no overlap of invalidity challenges. An FWD is likely to issue before the Texas trial (*see* Factor 2) and Petitioner will be estopped from arguing grounds raised or that reasonably could have been raised in this IPR. Thus, Factor 4 weighs against a discretionary denial.

Factor 5 (same parties):

Petitioner is a defendant in the related litigation. But in view of the other *Fintiv* factors—which heavily weigh against the Board’s exercise of §314(a) discretion—the similarity of the parties is of limited weight.

Factor 6 (other circumstances impacting the Board’s exercise of discretion):

Factor 6 favors institution because this Petition presents compelling evidence of unpatentability. Accordingly, in light of the guidance set forth in the *Fintiv* Memorandum at 2-4, IPR should be instituted.

C. The *Becton Dickinson* Factors Favor Institution

The factors in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, 2017 WL 6405100, Paper 8 at *17-18 (P.T.A.B. Dec. 15, 2017) (precedential as to § III.C.5, first para) strongly favor institution. *See also Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, 2020 WL 740292, Paper 6 (P.T.A.B. Feb. 13, 2020) (precedential). Hubbard-495, Hubbard-174, and Alperovitch were not cited or considered during prosecution of the ’386 Patent.

Moreover, the grounds presented in this Petition are not cumulative to anything discussed during prosecution of the '386 Patent. *See* Ex.1009, Patent File History of U.S. Patent No. 8,438,386.

During prosecution, the '386 Patent was rejected as anticipated by Dandliker, which described controlling access to network resources based on the resource's reputation. Ex.1009, 76-77. While Dandliker taught determining a reputation index for the network resource based on certain factors like its location (e.g., country the website is hosted in), Ex.1013, [0073], the applicant argued that Dandliker failed to disclose basing the resource's reputation on legitimacy and behavior factors or transmitting a decision transmission to the client about allowing or blocking the request. Ex.1009, 29. Unlike Dandliker, which does not mention "behavior" even once, Ex.1013, Hubbard-495 describes in detail "provid[ing] a *behavioral score or data* associated with *one or more behavior properties (e.g., a property such as 'writes to registry')*," Ex.1004, 21:24-28, and "identify[ing] *behavior of the web content affecting, for example,...network access, processor usage, memory usage, [and] use of system resources,*" *id.*, 22:7-11. Similarly, while Dandliker disclosed an access control decision at a proxy, Ex.1013, [0169]-[0170], Hubbard-495 and Hubbard-147 disclose transmitting a decision transmission (e.g., the allowed web page or filtered search results) to an Internet-enabled web browser. Ex.1004, 9:55-58; Ex.1005, 14:52-54.



Ex.1005, Fig.14.

Likewise, Alperovitch discloses security history factors and was neither applied nor discussed during prosecution. A different Alperovitch reference (U.S. Patent App. Pub. No. 2007/0130350) was listed in the Information Disclosure Statement, but was not discussed during prosecution of the '386 Patent—and would not be cumulative because it was not considered with either Hubbard reference. The Board has “held that a reference that ‘was neither applied against the claims nor discussed by the Examiner’ does not weigh in favor of exercising [] discretion under §325(d).” *Fasteners for Retail, Inc. v. RTC Indus., Inc.*, IPR2019-00994, Paper 9 at 7-11 (PTAB Nov. 5, 2019); *Whitewater West Indus., LTD v. Am. Wave Machs.*, IPR2022-01033, Paper 8 at 16 (PTAB Nov. 22, 2022) (concluding that “the criteria adopted by the Board for denying the petition in *Advanced Bionics* included not only

the fact the art was made of record, but also the fact it was applied and discussed during prosecution”).

In addition, whether the ’386 Patent would have been *obvious* to a POSITA in light of the grounds presented in this Petition was never discussed during prosecution.

VII. BRIEF OVERVIEW OF PRIOR ART REFERENCES

A. Hubbard-495

Hubbard-495 discloses methods and system for “controlling access to web content.” Ex.1004, 2:33-61. A “reputation scoring module generates a reputation score or other reputation indicator of targeted content associated with the URL.” *Id.*, 27:38-40. “The reputation scoring module 331 may generate the scores based on information about the URL of the web page (e.g., scoring criteria).” *Id.*, 18:61-64. The disclosed factors include, for example, “[g]eo-location data associated with the URL..., the name server that provides the IP address of the URL host or its domain, ...active content previously identified with reference to the host..., [and] historical data associated with the IP address of the URL host.” *Id.*, 18:61-19:23. The reputation score may be “relied upon by the gateway server module 120 to determine under what circumstances, if any, the user will be allowed to access the content associated with each scored URL.” *Id.*, 11:7-11.

B. Hubbard-174

Hubbard-174 “relates to controlling access to the Internet by monitoring data received in response to a data request to the Internet.” Ex.1005, 1:7-9. A “gateway server module” is configured to “intercept the content sent from the first device to the second device and determine a category for the content based at least partially on a comparison of the intercepted content with data in a categorized URL/content database.” *Id.*, 2:1-5. A “policy module” contains “instructions for modifying content based on the category of the content,” and a “content filtering module” “modif[ies] at least some of the content based at least in part on the instructions.” *Id.*, 2:5-9. Hubbard-174 discloses that “modifying the content” consists of “removing at least some of the content based at least in part on a classification” and “sending the modified content to the requesting device.” *Id.*, 1:61-64.

C. Alperovitch

Alperovitch discloses “[m]ethods and systems for assigning reputation to communications entities.” Ex.1006, Abstract. “Methods of assigning reputation to a communications entity can include: collecting data associated with entities originating communications,” “aggregating the collected data; analyzing the aggregated data to identify attributes respectively associated with entities originating communications; correlating the attributes to identify relationships between entities; updating a reputation associated with one or more entities based upon the

relationship to one or more other entities identified by correlating the attributes; and, handling, communications based upon the updated reputation information.” *Id.*, [0009].

**VIII. CLAIMS 1-13, 15, 16, AND 18 ARE UNPATENTABLE UNDER
37 C.F.R. § 42.104(B)(4)**

Under 37 C.F.R. § 42.104(b)(5) for evidence supporting challenge, a list of exhibits is provided at the beginning of the Petition. The relevance of this evidence and the specific portions supporting the challenge are provided herein in Section VIII. Petitioner submits a declaration of Dr. Michael Goodrich (Ex.1002) in support of this Petition under 37 C.F.R. § 1.68.

**A. GROUND 1: HUBBARD-495 IN COMBINATION WITH
HUBBARD-174 RENDERS OBVIOUS CLAIMS 1-13, 15, 16,
and 18.**

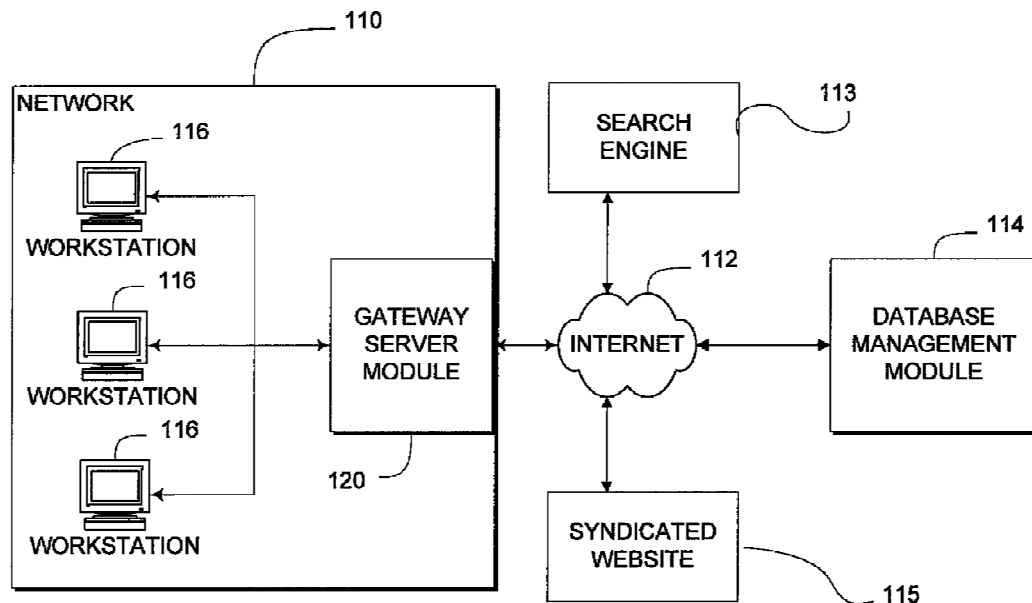
1. Claim 1

Hubbard-495, alone or in combination with Hubbard-174, renders obvious claim 1.

Motivation to Combine

A POSITA would have been motivated to combine Hubbard-495 and Hubbard-174. Each reference is analogous art to the '386 Patent at least because each is from the same field of endeavor, namely, methods and systems to determine conditions under which access to an Internet resource is allowed. Ex.1004, 2:33-61; Ex.1005, 1:7-9. A POSITA would understand that both disclose similar exemplary

systems that could be readily combined. Ex.1004,4:38-5:7; Ex.1005, 4:16-52. For example, both disclose embodiments that include a gateway server module 120 connected through the Internet to a database management module. Ex.1004, 4:50-67; Ex.1005, 4:29-46. In those embodiments, workstations make requests for web content that may be allowed or blocked by the gateway server module. *See* Ex.1004, 6:34-36, 6:53-7:3; Ex.1005, 6:10-12, 6:27-45.



Ex.1004, Fig.1; Ex.1005, Fig.1.

A POSITA would also have been motivated to combine because each reference teaches different functionalities of the same system. For example, Hubbard-495 discloses that “[t]he content filtering module 150 may be configured to parse the returned page and identify URL links in the returned search results and embedded items of content such as images or active content.” *Id.*, 8:37-41. Hubbard-

495 further discloses that “the content filtering module 150 may also be configured to remove objectionable content from the returned search engine results.” *Id.*, 8:50-52. As Hubbard-495 does not elaborate on how to remove objectionable content, it would have been natural to seek to combine with Hubbard-174, which discloses “removing certain portions of the data such as malicious or otherwise objectionable content.” Ex.1005, Abstract. Further, the two references share the same first-named inventor, were filed the same day, and listed the same assignee.

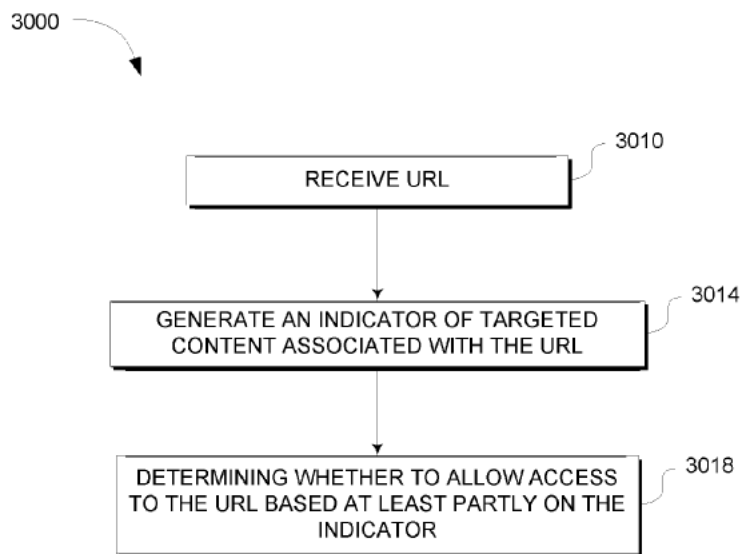
Similarly, Hubbard-174 describes a “scoring/classification system 186” that “provide[s] a score or classification...to web content” to “be delivered...to gateway server modules 120.” Ex.1005, 10:3-9. “[T]he gateway server module 120 may be configured to edit or identify returned URLs that are categorized as being ‘Malicious’ or ‘Spyware.’” *Id.*, 6:36-38. As Hubbard-174 does not elaborate on how to score web content, it would have been natural to seek to combine with Hubbard-495, which discloses “generating a score indicative of the reputation, or likelihood that a web site associated with an uncategorized URL contains active or other targeted content.” Ex.1004, Abstract.

A POSITA would have had a reasonable expectation of success in combining Hubbard-495 and Hubbard-174, as doing so would have yielded nothing more than the predictable results of enhancing the common system of them by adding the

functionalities described in each reference without the need for rearrangement or excessive modification of the system. Ex.1002, ¶¶50-53.

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

Hubbard-495 discloses the preamble, to the extent it is limiting. Ex.1002, ¶¶54-55. In Figure 25, Hubbard-495 discloses a method “of controlling access to *web content* based on the components of a *requested URL*.” *Id.*, 27:32-34.³ A POSITA would understand that a URL (Uniform Resource Locator) references the web content or an “Internet resource” at that location. Ex.1002, ¶55. The ’386 Patent discusses two examples of Internet resources: “www.c.reditcan.cn” and “www.USmoney.GOV.” Ex.1001, 12:61-64.



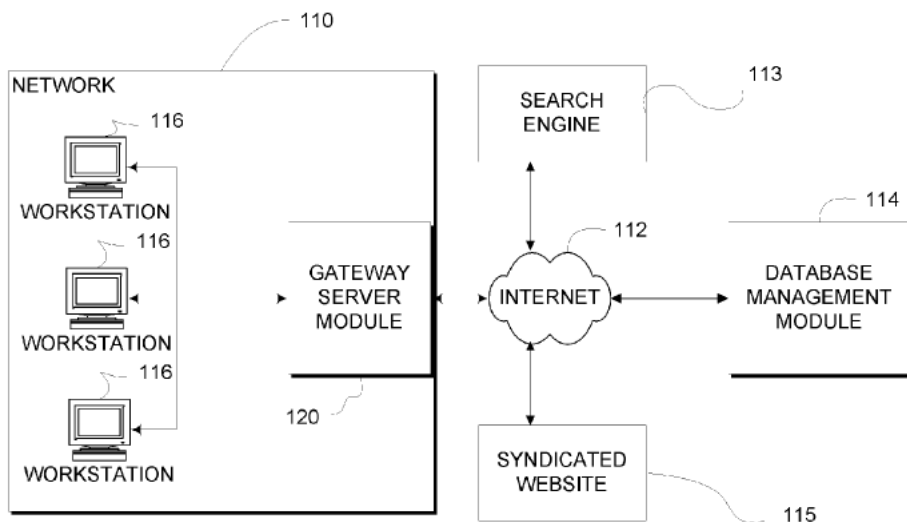
³ All emphasis is added unless otherwise noted.

FIG. 25

Ex.1004, Fig.25.

- b. 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;”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶56-62. In Figure 1, Hubbard-495 discloses “a network 110” that “may be a local area network” that includes one or more workstations 116. Ex.1004, 4:39-44. The workstations “may be various types of client computers that are attached to the network” and include applications that are Internet-enabled, “such as web browsers, e-mail programs, or the like.” *Id.*, 4:46-49.



Ex.1004, Fig.1.

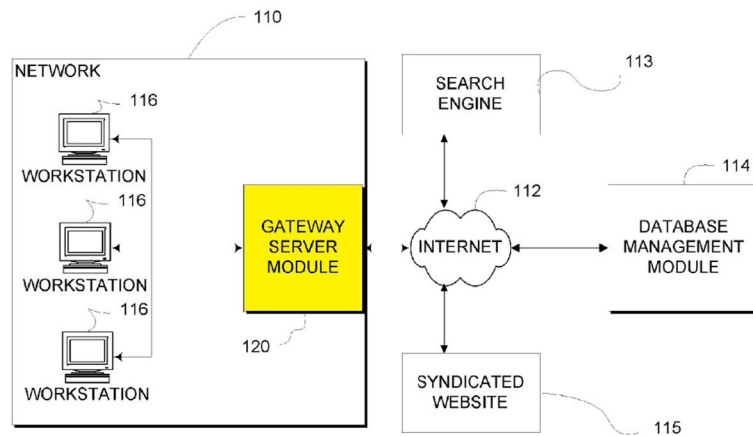
“[T]he workstation 116 requests a URL from the Internet 112.” *Id.*, 22:53-54.

For example, the workstation 116 may include “one or more URL request modules 136.” *Id.*, 5:16-17, 5:35-37. The functions of “the URL request modules 136 are performed by software applications such as web browsers, [e.g.,] Internet Explorer R, Mozilla Firefox, Opera, Safari,” but “[t]hese functions may also be performed by other types of software such as web feed readers, instant messaging programs,” “or some other applications.” *Id.*, 5:38-67.

Further, the workstation 116, via the URL request module 136, may “receive a data request from either a user or some system process,” which may be “a search engine request made to the search engine 113” or “a content request made to the syndicated website 115.” *Id.*, 5:40-49. In Figure 1, the search engine 113 and syndicated website 115 are both accessible via the Internet 112. *Id.*, Fig.1. The search engine 113 may “return one website or a list of websites (and URL links leading to those websites)” in response to the search, while the syndicated website 115 may return “one URL link or a list of URL links to the requested content.” *Id.*, 5:8-10, 5:45-51. A POSITA would understand that the search engine request and the content request would be examples of a “request for an Internet resource,” the “website or a list of websites” and “URL link or a list of URL links to the requested content” would constitute the response to such requests, and that such websites would reside at a web server. Ex.1002, ¶¶60-62.

- c. 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;”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶63-69. The '386 Patent describes the security appliance as “control[ling] access to the Internet by each of the plurality of client-side devices.” Ex.1001, 5:59-61. The security appliance “preferably comprises a network access 51 for *permitting access to the Internet* from the local area network 30, and a service engine 52 for determining if a requested Internet resource has a reputation index that meets a threshold established for the local area network 30.” Ex.1001, 10:12-16. Hubbard-495 discloses a gateway server module 120 that “may reside at the edge of the network 110 so that traffic sent to and from the Internet 112 may pass through it on its way into or out of the network 110.” *Id.*, 4:51-54. In Figure 1, the gateway server module 120 is part of the network 110, which may be a local area network. “[T]he gateway server module 120 may...protect[] the network 110 from unauthorized intrusions from the Internet 112,” *id.*, 6:26-30, and may also include a policy module 142 “used to *implement network policies* regarding how certain content will be handled by the gateway server module 120 or by a firewall or some other security software installed within the network 110,” *id.*, 6:53-58. A POSITA would understand that Hubbard-495’s gateway server module 120 is a “security appliance.” Ex.1002, ¶¶65-67.



Ex.1004, Fig.1 (annotated).

Hubbard-495 further teaches that the gateway server module may be in “two way communication with the workstation 116” and “also in two-way communication with the Internet 112.” *Id.*, 6:19-23. “Thus, *requests originating within the workstations 116 of the network 110 may be required to pass through the gateway server module 120 as they proceed to the Internet.*” *Id.*, 6:24-26.

- d. 1[c1]: “determining if a reputation index for the Internet resource is at or above a threshold value established for the local area network,”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶70-77. The '386 Patent describes a “reputation index, a score which can be used with empirically developed threshold values to block access where the reputation index is deemed to be too low to be safe.” Ex.1001, 9:38-41. Likewise, Hubbard-495 discloses “a reputation scoring module [] that generates *a score* or other data *representative of a reputation*

of the URL” or “of targeted content associated with the URL.” *Id.*, 9:29-33, 27:38-40.

Hubbard-495 explains that such a reputation score or index may be compared with a threshold value established for the local area network to determine whether the request will be blocked or allowed. For example, “***URLs with scores above a threshold*** are identified with a category, e.g., malicious, regardless of or in addition to, the category identified by content analysis of the web page.” Ex.1004, 20:65-21:10. The gateway server module may be used to protect a local area network and its policy module 142 “may be configured to provide the system guidance on how to handle URL requests for categorized URLs,” such as “disallow[ing] URL requests that are categorized as being ‘Malicious.’” *Id.*, 6:58-63.

In addition, the URL analysis module 149 may generate a “***sufficiently high reputation score*** (e.g., indicative of a good reputation...) for an uncategorized URL so that the policy module 142 allows access to the uncategorized URL when the policy module 142 would otherwise not allow access to the URL.” *Id.*, 11:29-36. A POSITA would understand that determining whether a reputation score is “sufficiently high” for the particular local area network on which the gateway server module is located would necessarily involve comparing it to a threshold value. Ex.1002, ¶75.

Hubbard-495 also discloses that the threshold values are established for the local area network, stating that the gateway server module's policy module may be "used to **implement network policies** regarding how certain content will be handled by the gateway server module 120 or by a firewall or some other security software installed within the network 110." *Id.*, 6:54-58. The network 110 may be a "local area network." *Id.*, 4:39-40. Thus, a POSITA would understand that the policy module 142 could be used to establish policies for the local area network. Ex.1002, ¶74. The policy module 142 "may be configured to **block access to URLs with low scores (e.g., indicative of poor reputation...)** where the applicable policy might otherwise allow access to the URL." *Id.*, 11:36-40.

- e. 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,"

As discussed in Section VIII.A.1.d for limitation 1[c1], Hubbard-495 discloses a reputation index. Hubbard-495 further discloses this limitation. Ex.1002, ¶¶78-95. The '386 Patent explains the "attributes of the [Internet] resource [are] collectively referred to as the reputation vector of the resource." Ex.1001, 1:24-28; *see id.*, 4:62. Likewise, Hubbard-495 discloses that a reputation score may be generated "based on information about the URL of the web page (e.g., scoring criteria)," and outlines exemplary factors, such as:

Geo-location data associated with the URL...historical data associated with the IP address of the URL host, creation date or expiration date associated with the registration of the URL host, ...meta tag categories associated with other URLs associated with the URL host..., 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 scoring based on site (host or domain) access statistics.

Ex.1004, 18:53-19:22. A POSITA would understand Hubbard-495's scoring criteria to constitute the claimed "reputation vector comprising a plurality of factors for the Internet resource." Ex.1002, ¶¶79-80.

Hubbard-495 discloses the plurality of factors for the Internet resource, including:

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.

Legitimacy. Legitimacy is determined, for example, by “the top-level domain, the investment in the Internet resource..., the traffic volume, the category age and the popularity rank.” Ex.1001, 9:10-17. As discussed in Section VIII.A.1.g for limitation 1[c4], Hubbard-495 discloses legitimacy as one of the plurality of factors. Ex.1002, ¶¶90-95.

Behavior. “Behaviors include the use of popup ads, browser hijacking and the use of auto-redirecting.” Ex.1001, 9:18-19. As discussed in Section VIII.A.1.h for limitation 1[c5], Hubbard-495 discloses behavior as one of the plurality of factors. Ex.1002, ¶¶96-103.

Associations. The ’386 Patent states that associations may include, for example, “the number of sites linking into the site, the reputations of the linked in sites and the reputations of the linked-to sites.” Ex.1001, 9:19-21. A POSITA would understand that “associations” would be information about *other* Internet resources that are not the requested Internet resource, such as the URLs, URL hosts, or networks disclosed, that have some relationship with the requested Internet resource, such as the meta tags, categories, fingerprints associated with content, and targeted or active content. Ex.1002, ¶83. Hubbard-495 discloses that “scoring criteria” may include “associations” for the Internet resource. Ex.1002, ¶83. For example,

Hubbard-495 discloses “meta tag categories associated with *other* URLs associated with the URL host (e.g., such as in the URL database 180 or the processed web page properties database 324),” and “categories associated with other URLs of the URL host (e.g., in the URL database 180).” Ex.1004, 18:61-19:13. Hubbard-495 further describes scores “based on the relative number of URLs in particular networks or domains that have a particular category,” such as “[i]f 95% of the URLs for a particular network in the URL database 180 are classified as having malicious active content, new URLs may be given a score indicative of the likelihood that other URLs referencing servers in the same network are also likely to have such targeted content.” *Id.*, 20:6-21.

Location. Location may include “the hosting country, the registration country, the region and the city,” as well as “the consistency between the registering and hosting country and the country associated with the IP address.” Ex.1001, 9:21-26. As discussed in Section VIII.A.1.f for limitation 1[c3], Hubbard-495 discloses location as a factor. Ex.1002, ¶¶85-89.

- f. 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,”

Hubbard-495 describes several examples of location data that “scoring criteria” may include, such as “[g]eo-location data associated with the URL (e.g., the URL host or host domain)” that can be used to determine or infer the country of

the URL. Ex.1004, 18:61-66. Indeed, identifying a “web site as being based in a particular country or with a particular service provider” could be “useful in scoring because certain countries and service providers have been correlated with certain types of web content due to different laws or lax enforcement of laws.” *Id.*, 20:8-14.

First, Hubbard-495 discloses determining a reputation score based on country of domain registration. Hubbard-495 discloses generating a reputation score “based on information about the registrar of the site (e.g., the domain name of a URL host). Such information may include the identity of the registrar, the registrant (including address and contact information),...and ***any other registrar data including data provided by the WHOIS protocol*** (e.g., Internet Engineering Task Force (IETF) RFC-3912).” The WHOIS protocol will return the data about the “Registrant Country” that is provided at the time someone registers/updates the domain name. *See, e.g.*, Ex.1011, 71-76 (describing obtaining the domain’s registered address through WHOIS lookup to determine location, including by country). A POSITA would understand that information about the registrant, such as “address and contact information of the registrant” and “registrar data including data provided by the WHOIS protocol,” would include the country of domain registration. Ex.1002, ¶86.

Second, Hubbard-495 discloses determining a reputation score based on country of service hosting. Hubbard-495 discloses that scoring criteria may include “[g]eo-location data associated with the URL” and “the network or blocks of IP

addresses associated with the host IP address or its domain.” Ex.1004, 18:61-19:2. Hubbard-495 also discloses that “entire subnetworks (e.g., all addresses matching 128.2.*.* may have a particular score)” and that such “networks or subnetworks help identify a web site as *being based in a particular country or with a particular service provider.*” *Id.*, 20:6-11. A POSITA would understand that a particular service provider provides service hosting within a particular country. Ex.1002, ¶88. A POSITA would also understand that a service provider controls a portion of a network or subnetwork of IP addresses, for lease to customers to connect hosts to the Internet. Ex.1002, ¶88. Thus, information about the country of service hosting could also be derived from geo-location data associated with the URL and the service provider that provides the IP address. Ex.1002, ¶88.

Third, Hubbard-495 discloses determining a reputation score based on the country of an internet protocol address block. Hubbard-495 discloses generating a reputation score based on “the network or *blocks of IP addresses associated with the host IP address or its domain.*” *Id.*, 18:61-19:2. Hubbard-495 also discloses “assign[ing] scores to entire subnetworks (e.g., all addresses matching 128.2.*.* may have a particular score)” and that such “networks or subnetworks help identify a web site as *being based in a particular country or with a particular service provider.*” *Id.*, 20:6-11. A POSITA would understand that “entire subnetworks (e.g., *all addresses matching 128.2.*.**)” describe IP address blocks. Ex.1002, ¶89.

- g. 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”

Hubbard-495 discloses determining a reputation score based on two or more legitimacy factors, such as age of a domain registration, popularity rank, internet protocol address, number of hosts, and top-level domain.

First, Hubbard-495 discloses determining a reputation score based on age of a domain registration. Hubbard-495 teaches “scoring criteria” may include “***creation date*** or expiration date ***associated with the registration of the URL host.***” Ex.1004, 18:61-19:6. Hubbard-495’s reputation scoring module 331 may also use “information about the registrar of the site (e.g., the domain name of a URL host)” such as “***when the registrar record was created***” to generate a reputation indicator. *Id.*, 20:22-28. A POSITA would understand that the creation date associated with the registration of the URL host or the registrar record would constitute the age of a domain registration. Ex.1002, ¶90. A POSITA would further understand that domains with earlier creation dates (hence, larger ages) would generally be considered more stable and trustworthy. Ex.1002, ¶90.

Second, Hubbard-495 discloses determining a reputation score based on popularity rank. Hubbard-495 discloses that “scoring criteria” may include “scoring based on site (host or domain) access statistics (e.g., generate higher reputation scores for frequently visited sites than for infrequently visited sites because

frequently visited sites...are less likely to have targeted content in newly visited URLs).” Ex.1004, 18:61-19:22. A POSITA would understand that scoring based on how frequently sites are visited would mean scoring based on popularity rank (i.e., popularity with visitors). Ex.1002, ¶91.

Third, Hubbard-495 discloses determining a reputation score based on IP address. Hubbard-495 discloses that “scoring criteria” may evaluate several different IP-address-related factors: “the name server that provides the IP address of the URL host or its domain, the network or blocks of IP addresses associated with the host IP address or its domain” and “historical data associated with the IP address of the URL host.” Ex.1004, 18:61-19:22. Hubbard-495 further discloses that the “IP address 230 may be used to identify websites that are hosting multiple domains of questionable content under the same IP address or on the same server.” *Id.*, 15:60-63. A POSITA would understand that an “internet protocol address” factor would include scoring based on information *about* the IP address. Ex.1002, ¶92.

Fourth, Hubbard-495 discloses determining a reputation score based on number of hosts. The number of hosts can be inferred from the “number of IP addresses associated with the domain.” Ex.1001, Table One. Hubbard-495 discloses that the reputation scoring module 331 may “generate a score based on the frequency with which the IP address changes for a particular...domain.” Ex.1004, 20:60-64. Thus, a POSITA would have understood the frequency of IP address changes for a

particular domain reflects the “number of hosts” for a particular domain within a given time period. Ex.1002, ¶93.

Fifth, Hubbard-495 discloses determining a reputation score based on top-level domain. Hubbard-495 discloses “the IP address 230 may be used to identify *websites that are hosting multiple domains* of questionable content under the same IP address or on the same server.” Ex.1004, 15:61-63. Hubbard-495 discloses that “the gateway server module 120 may rely at least in part on the top-level category of the domain in combination with the analysis by the reputation scoring module 331.” Ex.1004, 11:21-25.

- h. 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”

Hubbard-495 discloses determining a reputation score based on one or more behavior factors, such as plurality of run-time behaviors, script block count, and picture count.

First, Hubbard-495 discloses determining a reputation score based on a plurality of run-time behaviors. A POSITA would understand that “run-time” is descriptive of “[o]ccurring after a program has begun to be executed, such as evaluation of variable expressions and dynamic allocation of memory,” and that run-time behaviors would refer to how a program behaves at run-time, including how it interacts with other files and programs. Ex.1002, ¶96. Hubbard-495’s active analysis

module 332 may “*execute[] active content of a web page to identify its behavior properties*,” which may “then *be used to score* and classify the web page.” Ex.1004, 21:16-20. The active analysis module 332 “may provide a behavioral score or data associated with one or more behavior properties (e.g., a property such as ‘writes to registry’).” Ex.1004, 21:24-28. Hubbard-495 further discloses a sandbox module 370 that “monitors the state of the computer to *identify behavior of the web content affecting*, for example, ...*network access, processor usage, [and] memory usage*.” *Id.*, 22:6-11. A POSITA would understand these disclosures to encompass run-time behaviors of the web page/content. Ex.1002, ¶97.

Second, Hubbard-495 discloses determining a reputation score based on script block counts. Hubbard-495 discloses associating categories with the candidate URLs based on the “counts of the properties for each URL,” including “keywords to be identified in the document such as ‘<javascript>.’” *Id.*, 16:66-17:5. In Figure 13C, Hubbard-495 teaches that HTML content that includes more than two “<javascript>” block tags may be categorized as “Malicious.”

Definitions Database

Expression	Category
Content-Type = HTML and “<javascript>” > 2	Malicious
<object> = 6 and URL matches “a.com”	Gambling
“data=,*\txt” = “data=xyx333.txt	Spyware

Ex.1004, Fig.13C (annotated).

Hubbard-495 further discloses storing “counts of the keyword or regular expression found to be associated with each web page,” such as for example: “the value 3 referring to the number of times that the property ‘<javascript>’ appears in the page.” *Id.*, 17:33-47. A POSITA would understand that evaluation of the existence and number of times that Javascript entities are called is a type of “script block.” Ex.1002, ¶100.

Third, Hubbard-495 discloses determining a reputation score based on picture count. Hubbard-495 teaches “potentially executable web content may also be malicious content” and that “image files have been used to exploit vulnerabilities in certain operating systems when those images are processed for display.” *Id.*, 4:25-28. A POSITA would understand that image files may be embedded in web pages using an “” tag. Ex.1002, ¶102. Hubbard-495 discloses storing “numeric values for each *property*/URL corresponding to the keyword properties to *indicate the number of times that the particular property was found in the web page.*” Ex.1004, 17:57-61. “The content filtering module 150 may be configured to parse the returned page and *identify URL links in the returned search results and embedded items of content such as images or active content.*” *Id.*, 8:37-41. A POSITA would understand that a “particular property” “found in the web page” would include the items parsed by the content filtering module 150, such as “embedded items of content such as images or active content.” Ex.1002, ¶102.

- i. 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.”

The '386 Patent describes transmitting a “decision transmission” to the client that varies depending on whether access to the Internet resource was allowed or not. In a situation in which access is allowed, the '386 Patent explains “the decision transmission is the Web page for the Web site.” Ex.1001, 5:37-42.

Hubbard-495, alone or in combination with Hubbard-174, discloses this limitation. Ex.1002, ¶¶104-12. Hubbard-495 discloses that the gateway server module 120 may determine whether a “user will be allowed access to the website associated with the requested URL.” Ex.1004, 9:55-58. A POSITA would understand that an end user would not be able to view the allowed request unless the response had been transmitted *back* to the Internet-enabled client application of the client-side device that made the request. Ex.1002, ¶105. Hubbard-495 discloses client computers that may include “software modules such as *web browsers*,” and that each of the client computers may be in “communication with a gateway server module 120,” which is “in two way communication” with the client computers and the Internet. Ex.1004, 4:46-51, 6:19-23. “Thus, *requests* originating within” the client computers “may be required to pass through the gateway server module 120 as they proceed to the Internet.” *Id.*, 6:24-26. Hubbard-495 further discloses that the URL request from the client computer may be “intercepted at the Internet gateway

and forwarded to the gateway server module 120,” and the URL record is analyzed “to determine whether the category of the URL is one that should be blocked for the workstation user.” *Id.*, 22:53-62. “If the category is blocked, the process skips to block 1212 and the request is blocked. If the category is not blocked, however, the request is allowed at block 1208.” *Id.*, 22:62-65.

In addition, this claim limitation is obvious in view of Hubbard-174, which “specifies the action taken with respect to each data item such as ‘Observe’, ‘**Allow**’, or ‘**Block**.’” Ex.1005, 13:20-22. Hubbard-174 discloses a “content filtering module” that modifies Internet content to only show users material that is deemed safe. Ex.1005, 6:49-65. Hubbard-174 explains that, when modifications occur, “the *modifications* to the image search page 280 performed by the content filtering module 149 *are visible to the user and shown as blocks of disallowed data*” while the page 280 “includes *allowed images 282 returned by the search engine 113 and unobstructed by the gateway server module 120*, and also includes notifications of *blocked images 284*.” *Id.*, 14:46-52. The blocked images 284 may also be “replaced by a display element *notifying the user that the image has been blocked*.” *Id.*, 14:52-54.

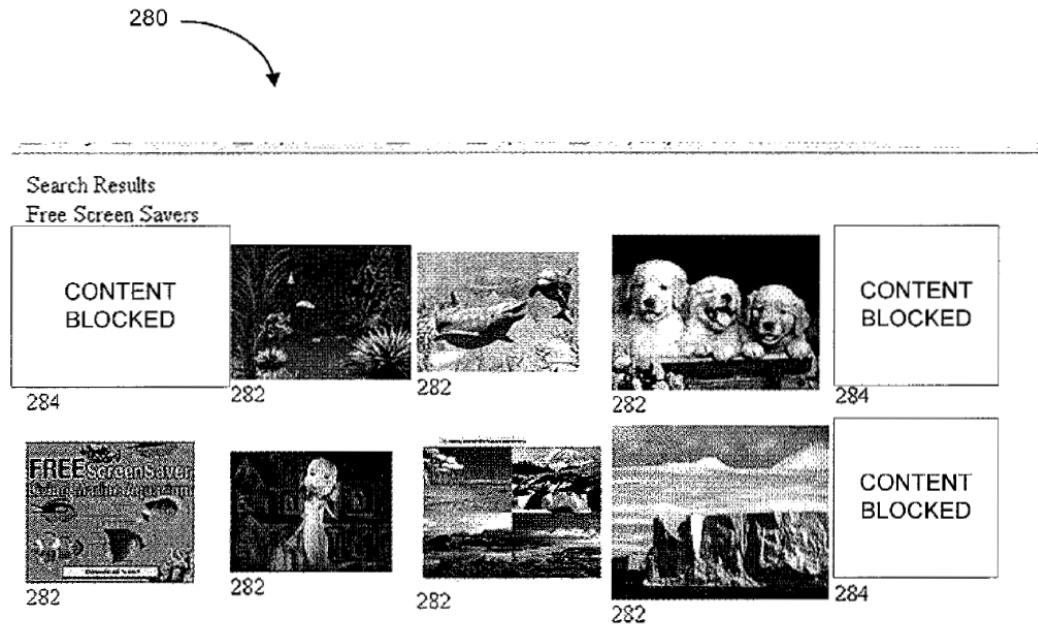


FIG. 14

Ex.1005, Fig.14.

In Figure 14, the allowed images constitute decisions to allow access to an Internet resource and are transmitted to the user (the images appearing on the display). The blocked images constitute decisions to deny access to an Internet resource, and the notifications that content has been blocked are transmitted to the user (the “CONTENT BLOCKED” boxes on the display). In this situation, a POSITA would understand that Hubbard-174 transmitted 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.1002, ¶111.

Further, a POSITA would understand that it would be desirable to transmit a decision transmission to the Internet-enabled client application on the workstations, for example, if the web content is blocked. Otherwise, a user may be confused that the request for the web content has merely been lost or delayed. Ex.1002, ¶107.

2. Claim 2

- a. “The method according to claim 1, wherein the reputation index for the Internet resource is at or above the threshold value and wherein the decision transmission is access to the Internet resource, the method further comprises transmitting the request for the Internet resource over the Internet to the first server for the Internet resource and receiving the Internet resource at the local area network.”

Hubbard-495, alone or in combination with Hubbard-174, discloses this limitation. Ex.1002, ¶¶113-16. Hubbard-495 discloses a scenario in which the Internet resource is at or above the threshold value as discussed for limitation 1[c1]. When a request is allowed, Hubbard-495, alone or in combination with Hubbard-174, teaches that the decision transmission is access to the Internet resource as discussed for limitation 1[d]. In addition, Hubbard-495 discloses “transmitting the request for the Internet resource over the Internet to the first server for the Internet resource” as discussed for limitations 1[a] and 1[b].

Hubbard-495, alone or in combination with Hubbard-174, further discloses receiving the Internet resource at the local area network. As discussed for limitation 1[a], Hubbard-495 discloses a client-side device of a local area network making a

request for an Internet resource. A POSITA would understand that “allow[ing] access” would mean allowing the client device to receive the requested Internet resource at the local area network. Ex.1002, ¶115. For example, Hubbard-174 describes that “[w]hen a user submits a search request to the search engine 113,” “results are returned to the user in a web page which displays data about the relevant pages and URL links which allow the user to access the identified pages.” Ex.1005, 12:30-39. Hubbard-495 discloses that a gateway server module may filter “portions of search results returned in response to a network request.” Ex.1004, 8:24-28. A POSITA would understand that such search results “returned” in response to a request would constitute receiving the Internet resource at the client device of the local area network. Ex.1002, ¶115.

3. Claim 3

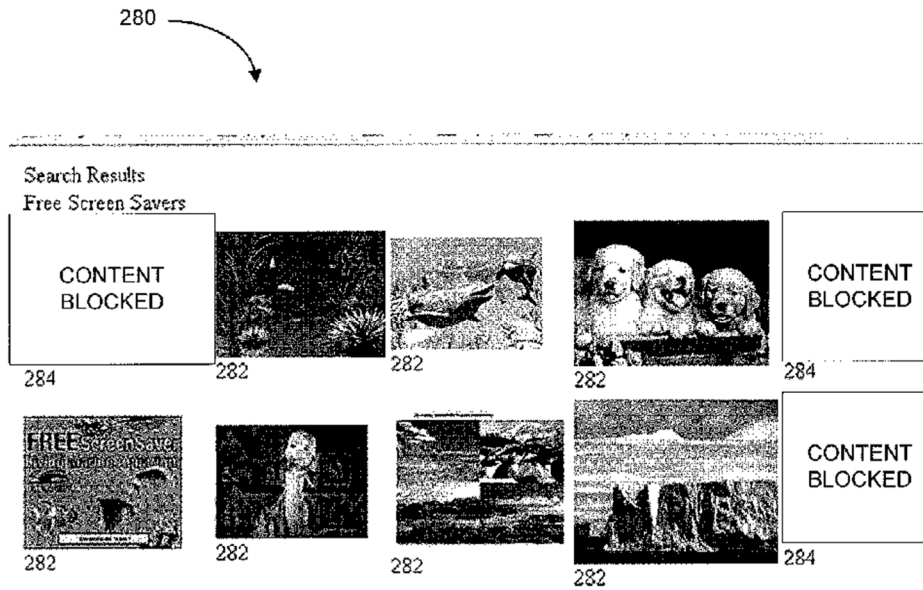
- a. “The method according to claim 1, wherein the reputation index for the Internet resource is below the threshold value, and wherein the decision transmission is a Web page from the local area network containing information that accessing the Internet resource is against an Internet policy established on the local area network.”

Hubbard-495, alone or in combination with Hubbard-174, renders this limitation obvious. Ex.1002, ¶¶117-23. Hubbard-495 discloses “block[ing] access to URLs with low scores (e.g., indicative of poor reputation or higher likelihood of active or other targeted content).” Ex.1004, 11:36-40. A POSITA would understand

“low scores” means the reputation index for the Internet resource is below the threshold value. Ex.1002, ¶119.

Hubbard-495, alone or in combination with Hubbard-174, discloses a “decision transmission” allowing or denying access to the Internet resource for the same reasons explained for limitation 1[d]. Ex.1002, ¶¶104-11. Hubbard-174 discloses that the “gateway module identifies an outgoing network request” and that “[w]hen data is sent back to the workstation 116 in response to the network request, the gateway server module 120 intercepts the returned data.” Ex.1005, 15:50-57. The gateway server module, which in some embodiments resides on the local area network, *id.*, 4:29-38, Fig.1, “modifies the content by either ***removing or blocking the objectionable content*** as identified in accordance with the ***policies defined in the policy module 142***,” *id.*, 16:21-25. “Once the content filtering module 148 has completed its modifications of the intercepted page, ***the modified page is then sent to the originating workstation 116***.” *Id.*, 6:25-28. A POSITA would understand that this modified page, created at the gateway server module 120 of the local area network, would necessarily be a Web page from the local area network. Ex.1002, ¶122.

Hubbard-174 further discloses that “the modifications to the image search page 280 performed by the content filtering module 149 are visible to the user” and “includes notifications of ***blocked images 284***.” *Id.*, 14:46-52.



Ex.1005, Fig.14.

The blocked images 284 may also be “replaced by a display element *notifying the user that the image has been blocked.*” *Id.*, 14:52-54. “For example, the notification may indicate that the URL link would access a page categorized as adult content in the URL/ content database 146 and that the policy module 142 has been configured to block such content.” Ex.1005, 13:63-67. A POSITA would understand that a modified image search page containing such a notification would constitute “a Web page from the local area network containing information that accessing the Internet resource is against an Internet policy established on the local area network.” Ex.1002, ¶123.

4. Claim 4

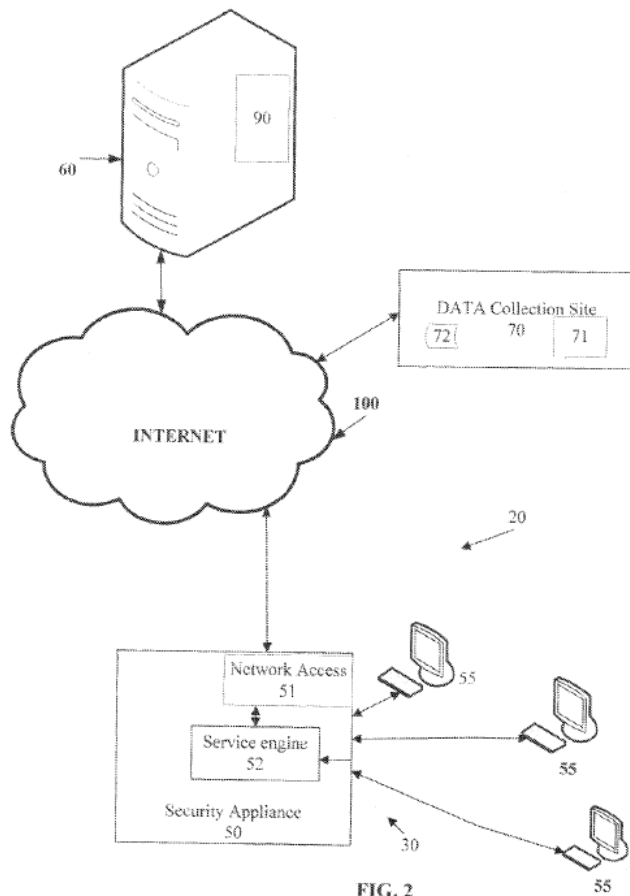
- a. “The method according to claim 1, wherein the Internet resource is one of a Web site, an email server and a voice communications server.”

Hubbard-495 discloses or renders obvious this limitation. Ex.1002, ¶124. Hubbard-495 teaches workstations 116 may be configured to “utilize the network through various software modules such as *web browsers, e-mail programs, or the like.*” Ex.1004, 4:46-49. Hubbard-495 discloses the requested Internet resource may be a website as discussed for limitation 1[a]. Similarly, a POSITA would understand that e-mail programs are configured to retrieve emails from an email server. Ex.1002, ¶124. A POSITA would also understand that the Internet resource could be a voice communications server, as VoIP was well understood at the time. Ex.1002, ¶124.

5. Claim 5

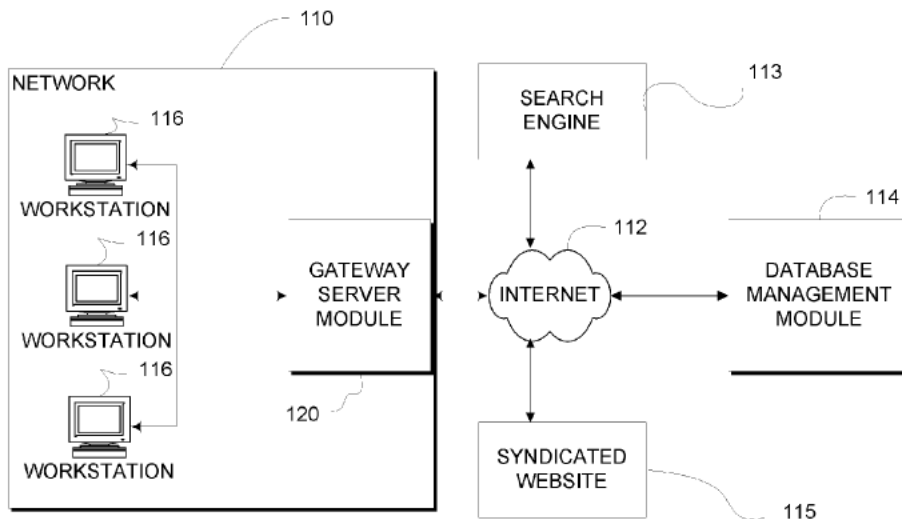
- a. “The method according to claim 1, wherein the reputation index is received from a data collection site accessible by the security appliance over the Internet.”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶125-30. In Figure 2, the ’386 Patent shows that the data collection site 70 is a remote system connected to a security appliance via the Internet. Ex.1001, Fig.2. The ’386 Patent describes a reputation generating site 70, “preferably having a crawler 71 and a database 72,” that “provides reputation indices to service engine 52 of the security appliance 50.” *Id.*, 10:42-58.



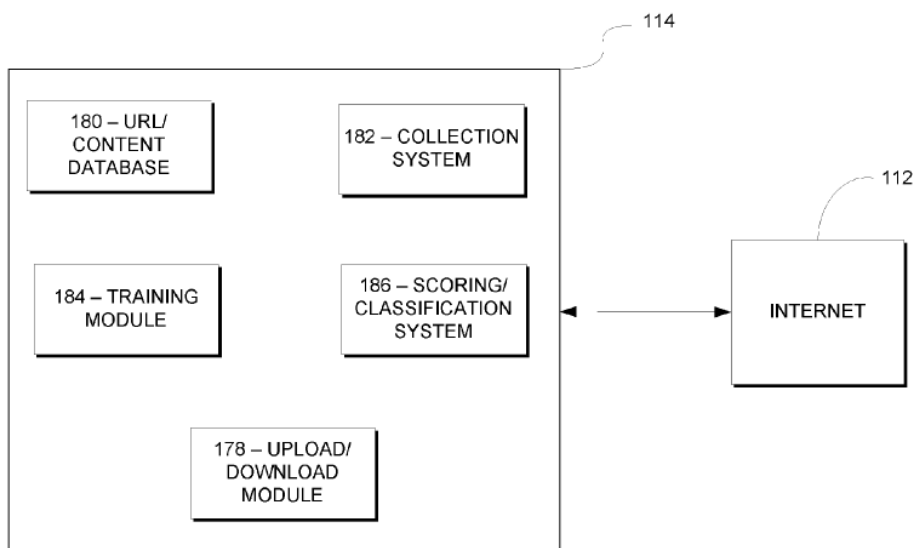
Ex.1001, Fig.2.

Likewise, Hubbard-495 discloses a database management module 114 connected to the gateway server module 120 via the Internet, in Figure 1. *See also* Ex.1004, 12:5-8. A POSITA would understand the gateway server module 120 constitutes the claimed “security appliance” for the same reasons explained for limitation 1[b]. Ex.1002, ¶¶65-67; 125.



Ex.1004, Fig.1.

The database management module 114 of Hubbard-495 further includes a URL/content database 180 and *a collection system 182*, which may include various subsystems such as a “webcrawler module 206,” Ex.1004, Fig.7, 12:55-58, 13:59-14:17, constituting the claimed “data collection site,” Ex.1002, ¶¶126-29; 158.



Ex.1004, Fig.7.

Hubbard-495 further discloses “a remotely located *reputation scoring module*,” which may be a reputation scoring module 331 “located at the database management module 114” that “communicates the results of the analysis performed by the reputation scoring module 331 *back to the gateway sever module* 120.” *Id.*, 9:43-54. A POSITA would understand a “reputation score” constitutes a “reputation index” as discussed in 1[c]. Ex.1002, ¶¶72; 125. A POSITA would also understand that the sending of scores by the database management module 114 to the gateway server module 120 would also mean receiving the scores at the gateway server module 120 from the database management module 114. Ex.1002, ¶130.

6. Claim 6

- a. “The method according to claim 1, wherein the reputation index is stored at a remote reputation generating site.”

Hubbard-495 discloses or renders obvious this limitation. Ex.1002, ¶¶131-33. Hubbard-495 discloses that the URL analysis module 149 “may rely upon a *remotely located reputation scoring module*,” which may be a reputation scoring module 331 “located at the database management module 114.” Ex.1004, 9:43-49; *see id.*, Fig.1. The URL analysis module 149 “communicates the requested URL to the database management module 114 *for scoring by the remotely located reputation scoring module 331*.” *Id.*, 9:49-52. The database management module 114 “may also include a database management module URL/content database 180.” *Id.*, 12:25-26. A

POSITA would understand that the reputation score could be stored in the URL/content database of the remotely located database management module 114 for efficiency, and that it would have been obvious to do so. Ex.1002, ¶133. Storing calculation results—such as at the remotely located database management module 114 of Hubbard-495—was a common technique in software design at the time to conserve processing and network resources. *Id.*

7. Claim 7

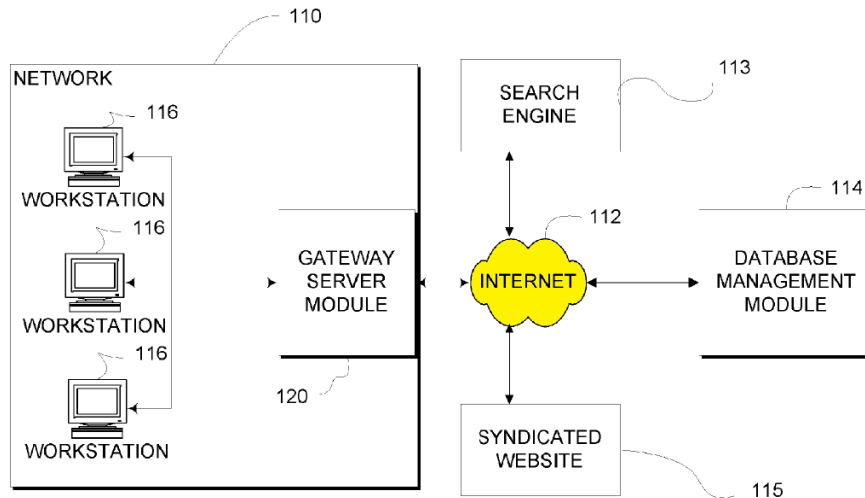
Hubbard-495, alone or in combination with Hubbard-174, renders obvious claim 7. Ex.1002, ¶134.

- a. 7[P]: “A system for controlling access to a Web site, the system comprising:”

To the extent the preamble is limiting, Hubbard-495 discloses “a system for controlling access to web content” served from websites over the Internet. Ex.1004, 2:41-42, 2:52-53, Fig.1; Ex.1002, ¶135.

- b. 7[a]: “a network, the network comprising the Internet;”

Hubbard-495 discloses this limitation in Figure 1. Ex.1002, ¶136.

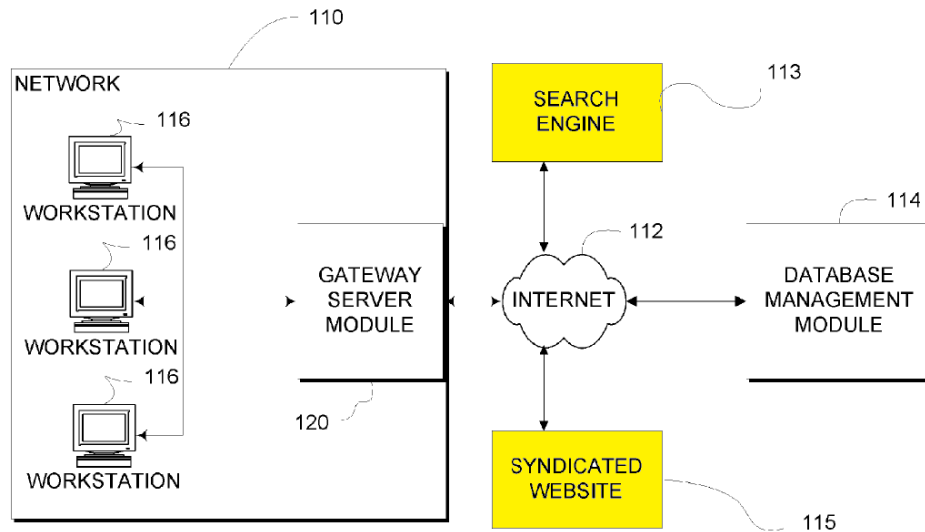


Ex.1004, Fig.1 (annotated).

Hubbard-495 teaches that the “gateway server module may reside at the edge of the network 110 so that traffic sent to and from *the Internet 112* may pass through it on its way into or out of the network 110.” Ex.1004, 4:51-54.

- c. 7[b]: “an Internet resource hosted at a first server and accessible over the Internet; and”

Hubbard-495 discloses this limitation in Figure 1. Ex.1002, ¶¶137-38.

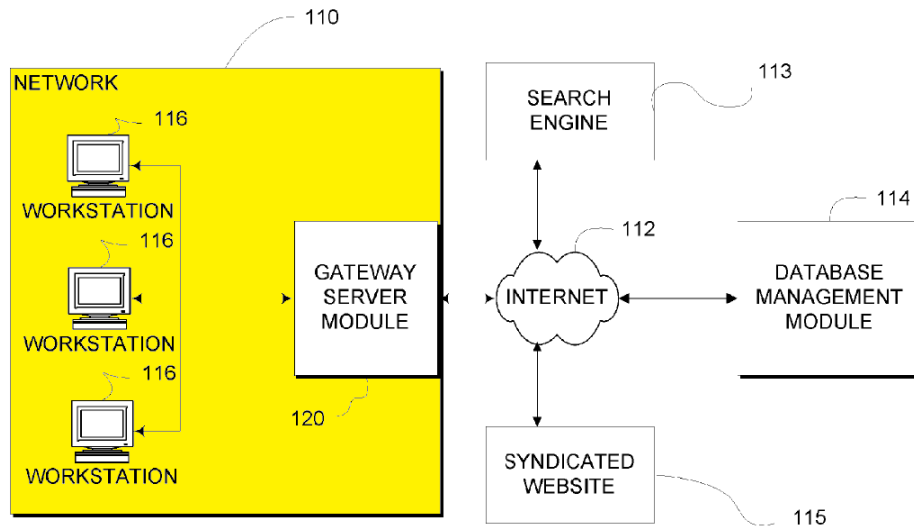


Ex.1004, Fig.1 (annotated).

In Figure 1, the search engine 113 and the syndicated website 115 are accessible via the Internet 112. Ex.1004, 5:1-7, 5:48-51. A POSITA would understand that the search engine 113 and the syndicated website 115 are examples of Internet resources that would be hosted at a server. Ex.1002, ¶137.

- d. 7[c]: “a local area network, the local area network comprising:”

Hubbard-495 discloses limitation 7[c] as discussed in 1[a], which recites a “local area network” (and other features). Ex.1002, ¶¶57; 139.

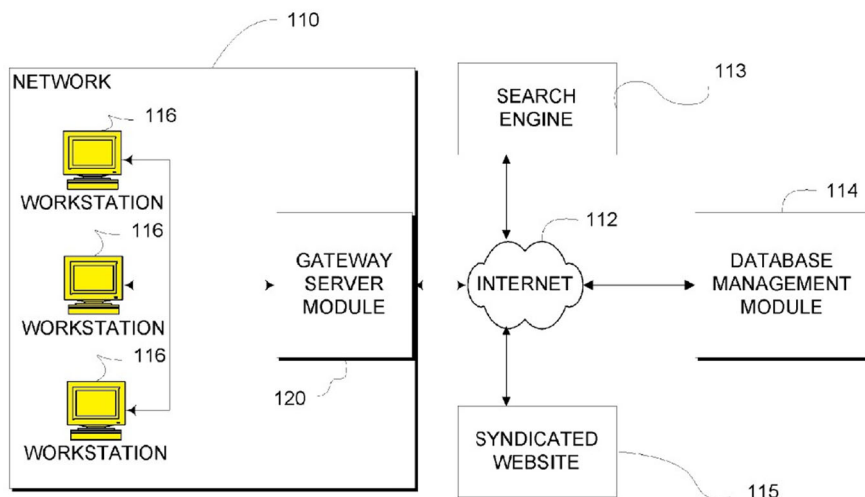


Ex.1004, Fig.1 (annotated).

- e. 7[d]: “a plurality of client-side devices, each of the client-side devices having a browser; and”

Hubbard-495 discloses limitation 7[d] as discussed in 1[a]. Ex.1002, ¶¶57-59;

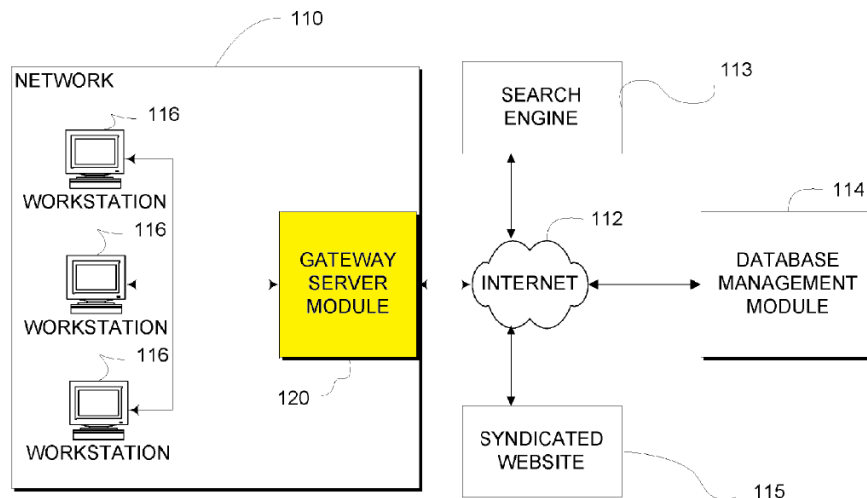
140.



Ex.1004, Fig.1 (annotated).

- f. 7[e1]: “a security appliance, the security appliance controlling access to the Internet by each of the plurality of client-side devices,”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶141-44. A POSITA would understand that the gateway server module 120 of Hubbard-495 would constitute the “security appliance,” as discussed in 1[b]. Ex.1002, ¶¶65-67; 143.



Ex.1004, Fig.1 (annotated).

Hubbard-495 discloses that “*requests originating within the workstations 116 of the network 110 may be required to pass through the gateway server module 120 as they proceed to the Internet.*” Ex.1004, at 6:24-26. The gateway server module 120 “may receive URL requests” from the workstations 116, *id.*, 6:34-36, and “determines whether to *allow access* to the URL based at least partly on the reputation score.” *Id.*, 27:51-53; *see id.*, 27:58-61. A POSITA would understand that by determining whether to allow access to a website or URL by the workstations

116, the gateway server module 120 controls access to the Internet by each of the plurality of client-side devices. Ex.1002, ¶144.

- g. 7[e2]: “the security appliance having a service engine for analyzing a reputation vector for the Web site and generating a reputation index for the Web site from the reputation vector,”

Hubbard-495 discloses this limitation. Ex.1002, ¶145. Hubbard-495 discloses that after “the URL analysis module 149 of the gateway server module 120” “receives a request for a URL from a workstation 116,” “a *reputation scoring module generates a reputation score* or other reputation indicator of targeted content associated with the URL.” Ex.1004, 27:34-40; *see id.*, 9:29-33. “The reputation scoring module *may be located locally at the gateway server module 120.*” *Id.*, 27:40-42. “When located within the gateway server module 120, the reputation scoring module...*may directly analyze* the reputation of the URL.” *Id.*, 9:34-38. A POSITA would understand the reputation scoring module located within the gateway server module 120 would constitute the claimed “service engine for analyzing a reputation vector for the Web site.” Ex.1002, ¶145. Hubbard-495 discloses that “the reputation scoring module 331 may *generate the scores based on information about the URL of the web page.*” Ex.1004, 18:61-19:22. For the reasons described in 1[c2], a POSITA would understand that the information about the URL (an Internet resource) on which a reputation score may be based would constitute the claimed “reputation vector.” Ex.1002, ¶¶79-80;145.

- h. 7[e3]: “the reputation vector comprising a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location,”

Hubbard-495 discloses limitation 7[e3] as discussed in 1[c2]. Ex.1002, ¶¶78-84;146.

- i. 7[e4]: “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,”

Hubbard-495 discloses limitation 7[e4] as discussed in 1[c3]. Ex.1002, ¶¶85-89;147.

- j. 7[e5]: “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”

Hubbard-495 discloses limitation 7[e5] as discussed in 1[c4]. Ex.1002, ¶¶90-95;148.

- k. 7[e6]: “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;”

Hubbard-495 discloses limitation 7[e6] as discussed in 1[c5]. Ex.1002, ¶¶96-103;149.

- l. 7[f]: “wherein access to the Internet resource by any of the plurality of client-side devices is determined based on the reputation index exceeding a threshold value established for the local area network.”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶150-54. As discussed above for other limitations, Hubbard-495 discloses access to the Internet resource by any of the plurality of client-side devices (1[P], 1[a]) determined based on the reputation index exceeding a threshold value established for the local area network (1[c1]). This limitation is further obvious as explained in 1[d].

8. Claim 8

- a. “The system according to claim 7, wherein the client-side device is a personal computer or a PDA.”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶155-156. Hubbard-495 discloses that the client computers 116 “may be *desktop computers, notebook computers, handheld computers or the like.*” Ex.1004, 4:44-49. A POSITA would understand these as “personal computers.” Ex.1002, ¶156. Similarly, a POSITA would understand that a PDA is a type of handheld computer. Ex.1002, ¶156.

9. Claim 9

- a. “The system according to claim 7, further comprising a data collection site accessible over the Internet, the security site having a crawler for collecting a plurality of factors from a plurality of Internet resources.”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶157-62.

Hubbard-495 discloses a data collection site accessible over the Internet as discussed for claim 5.

A POSITA would understand that the claimed “security site having a crawler for collecting a plurality of factors from a plurality of Internet resources” refers to the “data collection site.”⁴ Ex.1002, ¶158.

Hubbard-495 discloses a data collection site having a crawler for collecting a plurality of factors from a plurality of Internet resources. A POSITA would understand the database management module 114 of Hubbard-495 would constitute the claimed “data collection site.” Ex.1002, ¶¶126-29; 158; *supra* § VIII.A.5.

Hubbard-495 discloses that the database management module 114 may include a webcrawler module 206 and honey client module 208. Ex.1004, 12:55-58, 13:59-14:17; *see id.*, Fig.9. A POSITA would understand this to constitute the claimed “crawler.” Ex.1002, ¶160.

⁴ The '386 Patent describes a reputation generating site 70 or data collection site 70, “preferably having a crawler 71 and a database 72,” that “provides reputation indices to...the security appliance 50.” Ex.1001, 10:42-58.

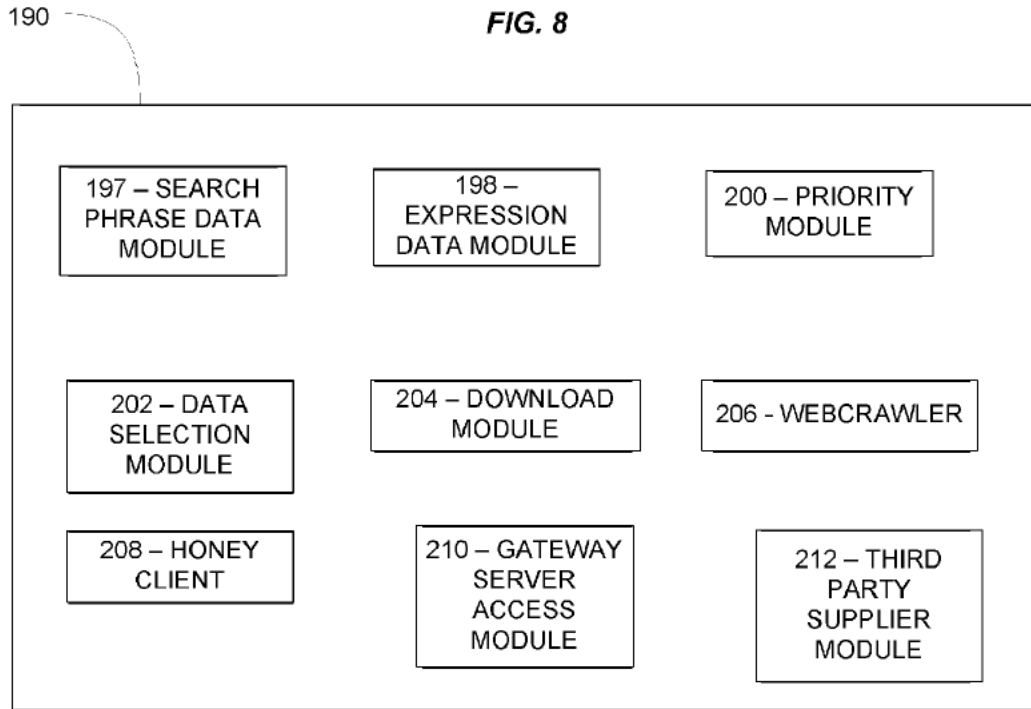


FIG. 9

Ex.1004, Fig.9.

The webcrawler module 206 “may be configured...to simultaneously *crawl many websites* and report the visited URLs back to the database management module URL/content database 180.” *Id.*, 14:3-8. The honey client module 208 may be “configured to mimic the behavior of a web browser” that may “*visit the web sites* and track the behavior of the websites and *download the content back to the URL/content database 180 for further analysis.*” *Id.*, 14:8-17. Hubbard-495 discloses honey miners “similar to a web crawler,” but “unlike the web crawler which merely visits the website and reports the URL links available from that site, the passive honey miners may be configured to *download the page content and*

return it to the control servers 220 for insertion into the URL database 180.” Id., 14:57-64. The collected content may include “a URL 232,” “the page content 234 for a particular URL,” and an “indication of whether the URL has executable content 236 within its page code.” Ex.1004, 16:1-20. A POSITA would understand that the collected data would encompass various information about the URLs of visited web pages, i.e., a plurality of factors from a plurality of Internet resources. Ex.1002, ¶161.

10. Claim 10

- a. “The system according to claim 9, wherein the data collection site has a database containing reputation indices for a plurality of Internet resources.”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶163-66. Hubbard-495 discloses a database management module 114 (that may include a reputation scoring module) that constitutes the claimed “data collection site” as explained for claim 5. Ex.1002, ¶¶126-29; 163. The database management module 114 “may also include a database management module URL/content database 180.” Ex.1004, 12:25-26. The URL/content database 180 “may take the form of a data warehouse which stores URL strings and information about *URLs* that have been collected by a collection system 182.” *Id.*, 12:27-31. Further, “[i]n one embodiment, the URL database 180 includes the *categorized web page database.*” *Id.*, 27:8-9; *see id.* 27:43-61. A POSITA would understand that the URL/content database 180 contains information regarding a plurality of Internet resources, as Hubbard-495 discloses a database

containing information about multiple URLs, a type of Internet resource. Ex.1002, ¶¶164-66. It would have been obvious to a POSITA to store reputation scores in the URL/content database 180, along with other information about the URLs, for efficiency. Ex.1002, ¶¶165-66. Storing calculation results—such as at the database management module of Hubbard-495—was a common technique in software design at the time. Ex.1002, ¶165.

11. Claim 11

Hubbard-495, alone or in combination with Hubbard-174, renders obvious claim 11. Ex.1002, ¶167.

- a. 11[P]: “A method for controlling access to an Internet resource, the method comprising:”

If the preamble is found limiting, Hubbard-495 discloses this limitation as explained for 1[P]. Ex.1002, ¶¶54-55, 168.

- b. 11[a]: “transmitting a request for an Internet resource from a Web browser for a client-side device of a local area network, the Internet resource residing at a first server;”

Hubbard-495 discloses limitation 11[a] as explained in 1[a]. Ex.1002, ¶¶56-62, 169.

- c. 11[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;”

Hubbard-495 discloses limitation 11[b] as explained in 1[b]. Ex.1002, ¶¶63-69, 170.

- d. 11[c1]: “accessing a reputation index for the Internet resource,”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶71-77; 171-172. Hubbard-495 discloses that “the reputation scoring module 331 *may generate the scores based on information about the URL of the web page.*” Ex.1004, 18:61-19:22. “Each *reputation score* may then be unique to each website URL and *relied upon by the gateway server module 120* to determine...if...the user will be allowed to access the content associated with each scored website URL.” *Id.*, 10:64-11:2. A POSITA would understand that the gateway server module 120 would need to access the generated reputation score in order to rely upon the score to determine whether access would be allowed for the requested web content, which a POSITA would understand to be an Internet resource. Ex.1002, ¶172.

- e. 11[c2]: “the reputation index based on a reputation vector for the Internet resource comprising security history, legitimacy, behavior, associations and location,”

Hubbard-495 discloses limitation 11[c2] as explained in 1[c2]. Ex.1002, ¶¶78-84, 173.

- f. 11[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,”

Hubbard-495 discloses limitation 11[c3] as explained in 1[c3]. Ex.1002, ¶¶85-89, 174.

- g. 11[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”

Hubbard-495 discloses limitation 11[c4] as explained in 1[c4]. Ex.1002, ¶¶90-95, 175.

- h. 11[c5]: “wherein the behavior factor of the plurality of factors for the reputation vector comprises at least one of: plurality of run-time behaviours, script block count, picture count, immediate redirect and response latency;”

Hubbard-495 discloses limitation 11[c5] as explained in 1[c5]. Ex.1002, ¶¶96-103, 176.

- i. 11[d]: “determining if the reputation index for the Internet resource is at or above a threshold value established for the local area network; and”

Hubbard-495 discloses limitation 11[d] as explained in 1[c1]. Ex.1002, ¶¶71-77, 177.

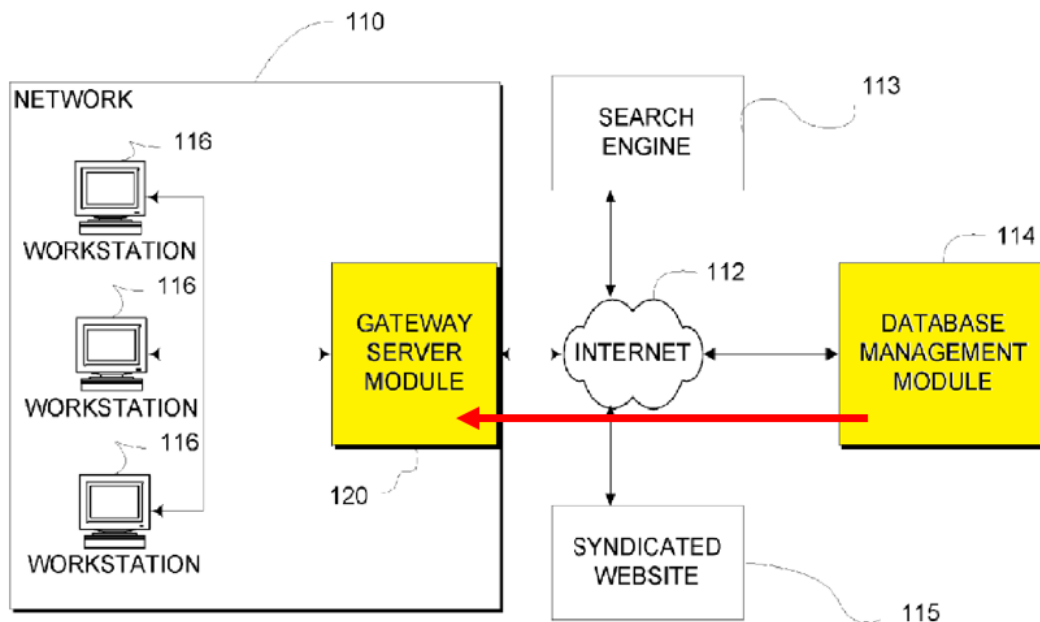
- j. 11[e]: “transmitting a decision transmission to the Web browser of the client-side device, the decision transmission allowing or denying access to the Internet resource.”

Limitation 11[e] is obvious as explained in 1[d]. Ex.1002, ¶¶104-11; 178. A POSITA would understand that a “Web browser” is simply a type of “Internet-enabled client application.” Ex.1002, ¶178.

12. Claim 12

- a. “The method according to claim 11, further comprising transmitting the reputation index over the Internet to the local area network.”

Hubbard-495 discloses this limitation as explained in claim 5. Ex.1002, ¶¶126-29; 179-80. Hubbard-495 discloses the database management module 114 “communicates the results of the analysis performed by the reputation scoring module 331 back to the gateway server module 120.” *Id.*, 9:49-54. As illustrated in Figure 1, a POSITA would understand that this involves transmitting the “results of the analysis performed by the reputation scoring module” in the database management module over the Internet to the local area network 110. Ex.1002, ¶180.



Ex.1004, Fig.1 (annotated).

13. Claim 13

Hubbard-495, alone or in combination with Hubbard-174, renders obvious claim 13. Ex.1002, ¶181.

- a. 13[P]: “A method for building a reputation database for Internet resources, the method comprising:”

Hubbard-495 discloses the preamble, to the extent it is limiting. Ex.1002, ¶¶182-84. Hubbard-495 discloses “a database management module URL/content database 180” that “may take the form of a data warehouse which stores URL strings and information about URLs that have been collected.” Ex.1004, 12:25-31; *see id.*, Fig.12. The “URL/content database 180 may be a relational database that is indexed to provide quick and effective searches for data.” *Id.*, 12:31-33. As explained for claim 6, a POSITA would understand the reputation score could be stored in the database to “provide quick and effective searches for data” and to minimize repeated calculations if a reputation score is requested for the same URL. Ex.1002, ¶183.

As explained for claim 9, the collection system 182 may include a webcrawler module 206 and a honey client module 208 that adds information to the URL/content database 180. The URL/content database 180 “may include data such as URL strings, the content associated with those strings, information about how the content was gathered,” and “the date...the URL was written into the URL/content database 180.” *Id.*, 12:36-42. A POSITA would understand that since Hubbard-495

describes methods to populate such databases and possible configurations, a method to build a reputation database is described. Ex.1002, ¶184.

- b. 13[a]: collecting a plurality of factors for an Internet resource site to populate a reputation vector for the Internet resource to perform reputation analysis of the Internet resource;”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶185-88. Hubbard-495 discloses a collection system 182, which may include a database management collection module 190 “associated with one or more collection sources 194 from which it may *collect data about URLs.*” *Id.*, 12:55-13:10. The database management collection module 190 “may be used by the database management module 114 to *collect data for the URL/content database 180 about URLs.*” *Id.*, 12:58-61. The URL/content database 180 “may take the form of a data warehouse which stores *URL strings and information about URLs* that have been *collected by a collection system 182.*” *Id.*, 12:27-31. A POSITA would understand that the collected information for the Internet resource would be used to populate the information about the URL of the web page (e.g., scoring criteria) and constitute the claimed “reputation vector for the Internet resource.” Ex.1002, ¶187.

Further, Hubbard-495 discloses that the reputation scoring module 331 “may *generate the scores based on information about the URL of the web page*” such as “URL content strings,” “meta tag categories associated with other URLs associated with the URL host,” and “categories associated with other URLs of the URL host.”

Ex.1004, 18:61-19:22. A POSITA would understand that the reputation scoring module 331 uses collected information about the URL of the web page (e.g., scoring criteria) to generate a reputation score. Ex.1002, ¶188. As discussed in Section VIII.A.13.i for limitation 13[d], a POSITA would understand generating a reputation score for a URL would constitute performing a reputation analysis of the Internet resource. *Id.*

- c. 13[b]: “receiving the plurality of factors for the Internet resource at a data collection site;”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶189-90. Hubbard-495 discloses a database management module 114 that constitutes the claimed “data collection site” as explained for claim 5. Ex.1002, ¶¶126-29; 190. The database management module 114 may “also include a database management module URL/content database 180,” and “may take the form of a data warehouse which *stores URL strings and information about URLs that have been collected by a collection system* 182.” Ex.1004, 12:25-31. As described in Section VIII.A.13.b for limitation 13[a], the information collected by the collection system 182 would constitute the claimed “plurality of factors for the Internet resource.” A POSITA would understand that the information collected by the collection system 182 must be *received* to be stored. Ex.1002, ¶190.

- d. 13[c1]: “constructing a reputation vector for the Internet resource at the data collection site,”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶191-92. As discussed for limitations 13[a] and 13[b], a POSITA would understand that the database management module 114 (data collection site) could collect and store “information about the URL of the web page (e.g., scoring criteria),” i.e., constitute the claimed “reputation vector comprising a plurality of factors for the Internet resource.” Ex.1002, ¶¶185-90; 192. Hubbard-495 teaches that the “database management module URL/content database 180 may be a relational database that is indexed to provide quick and effective searches for data.” Ex.1004, 12:31-33. A POSITA would understand that the database would store information about the URL (plurality of factors) as a vector (e.g., database record) used for determining the reputation of the Internet resource. Ex.1002, ¶192.

- e. 13[c2]: “the reputation vector comprising a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location,”

Hubbard-495 discloses limitation 13[c2] for the same reasons explained for limitation 1[c2], which recites the same features (and other features). Ex.1002, ¶¶78-84, 193.

- f. 13[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,”

Hubbard-495 discloses limitation 13[c3] as discussed in 1[c3]. Ex.1002, ¶¶85-89, 194.

- g. 13[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”

Hubbard-495 discloses limitation 13[c4] as discussed in 1[c4]. Ex.1002, ¶¶90-95, 195.

- h. 13[c5]: “wherein the behavior factor of the plurality of factors for the reputation vector comprises at least one of: plurality of run-time behaviours, script block count, picture count, immediate redirect and response latency;”

Hubbard-495 discloses limitation 13[c5] as discussed in 1[c5]. Ex.1002, ¶¶96-103, 196.

- i. 13[d]: “analyzing the reputation vector to generate a reputation index for the Internet resource based on the analysis of the plurality of factors and the reputation classifier;”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶197-201. Hubbard-495 discloses that “the reputation scoring module 331 may *generate the scores based on information about the URL of the web page (e.g., scoring criteria).*” Ex.1004, 18:61-19:22. In addition, “[t]he database management module 114 may further provide a scoring/classification system 186 which utilizes the definitions and properties created by the training system 184 to provide a score or classification (e.g., a categorization) to web content.” Ex.1004, 12:43-53. In Figure 13C, the categories may include “malicious,” “gambling,” or “spyware.” A POSITA would understand these categories to provide a classification related to the likelihood of the

URL or Internet resource being malicious or spyware, i.e., a reputation classifier. Ex.1002, ¶200. A POSITA would understand to use both information about the URL of the web page and the category classifications of Hubbard-495 to generate a reputation score. Ex.1002, ¶201.

Definitions Database

FIG. 13C

Expression	Category
Content-Type = HTML and "<javascript>" > 2	Malicious
<object> = 6 and URL matches "a.com"	Gambling
"data=,*\txt" = "data=xyx333.txt"	Spyware

Ex.1004, Fig.13C.

- j. 13[e]: "storing the reputation index for the Internet resource at the data collection site; and"

Hubbard-495 discloses limitation 13[e] as discussed for claims 5 and 6.

Ex.1002, ¶¶131-33; 202.

- k. 13[f]: "transmitting the stored reputation index to a local area network upon request for managing access to the Internet resource."

Hubbard-495 discloses or renders obvious this limitation. Ex.1002, ¶¶203-05.

As discussed for claim 12, Hubbard-495 discloses "transmitting the stored reputation index over the Internet to the local area network." Ex.1002, ¶¶179-80; 203.

Hubbard-495 further discloses a "network request" that includes "*user requests* for content." Ex.1004, 5:51-54. Hubbard-495 discloses that such requests "may be required to pass through the gateway server module 120 as they proceed to

the Internet.” *Id.*, 6:24-26. Hubbard-495 discloses that the URL analysis module 149 “*communicates the requested URL to the database management module 114 for scoring by the remotely located reputation scoring module 331*” and that the database management module 114 “*communicates the results of the analysis performed by the reputation scoring module 331 back to the gateway server module 120.*” *Id.*, 9:49-54. The gateway server module “determines whether to *allow access to the URL based at least partly on the reputation score.*” *Id.*, 27:51-53. A POSITA would understand the gateway server module’s request for a reputation score is a request for managing access to the Internet resource. Ex.1002, ¶204. And as discussed in Sections VIII.A.6 and VIII.A.13.j for claim 6 and limitation 13[e], a POSITA would understand that the database management module 114 could store the reputation score for an Internet resource. Ex.1002, ¶205. A POSITA would understand to transmit the reputation score stored in the database to minimize repeat calculations if a reputation score was requested for the same Internet resource, for efficiency. Ex.1002, ¶205. This limitation is further obvious as explained in 1[d].

14. Claim 15

- a. “The method according to claim 13, further comprising obtaining the plurality of factors for the Internet resource using a crawler.”

Hubbard-495 discloses claim 15 for the reasons explained for claim 9. Ex.1002, ¶¶157-62; 206.

15. Claim 16

- a. “The method according to claim 15, wherein obtaining the plurality of factors for the Internet resource comprises accessing the Internet service, analyzing a plurality of HTML documents for the Internet resource, and crawling a plurality of linked Internet resources of the plurality of HTML documents for Internet resource.”

Hubbard-495 discloses this limitation. Ex.1002, ¶¶207-10. Hubbard-495 discloses a collection system 182 that “may include a database management collection module 190,” which may include the webcrawler module 206 and honey client module 208. Ex.1004, 12:55-58, 13:59-14:17. The webcrawler module “may be configured...to simultaneously *crawl many websites* and *report the visited URLs* back to the...URL/content database 180.” *Id.*, 14:3-8. The web crawler “*visits the website and reports the URL links available from that site.*” *Id.*, 14:58-64. A POSITA would understand that visiting the websites would constitute “accessing the Internet service.” Ex.1002, ¶208.

The honey client module may be “configured to mimic the behavior of a web browser” and may “*visit the web sites...and download the content back to the URL/content database 180 for further analysis.*” Ex.1004, 14:8-17. Hubbard-495 further discloses “honey miners” that “may be configured to *download the page content and return it...for insertion into the URL database 180.*” *Id.*, 14:57-64. Hubbard-495 discloses “identifying and categorizing web content, including *potentially executable web content and malicious content*, that is found at locations

identified by [URLs].” *Id.*, 4:3-7. Such web content may include “***executable code embedded in HTML or other hypertext documents***” and “a ***HTML web page that includes an ‘OBJECT’ element***, and thus can cause execution of...executable components.” *Id.*, 4:10-22. Malicious content may refer to “interactive content such as ‘phishing’ schemes in which a ***HTML form or other web content*** is designed to appear [as a trusted site].” *Id.*, 4:28-34. A POSITA would understand that such reporting of websites and web content back to the URL/content database 180 for further analysis would constitute “analyzing a plurality of HTML documents for the Internet resource.” Ex.1002, ¶209.

Hubbard-495 further discloses that “the miners 222 ***may be configured to follow links on the URL content*** so that in addition to visiting URLs..., the miners may visit content that it linked to those URLs.” Ex.1004, 15:9-13. A POSITA would understand that such following of links on the URL content would constitute “crawling a plurality of linked Internet resources of the plurality of HTML documents for Internet resource.” Ex.1002, ¶210.

16. Claim 18

- a. “The method according to claim 13, wherein the stored reputation index is transmitted over the Internet to a local area network.”

Hubbard-495 discloses this limitation as discussed in 13[f]. Ex.1002, ¶¶211-12.

Further, Hubbard-495 discloses a database management module 114 that constitutes the claimed “data collection site” for the same reasons explained for claim 5. Ex.1002, ¶¶126-29; 212. The database management module 114 “may be located remotely (*accessible via Internet 112*) *from the network 110* and its associated workstations 116.” Ex.1004, 12:5-8. A POSITA would understand that the reputation scores could be stored in the database management module URL/content database 180 of the database management module 114, along with other information about the URLs for efficiency. Ex.1002, ¶211. A POSITA would understand that information sent from the database management module 114 to the gateway server module would be over the Internet to the local area network, as the database management module 114 is connected to the gateway server module and the local area network via the Internet. Ex.1002, ¶212.

B. GROUND 2: HUBBARD-495 IN COMBINATION WITH HUBBARD-174 and ALPEROVITCH RENDERS OBVIOUS CLAIMS 1-13, 15, 16, and 18.

1. Claims 1, 7, 11, and 13

Hubbard-495 in combination with Hubbard-174 renders obvious claims 1, 7, 11, and 13 for the reasons explained in Section VIII.A. To the extent that Hubbard-495 does not expressly disclose “the reputation vector comprising a plurality of factors for the Internet resource comprising security history” limitation of claims 1,

7, 11, and 13, a POSITA would have looked to Alperovitch to supply that limitation. Ex.1002, ¶213.

Motivation to Combine

A POSITA would have been motivated to combine Hubbard-495 and Hubbard-174 for the reasons stated in Section VIII.A.1. A POSITA would have been further motivated to combine those references with the disclosures of Alperovitch as each are analogous art to the '386 Patent at least because each is from the same field of endeavor, namely, methods and systems to determine conditions under which access to an Internet resource is allowed. *E.g.*, Ex.1004, 2:33-61; Ex.1005, 1:7-9; Ex.1006, [0073]. Ex.1002, ¶¶216-17.

Further, Hubbard-495 discloses that reputation scores may be generated “based on information about the URL of the web page (e.g., scoring criteria) such as [] the name server that provides the IP address of the URL host or its domain, the network or blocks of IP addresses associated with the host IP address or its domain, active content previously identified with reference to the host, the hosts’ domain, or the URL path, historical data associated with the IP address of the URL host, creation date or expiration date associated with the registration of the URL host,” among others. Ex.1004, 18:53-19:22. Likewise, Hubbard-174 discloses a “scoring/classification system 186 which utilizes the definitions and properties created by the training system 184 to provide a score or classification (e.g., a

categorization) to web content so that the categorization may be delivered via the upload/download module 178 to gateway server modules 120.” Hubbard-174, 10:3-9. A POSITA would understand these to be non-exclusive examples of information relevant to the reputation of the URL. Ex.1002, ¶217. Alperovitch discusses “methods and systems for assigning reputation to communications entities” as “hackers often attempt to use various network-type applications (e.g., e-mail, web, instant messaging (IM) etc.) to create a pre-textual connection with the networks 110 a-n in order to exploit security holes created by these various applications using entities 130 a-e.” Ex.1006, Abstract, [0032]. Hubbard-495 and Hubbard-174 recognize this risk in “phishing” messages in the context of malicious web content, “in which a HTML form or other web content is designed to appear to be provided by another, typically trusted, web site such as a bank, in order to deceive the user into providing credentials or other sensitive information to an unauthorized party.” Ex.1004, 4:28-34; Hubbard-174, 4:10-15. A POSITA would understand that the system of Hubbard-495 and Hubbard-174 could be predictably improved with Alperovitch’s related reputation analysis system. Ex.1002, ¶217.

A POSITA would have had a reasonable expectation of success in enhancing the system of Hubbard-495 and Hubbard-174 with Alperovitch by providing, for example, further “information about the entities 300a-c sending and receiving messages, including, transmission patterns, volume, or whether the entity has a

tendency to send certain kinds of message (e.g., legitimate messages, spam, virus, bulk mail, etc.), among many others” on which to base a reputation score. Ex.1006, [0037]; Ex.1002, ¶217.

- a. “the reputation vector comprising a plurality of factors for the Internet resource comprising security history,”

Claims 1, 7, 11, and 13 of the '386 Patent recite this claim limitation,⁵ which Alperovitch discloses. Ex.1002, ¶¶214-15. 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

⁵ Claim 11 differs slightly—“a reputation vector for the Internet resource comprising security history...[and other factors]”—but does not alter the analysis.

Alperovitch discloses historical events that flag security risks, e.g., a “security history” factor. Ex.1002, ¶215.

2. Claims 2, 3, 5, 6, 8, 9, 10, 12, 15, 16, and 18

Hubbard-495 in combination with Hubbard-174 renders obvious claims 2, 3, 5, 6, 8, 9, 10, 12, 15, 16, and 18 for the reasons explained as to the corresponding claims. *Supra* Sections VIII.A.2-3, 5-6, 8-10, 12, 14-16. Ex.1002, ¶218.

3. Claim 4

- a. “The method according to claim 1, wherein the Internet resource is one of a Web site, an email server and a voice communications server.”

Hubbard-495 discloses or renders obvious the limitations of claim 4 for the reasons explained in Section VIII.A.4. In addition, Alperovitch discloses that “the Internet resource is one of a...voice communications server.” Ex.1002, ¶219. Alperovitch discloses that reputation engines can assist in identifying “malicious communications,” which may include “malicious communications in *an email, instant messaging, VoIP, SMS or other communication protocol system.*” Ex.1006, [0034]. Upon establishing a VoIP call, an IP phone establishes a connection to the local network, which “can be exploited similarly to the way *e-mail, web, instant messaging, or other internet applications* can be exploited for providing unregulated connect to a network.” *Id.*, [0072]. A POSITA would understand that due to the similarities in which VoIP calls and e-mail, web, instant messaging, or other internet applications interact with the local area network,

Hubbard-495's system in view of Alperovitch would extend similarly to voice communications servers, in addition to Web sites and email servers. Ex.1002, ¶219.

IX. SECONDARY CONSIDERATIONS

There is no evidence of secondary considerations that would support a determination of non-obviousness of the claimed subject matter in the '386 Patent.

X. CERTIFICATION OF GROUNDS FOR STANDING UNDER 37 C.F.R. § 42.104

Petitioner certifies pursuant to Rule 42.104(a) that the '386 Patent is available for IPR and that Petitioner is not barred or estopped from requesting an IPR of the Challenged Claims on the grounds identified in this Petition.

XI. MANDATORY NOTICES

A. Real Party-in-Interest Under 37 C.F.R. § 42.8(b)(1)

The real party-in-interest is Forcepoint LLC.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

To the best of Petitioner's knowledge, the '386 Patent is, or has been, involved in the following district court litigations, appeals, and Board proceedings: *Webroot, Inc. et al v. Forcepoint LLC*, No. 6:22-cv-342 (W.D. Tex.) (filed March 31, 2022) (consolidated with lead case No. 6:22-cv-243).

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Lead Counsel	Back-Up Counsel
Kat Li Reg. No. 64,857 kat.li@kirkland.com <u>Postal and Hand-Delivery Address:</u> KIRKLAND & ELLIS LLP 401 Congress Avenue Austin, TX 78701 Telephone: (512) 678-9100 Facsimile: (512) 678-9101	Akshay S. Deoras (<i>pro hac vice</i> to be filed) akshay.deoras@kirkland.com <u>Postal and Hand-Delivery Address:</u> KIRKLAND & ELLIS LLP 555 California Street San Francisco, CA 94104 Telephone: (415) 439-1400 Facsimile: (415) 439-1500 Nadia E. Haghighatian (<i>pro hac vice</i> to be filed) nadia.haghighatian@kirkland.com <u>Postal and Hand-Delivery Address:</u> KIRKLAND & ELLIS LLP 401 Congress Avenue Austin, TX 78701 Telephone: (512) 678-9100 Facsimile: (512) 678-9101

D. Service Information Under 37 C.F.R. § 42.8(b)(4)

Petitioner concurrently submits a Power of Attorney under 37 C.F.R. §42.10(b), and consents to electronic service to Forcepoint_Webrooot_IPR@kirkland.com.

XII. PAYMENT OF FEES UNDER 37 C.F.R. §42.103

The undersigned authorizes the Office to charge the fee set forth in 37 C.F.R. §42.15(a)(1) for this Petition to Deposit Account No. 506092. Review of sixteen claims is requested. The undersigned further authorizes payment for any additional

fees that may be due in connection with this Petition to be charged to the above-referenced deposit account.

XIII. CONCLUSION

Petitioner requests that the Board institute *inter partes* review and cancel claims 1-13, 15, 16, and 18 of the '386 Patent.

Respectfully submitted,

Dated: March 31, 2023

By: /Kat Li/
Kat Li (Reg. No. 64,857)
kat.li@kirkland.com
Nadia E. Haghighatian
nadia.haghighatian@kirkland.com
KIRKLAND & ELLIS LLP
401 Congress Avenue
Austin, TX 78701
Telephone: (512) 678-9100
Facsimile: (512) 678-9101

Akshay S. Deoras
akshay.deoras@kirkland.com
KIRKLAND & ELLIS LLP
555 California Street
San Francisco, CA 94104
Telephone: (415) 439-1400
Facsimile: (415) 439-1500

**CERTIFICATE OF COMPLIANCE WITH
TYPE-VOLUME LIMITATION PURSUANT TO 37 C.F.R. § 42.24**

This brief complies with the type-volume limitation of 37 C.F.R. § 42.24(a)(1)(i).

The brief contains 13,997 words, excluding the parts of the brief exempted by 37 C.F.R. § 42.24(a).

The brief has been prepared in a proportionally spaced typeface using Microsoft Word in a 14-point Times New Roman font.

Dated: March 31, 2023

/Kat Li/
Kat Li (Reg. No. 64,857)

CERTIFICATE OF SERVICE

In compliance with 37 C.F.R. §§ 42.105, 42.6(e), the undersigned hereby certifies that a copy of the foregoing document was served on March 31, 2023, via Federal Express® directed to POs at the correspondence address of record:

Sheridan Ross PC
1560 Broadway, Suite 1200
Denver, CO 80202

A courtesy copy was also served by electronic mail on the attorneys below for the following related matter:

Webroot, Inc. et al v. Forcepoint LLC, No. 6:22-cv-342 (W.D. Tex.)

JEFFREY D. MILLS
jmills@kslaw.com
KING & SPALDING LLP
500 W. 2nd Street, Suite 1800
Austin, TX 78701
Telephone: (512) 457-2027
Telecopier: (202) 626-3737

CHRISTOPHER C. CAMPBELL
ccampbell@kslaw.com
PATRICK M. LAFFERTY
plafferty@kslaw.com
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Washington, DC 20006
Telephone: (202) 737-0500
Telecopier: (202) 626-3737

BRIAN J. EUTERMOSER
beutermoser@kslaw.com
BRITTON F. DAVIS
bfdavis@kslaw.com
KING & SPALDING LLP
1401 Lawrence Street, Suite 1900
Denver, Colorado 80202
Telephone: (720) 535-2300
Telecopier: (720) 535-2400

MARK D. SIEGMUND
mark@cjsjlaw.com
**CHERRY JOHNSON SIEGMUND
JAMES, PLLC**
400 Austin Ave., 9th Floor
Waco, Texas 76701
Telephone: (254) 732-2242
Telecopier: (866) 627-3509

/Kat Li/

Kat Li (Reg. No. 64,857)