

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORCEPOINT LLC,
Petitioner

v.

OPEN TEXT INC.,
Patent Owner

Case IPR2023-00784
Patent No. 8,438,386

PATENT OWNER'S PRELIMINARY RESPONSE

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a)	4
III.	THE ’386 PATENT	20
A.	Inadequacy Of The Prior Art And The Need For Improved Internet Access Control	20
B.	Innovations Of The ’386 Patent	21
C.	Claim Construction.....	26
	“Security History”	27
D.	Level Of Ordinary Skill In The Art.....	28
IV.	THE PETITION IS NOT REASONABLY LIKELY TO SUCCEED	29
A.	Petitioner’s Cited Prior Art References.....	29
1.	Hubbard-495	29
2.	Hubbard-174	32
3.	Alperovitch.....	33
B.	Ground 1: Petitioner Fails To Establish That The Combination Of Hubbard-495 And Hubbard-174 Renders Obvious The “Security History” Factor Limitation In All Challenged Claims.....	35
C.	Ground 2: Petitioner Fails To Establish That The Combination Of Hubbard-495, Hubbard-174, And Alperovitch Renders Obvious The “Security History” Limitation In All Challenged Claims.....	42

Patent Owner’s Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 8,438,386

1.	Alperovitch Does Not Disclose or Render Obvious the Claimed “Security History” Factor.....	42
2.	There Was No Motivation to Combine Hubbard-495 and Hubbard-174 with Alperovitch.....	45
V.	PETITIONER’S GROUNDS FAIL TO ANTICIPATE OR RENDER OBVIOUS ALL DEPENDENT CLAIMS	50
VI.	OTHER LIMITATIONS NOT ADDRESSED	50
VII.	SECONDARY OBJECTIVE INDICIA OF NONOBVIOUSNESS	50
VIII.	CONCLUSION.....	52

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	<i>passim</i>
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 15 (PTAB May 13, 2020)	11, 12
<i>Cisco Sys., Inc. v. Monarch Networking Solutions LLC</i> , IPR2020-01227, Paper 11 (PTAB Mar. 4, 2021)	15
<i>Commscope Techs. v. Dali Wireless, Inc.</i> , IPR 2022-01242, , Paper 23 (PTAB Feb. 27, 2023).....	19
<i>Eclinical Works, LLC v. Decapolis LLC</i> , IPR2022-00229, Paper 10 (PTAB Apr. 13, 2022)	13
<i>Ericsson Inc. v. Collision Comms., Inc.</i> , IPR2022-01233, Paper 12 (PTAB Jan. 19, 2023)	15
<i>Google LLC v. EcoFactor, Inc.</i> , IPR2021-00454, Paper 9 (PTAB July 22, 2021).....	18
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966).....	50
<i>In re Huang</i> , 100 F.3d 135 (Fed. Cir. 1996)	50
<i>Intellectual Ventures I LLC v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA (W.D. Tex. Dec. 22, 2022).....	7
<i>Leo Pharm. Prods., Ltd. v. Rea</i> , 726 F.3d 1346 (Fed. Cir. 2013)	51
<i>Luxshare Precision Industry v. Amphenol Corp.</i> , IPR2022-00132, Paper 10 (PTAB May 3, 2022)	11

Patent Owner’s Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 8,438,386

<i>mCom IP, LLC v. Cisco Sys., Inc.</i> , No. 6:22-00261-ADA (W.D. Tex. Oct. 20, 2022).....	7
<i>Magellan Midstream Partners L.P v. Sunoco Partners Mktg. & Terms. L.P.</i> , IPR2019-01445, Paper 12 (PTAB Jan. 22, 2020)	13
<i>Motorola Mobility LLC v. Ironworks Patents, LLC</i> , IPR2021-00421, Paper 11 (PTAB July 22, 2021)	12
<i>NHK Spring Co., Ltd. v. Intri-Plex Techs., Inc.</i> , IPR2018-00752, Paper 8 (PTAB Sept. 12, 2018).....	13
<i>Nintendo Co. v. Gamevice, Inc.</i> , IPR2020-01197, Paper 13 (PTAB Jan. 12, 2021)	11
<i>Nokia of Am. Corp. v. Godo Kaisha IP Bridge</i> , IPR2022-00755, Paper 9 (PTAB Nov. 2, 2022).....	18
<i>NXP USA, Inc. v. Impinj, Inc.</i> , PGR2022-00005, Paper 20 (PTAB Aug. 25, 2022)	14
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	26
<i>Regeneron Pharms. Inc. v. Novartis Pharma AG</i> , IPR2020-01317, Paper 15 (PTAB Jan. 15, 2021)	15, 16
<i>Robert Bosch Tool Corp. v. SD3, LLC</i> , IPR2016-01751, Paper 15 (PTAB March 22, 2017)	51
<i>Samsung Elecs. Co. v. California Institute of Tech.</i> , IPR2023-00131, Paper 10 (PTAB May 4, 2023)	12, 13
<i>Samsung Elecs. Co. v. Clear Imaging Research LLC</i> , IPR2020-01399, Paper 13 (PTAB Feb. 3, 2021).....	11
<i>Sonrai Memory Ltd. v. Kingston Tech. Co.</i> , No. 6:21-cv-1284-ADA (W.D. Tex. Oct. 18, 2022)	7
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020)	18

<i>Vizio, Inc. v. Maxell, Ltd.</i> , IPR2022-01459, Paper 7 (PTAB Apr. 11, 2023)	18
---	----

Statutes

35 U.S.C. § 314(a)	4, 18
AMERICA INVENTS ACT, Congress. H. Rept. 112-98 Part 1 (June 1, 2011).....	1

Other References

Memo, <i>Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation</i> (June 21, 2022)	4, 5, 12, 19
--	--------------

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Professor Alessandro Orso, Ph. D.
2002	<i>Curriculum Vitae</i> of Professor Alessandro Orso, Ph. D.
2003	<i>Sonrai Memory Ltd. v. Kingston Tech. Co. and Kingston Tech. Corp.</i> , Case No. 6:21-cv-1284-ADA, Order Denying Kingston Tech. Co. and Kingston Tech. Corp.’s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 94 (W.D. Tex., Oct. 18, 2022)
2004	<i>mCom IP, LLC v. Cisco Systems, Inc.</i> , Case No. 6:22-cv-00261-ADA, Order Denying Defendant’s Motion to Stay Pending <i>Inter Partes</i> Review, Dkt. 42 (W.D. Tex., Oct. 20, 2022)
2005	<i>Intellectual Ventures I LLC et al. v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA, Order Denying Hewlett Packard Enterprise Company’s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 104 (W.D. Tex., Dec. 22, 2022)
2006	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Dec. 9, 2022 Transcript of Motions Hearing, Dkt. 133 (W.D. Tex. Dec. 15, 2022) (excerpted)
2007	Dani Kass, “Catching Up On Patent Litigation With Judge Albright” (Law360 Mar. 14, 2023); https://www.law360.com/pulse/articles/1582438/print?section=pulse/courts
2008	U.S. District Courts—Federal Court Management Statistics—Profiles—During the 12-Month Periods Ending March 31, 2018 Through 2023, “Table N/A—U.S. District Courts—Combined Civil and Criminal Federal Court Management Statistics (March 31, 2023)”, <i>available</i> https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_dlistprofile0331.2023.pdf

Patent Owner's Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 8,438,386

Exhibit	Description
2009	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Order Granting Fourth Amended Scheduling Order, Dkt. 160 (W.D. Tex. Jan. 22, 2023)
2010	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Claim Construction Order, Dkt. 236 (W.D. Tex. Mar. 16, 2023)
2011	<i>Webroot, Inc. and Open Text Inc., v. Forcepoint LLC</i> , Case No. 6:22-cv-342-ADA-DTG, Defendant Forcepoint LLC's Preliminary Invalidity Contentions (W.D. Tex. Sept. 13, 2022) (excerpted)
2012	<i>Webroot, Inc. et al. v. AO Kaspersky Lab et al.</i> , No 6-22-cv-00243, Dkt. 121, Second Amended Complaint For Patent Infringement (<i>Forcepoint LLC</i> , Case No. 22-cv-00342-ADA-DTG) (W.D. Tex. Dec. 9, 2022)

Open Text Inc. (“Patent Owner”) submits this Preliminary Response to the Petition of Forcepoint Inc. (“Petitioner” or “Forcepoint”) seeking *inter partes* review (“IPR”) of U.S. Patent No. 8,438,386 (“the ’386 patent”).

I. INTRODUCTION

The Board should decline to institute trial because IPR of the ’386 patent would duplicate the parties’ district court litigation efforts and because the petition presents weak unpatentability arguments using prior art that fails to disclose key claim limitations.

First, the Board should deny institution under *Fintiv* because instituting this IPR would undermine Congress’s stated goals in creating IPR proceedings: to provide “quick and cost effective alternatives to litigations” and “limit unnecessary and counterproductive litigation costs.” H.R. Rep. No. 112-98, pt. 1, at 40 (2011), 2011 U.S.C.C.A.N. 67, 69. An IPR here would be neither quicker than, nor an alternative to, ongoing district court litigation. The Western District of Texas (“WDTX”) is scheduled to proceed to trial on the ’386 patent three months *before* a final written decision on the petition would be due—so IPR is not quicker. And, the district court has indicated it will not issue a stay when, as here, it can resolve the same issues before the Board does—so IPR is not an alternative to litigation. Moreover, Petitioner has asserted in the district court the same primary prior art

raised in the petition and two of the three petitioned references, which the district court will address regardless of whether the Board institutes IPR. Therefore, instituting IPR would generate the unnecessary and counterproductive litigation costs that Congress sought to avoid.

Second, the Board should deny institution because Petitioner fails to demonstrate a reasonable likelihood that it will prevail on the merits. The '386 patent claims a novel approach to identifying potentially malicious websites using a reputation vector to determine the reputation index of a particular internet resource using a specifically recited set of factors including a "security history" factor. Claim 1, for example, recites a "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..." (EX-1001 cl 1.) The claim language reciting the "security history" factor requires (1) a security history that is a history of security events for the resource whose reputation index is being determined; and (2) the use of that security history in determining the reputation index of the internet resource, e.g., adjusting the reputation index to account for the extent of historical security events.

In Ground 1, Petitioner asserts the combination of Hubbard-495 and Hubbard-174. Institution on Ground 1 should be denied because Petitioner fails to establish

that Hubbard-495 or the combination of Hubbard-495 and Hubbard-174, discloses or renders obvious the claimed “security history” factor.

Tacitly acknowledging that Ground 1 is insufficient, Petitioner asserts Ground 2, where it attempts to combine a third reference, Alperovitch, with the Hubbard prior art. Institution on Ground 2 should be denied because Petitioner similarly fails to establish that Alperovitch discloses or renders obvious the claimed “security history” factor.

Indeed, many of the prior art disclosures Petitioner relies on describe information that relates to one of the other factors recited by the claims (e.g., legitimacy or behavior). Others highlight the very weaknesses in the art the '386 patent successfully sought to address. And Petitioner fails to establish that any of the cited references employ an internet resources history of security events combined with four other specific factors of a reputation vector to determine the reputation index of the internet resource that adjusts for that particular resource's historical security events.

Accordingly, the petition is not reasonably likely to succeed and must therefore be denied.

II. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a)

The '386 patent is one of dozens of patents asserted in claims and counterclaims among six different parties in a series of cases pending in the Western District of Texas. The district court has already issued its claim constructions and is on track to adjudicate the same primary prior art reference asserted in all petitioned grounds, and will specifically adjudicate two of the three petitioned references, months before the Board issues a final written decision. Institution of a parallel IPR proceeding lagging well behind the district court would needlessly increase the cost of resolving the underlying dispute. Under these circumstances, the Board should exercise its discretionary authority to deny institution under 35 U.S.C. § 314(a).

Because Congress's goal in enacting post-grant proceedings like IPRs was "to ... limit unnecessary and counterproductive litigation costs," Director Vidal has instructed the Board not to institute IPRs that would "increase, rather than limit, litigation costs." Director's Memo, *Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation* ("Guidance") at 1 (June 21, 2022).

Instituting this IPR would cause just such an increase. A district court stay is out of the question, and the district court will consider the very same primary prior art reference presented in the petition. Accordingly, for the next year, the Board and

the district court will labor to decide the very same issues with the district court well ahead of—and scheduled to reach a final decision months before—the Board. The year-long parallel tracks of two adjudicatory bodies will “increase, rather than limit, litigation costs,” create “potential conflict between the ... (PTAB) and district court proceedings,” and generally increase “the potential for inefficiency and gamesmanship.” Guidance at 1. This is precisely the situation that Director Vidal sought to avoid when she instructed the Board to take “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review.” *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 6 (PTAB Mar. 20, 2020).

Confirming this conclusion, every one of the *Fintiv* factors weighs for discretionary denial:

(1) A stay of the co-pending district court litigation—involving thirty-nine patents and five defendants—is highly unlikely. Petitioner cannot avoid that trial because it has petitioned for review of only two of the eight patents asserted against it. And this IPR will not narrow the issues on which discovery and trial must proceed—the '386 patent is currently asserted in a now-consolidated case that includes four other defendants.

(2) Trial in the district court is expected three months *before* a final written decision. The district court case remains on track. The court has construed the claims of the '386 patent, and discovery is well underway.

(3) The parties and district court have already invested heavily in carrying the parallel litigation past claim construction—eight months before any anticipated institution decision—and well into discovery.

(4) The primary prior art reference raised in the petition is the same as that the district court has before it, and the district court will consider two of the three petitioned references. Petitioner has not offered *any* stipulation that it will not simultaneously pursue in the district court *precisely the same arguments* based on *precisely the same prior art* asserted in its petition during the pendency of any IPR, irrespective of the Board's institution decision.

(5) Petitioner will get its chance to make its arguments before the district court because Petitioner is a defendant in the parallel litigation.

(6) As shown below, the petition's grounds of unpatentability are weak. Thus, every *Fintiv* factor here weighs for discretionary denial. The district court is well on its way to an efficient resolution of the disputes between Patent Owner, Petitioner, and Petitioner's codefendants. Both the goals of the AIA and the general welfare of the patent system would be best served by denying institution.

A. Factor 1: The District Court Has Not Granted And Will Not Grant A Stay

The first *Fintiv* factor asks “whether [1.] the court granted a stay or [2.] evidence exists that one may be granted if a proceeding is instituted.” *Fintiv*, IPR2020-00019, Paper 11 at 6.¹ Here, the undisputed answer to both questions is *no*: no stay has been requested or ordered, and Petitioner has identified no evidence that one will (or even might) be. To the contrary, all evidence indicates that a stay is unlikely.

¹ The decision in *Fintiv* addresses various scenarios that may indicate whether a stay may be granted. *Fintiv*, IPR2020-00019, Paper 11 at 6-9. However, nothing in *Fintiv* suggests that these are the only scenarios that a panel may consider. In particular, *Fintiv* does not hold that an actual denial of a stay is the only consideration relevant to this factor. Rather, *Fintiv* contemplates that any type of evidence may be relevant. For example, *Fintiv* holds that one way to “support the arguments that ... a stay may be less likely, and instituting would lead to duplicative costs,” is to show the “work completed by the parties and court in the parallel proceeding.” *Fintiv*, IPR2020-00019, Paper 11 at 10.

First, the district court considers issue simplification “the most important factor” in deciding whether to stay patent litigation²—and here, a stay would not simplify anything. The validity of the ’386 patent will be litigated in the consolidated district court action, whether this petition is instituted or not, particularly because Petitioner offers no stipulation to not pursue the same grounds in the district court and because the district court trial will decide validity of the ’386 before the Board reaches its final written decision.

²See, e.g., EX-2003, *Sonrai Memory Ltd. v. Kingston Tech. Co.*, No. 6:21-cv-1284-ADA, slip op. at **4-5 (W.D. Tex. Oct. 18, 2022) (denying a stay following IPR institution because issue simplification was the “most important factor” and the Court had already held a *Markman* hearing and “expended significant resources”); EX-2004, *mCom IP, LLC v. Cisco Sys., Inc.*, No. 6:22-00261-ADA, slip op. at *5 (W.D. Tex. Oct. 20, 2022) (finding “simplification... is not likely” where the IPR did not challenge all of the claims asserted in the district court, since the other claims would still require a trial); EX-2005, *Intellectual Ventures I LLC v. Hewlett Packard Enterprise Co.*, No. 6:21-cv-00596-ADA, slip op. at *7-8 (W.D. Tex. Dec. 22, 2022) (denying a stay following IPR institution, as even IPR estoppel would not simplify the invalidity case, given the defendants’ reliance on prior art systems).

Moreover, the validity of the '386 patent will be litigated in the district court alongside issues regarding 38 *other* patents asserted by and against Petitioner and *four other* defendants—issues that the district court is highly unlikely to delay deciding in favor of letting the Board proceed with this IPR. The case against Petitioner alone involves thirteen patents—eight asserted by Patent Owner and five asserted in counterclaims by Petitioner.

The table below illustrates the patents, parties, and IPR petitions involved in this highly complex litigation:

**Table 1. Patent Owner's Asserted Patents
Against Each WDTX Defendant and Resulting Review Petitions**

Patent	Kaspersky	CrowdStrike	Forcepoint	Sophos	Trend Micro
8,438,386	<i>N/A</i>	<i>N/A</i>	IPR2023-00784	<i>N/A</i>	<i>N/A</i>
10,025,928	<i>N/A</i>	<i>N/A</i>	IPR2023-00786	<i>N/A</i>	<i>N/A</i>
10,284,591	IPR2023-00895	IPR2022-01522	<i>N/A</i>	Asserted; no IPR	IPR2023-00692
9,578,045	IPR2023-01199	IPR2023-00124	<i>N/A</i>	Asserted; no IPR	IPR2023-00677
8,201,243	Asserted; no IPR	IPR2023-01052	Asserted; no IPR	IPR2023-00731	Asserted; no IPR
8,719,932	Asserted; no IPR	IPR2023-01051	Asserted; no IPR	IPR2023-00732	Asserted; no IPR
8,418,250	Asserted; no IPR	IPR2023-00289	<i>N/A</i>	IPR2023-0699	IPR2023-00655

Patent	Kaspersky	CrowdStrike	Forcepoint	Sophos	Trend Micro
8,726,389	Asserted; no IPR	IPR2023- 00556	Asserted; no IPR	IPR2023- 00633	Asserted; no IPR
10,599,844	Asserted; no IPR	Asserted; no IPR	Asserted; no IPR	IPR2023- 00528	IPR2023- 00662
9,413,721	N/A	N/A	Asserted; no IPR	IPR2023- 00491	N/A
10,257,224	IPR2023- 01011	IPR2023- 00126	N/A	Asserted; no IPR	IPR2023- 00657
8,856,505	Asserted; no IPR	IPR2023- 01159	N/A	Asserted; no IPR	Asserted; no IPR
8,181,244	N/A	IPR2023- 01158	N/A	Asserted; no IPR	Asserted; no IPR
11,409,869	IPR2023- 01160	IPR2023- 01053	Asserted; no IPR	PGR2023- 00031	Asserted; no IPR
8,763,123	N/A	IPR2023- 1050	N/A	Asserted; no IPR	N/A

As U.S. Magistrate Judge Gilliland noted during a December 9, 2022 hearing, this is “a phenomenal case that I’m hoping one day maybe people will write songs about because it is about as complicated as you’re going to get with patent cases.” (EX-2006 52.)

Second, the district court has been clear in public comments that it will not stay cases where, as here, the court can resolve the case as quickly as the Board can:

[T]here’s no unfairness to either side by not staying a case for the PTAB when I can try the case as quickly as they can resolve it.... And so far, I think that’s proven to be true.

(EX-2007 3.) Indeed, as commentators have observed, “Judge Albright almost never stays proceedings to let the PTAB make its decision first.” (*Id.* 2.)

Judge Albright's public comments apply squarely to the situation here. The median time-to-trial in WDTX is 28.2 months. (EX-2008 37.) On that timeline, trial is expected in this case in mid-July 2024. Trial is currently scheduled for August 2024. (EX-2009 6.) The deadline for a final written decision in an IPR here would not be until many months later (in November 2024). That Judge Albright has made public comments indicating his practice is to deny a stay in precisely the circumstances presented here is further evidence that he would not stay the WDTX case in response to institution of this IPR.

Petitioner acknowledges that no stay has been entered in the parallel litigation. (Petition 8.) Even where no stay has been requested, the Board has found Factor 1 to favor discretionary denial where (as here) “Petitioner present[ed] no evidence that it has requested a stay [] or that a stay is likely.” *Luxshare Precision Industry v. Amphenol Corp.*, IPR2022-00132, Paper 10, at 9 (PTAB May 3, 2022). And such a decision is particularly appropriate where the circumstances show that “a stay ... is unlikely.” *Nintendo Co. v. Gamevice, Inc.*, IPR2020-01197, Paper 13, at 11-12 (PTAB Jan. 12, 2021); *Samsung Elecs. Co. v. Clear Imaging Research LLC*, IPR2020-01399, Paper 13 at 11-12 (PTAB Feb. 3, 2021) (holding Factor 1 may

weigh for denial where there is evidence that the district court is unwilling “to avoid duplicative efforts and await the PTAB’s final resolution”); *Motorola Mobility LLC v. Ironworks Patents, LLC*, IPR2021-00421, Paper 11 at 7-8 (PTAB July 22, 2021).

In sum, the district court has not granted a stay, and there is no evidence suggesting that the district court would grant a stay of a multi-patent, multi-defendant case so that the Board can reach a decision months *after* the current trial date on *just one* patent. Factor 1 weights in favor of discretionary denial. *Samsung*, IPR2020-01399, Paper 13 at 11-12; *Motorola*, IPR 2021-00421, Paper 11 at 7-8.

B. Factor 2: A District Court Trial Is Expected Before The Projected Statutory Deadline

Factor 2—the implications of the district court and IPR schedules—also weighs for denial. “[A] parallel proceeding in an advanced state implicates considerations of efficiency and fairness, which can serve as an independent reason to apply discretion to deny institution.” *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 11-12, 17 (PTAB May 13, 2020) (*informative*); Guidance at 1.

Here, an IPR would overlap entirely with the parallel district court litigation. WDTX’s median time-to-trial is 28.2 months (EX-2008 37), indicating a trial by mid-July 2024—a date consistent with the currently scheduled trial date of August 19, 2024. (EX-2009 6.) Should the Board institute, its final written decision deadline would be November 17, 2024, three months *after* the scheduled trial date.

Petitioner's speculation that the complexity of the case will result in delay is just that—speculation. (Petition 8-9.) And the district court has scheduled a single trial. (EX-2009 6.) Applying *either* the trial date set by the Court or WDTX's median time-to-trial, trial here would not be complete before the '386 patent's validity is decided in the district court.

In other words, if the Board institutes IPR here, the IPR proceedings would not produce a result before the trial, and the parties would spend a year on precisely the “duplicative,” “unnecessary[,] and counterproductive litigation costs” the AIA was designed to avoid. *Fintiv*, IPR2020-00019, Paper 11 at 5 (citing *Magellan Midstream Partners L.P v. Sunoco Partners Mktg. & Terms. L.P.*, IPR2019-01445, Paper 12 at 10 (PTAB Jan. 22, 2020)); *see Fintiv*, IPR2020-00019, Paper 15 at 17 (discretionarily denying institution where district court trial was scheduled two months before the final decision deadline); *NHK Spring Co., Ltd. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 at 20 (PTAB Sept. 12, 2018) (*precedential*) (finding that institution of IPR when the district court trial would resolve validity before the PTAB “would not be consistent with an objective of the AIA...to provide an effective and efficient alternative to district court litigation”); *Samsung Elecs. Co. v. California Institute of Tech.*, IPR2023-00131, Paper 10 at 15, 24 (PTAB May 4, 2023) (discretionarily denying institution where “[r]egardless of whether we

consider the scheduled trial date or the trial date expected based on time-to-trial statistics, the trial in the underlying litigation would commence several months before the expected date of our final written decision”); *Eclinical Works, LLC v. Decapolis LLC*, IPR2022-00229, Paper 10 at 9 (PTAB Apr. 13, 2022) (discretionarily denying institution where WDTX trial was scheduled “roughly one to two months before any final decision would have been due”).

Because the district court will resolve validity before the Board reaches its final written decision, the second *Fintiv* factor also favors denial.

C. Factor 3: The Parties Have Invested Significant Resources In The District Court Proceeding

Factor 3—the resources invested in the parallel district court proceeding—favors denial “if, at the time of the institution decision, the district court has issued substantive orders related to the patent.” *Fintiv* at 9-10; *see also id.* at n.16 (collecting cases). *Fintiv* holds specifically that “claim construction orders may indicate that the court and parties have invested sufficient time in the parallel proceeding to favor denial.” *Id.* at 10.

The parties have invested significant resources in the parallel litigation over the last seventeen months. For example, the parties long ago exchanged infringement and invalidity contentions (in July 2022 and September 2022, respectively), and fact discovery is underway. Claim construction too, is long since complete. (EX-2010.)

And while *Fintiv* directs consideration of resource investment at the time of institution, the overlapping schedules here counsel the Board to further consider the redundant resources that *will be* wasted should IPR be instituted. *Fintiv*, IPR2020-00019, Paper 11 at 6; *NXP USA, Inc. v. Impinj, Inc.*, PGR2022-00005, Paper 20 at 7 (PTAB Aug. 25, 2022) (Board should consider “the duplicative efforts that will occur during the [] duration of a [inter partes] review”); *Cisco Sys., Inc. v. Monarch Networking Solutions LLC*, IPR2020-01227, Paper 11 at 11-12 (PTAB Mar. 4, 2021) (finding that more work completed by the parties and the court suggests that institution would lead to duplicative costs).

The investment in this case is colossal. The district court has already held multiple *Markman* hearings and completed claim construction, including for the '386 patent. (EX-2010 8.) And, the parties have engaged in extensive discovery on the parties' contentions, during which Patent Owner has made approximately 50TB of source code available. The Court has held multiple discovery hearings. Furthermore, Petitioner's and Patent Owner's experts have already invested an extensive number of hours preparing for their reports by reviewing the patent, prior art, and the defendants' invalidity contentions, as well as traveling to review source code. *See Regeneron Pharmas. Inc. v. Novartis Pharma AG*, IPR2020-01317, Paper 15 at 17 (PTAB Jan. 15, 2021) (denying institution where the parties had expended

considerable resources in claim construction, substantial fact discovery, and preparation for expert reports).

The minimal resources Petitioner invested in its petition overlap with the very same investment in Petitioner's district court invalidity grounds and, therefore, would not "be lost" as Petitioner claims. (Petition 9.) Furthermore, institution will do nothing to reduce the substantial expenses in the related litigation (*id.*), as the district court trial will be held three months before the Board reaches its final written decision.

Petitioner's delay in filing this petition further weighs for denial. Petitioner waited almost exactly twelve months after receiving Patent Owner's March 31, 2022 complaint, eight months after receiving Patent Owner's infringement contentions, and six months after serving its invalidity contentions before filing its petition. Petitioner offers no explanation for its delay, which weighs for denial. *Fintiv*, IPR2020-00019, Paper 11 at 11-12; *Ericsson Inc. v. Collision Comms., Inc.*, IPR2022-01233, Paper 12 at 15 (PTAB Jan. 19, 2023) (finding that where the parties invested significant resources and "Petitioner waited almost a year" to file its petition, "this factor weighs decidedly in favor of discretionary denial"); *Regeneron*, IPR2020-01317, Paper 15 at 17 (finding that even where the petition was filed "less

than a month after learning of the complaints,” the investment by the parties in the parallel proceeding “outweighs the effort expended so far in this proceeding”).

D. Factor 4: The Issues And Parties Overlap Significantly

Factor 4—the degree of overlap between the issues in the petition and those before the district court—also strongly supports denial.

Regarding this fourth factor, *Fintiv* explains that “concerns of inefficiency and the possibility of conflicting decisions [are] particularly strong” where “the Board [is] presented with substantially identical prior art arguments...at issue in district court.” *Fintiv*, IPR2020-00019, Paper 11 at 12. “Accordingly, if the petition includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel proceeding, this fact has favored denial.” *Id.*

Here, Petitioner has not offered *any* stipulation that it will not simultaneously pursue in the district court *precisely the same arguments* based on *precisely the same grounds* asserted in its petition during the pendency of any IPR. Indeed, Petitioner asserts two of the three same primary prior art references in the district court—Hubbard 495 and Alperovitch. (EX-2011 121-123.) In light of the inevitable parallel tracks, instituting IPR would not only multiply the burden on Patent Owner, it would also create the possibility of inconsistent decisions between the district court and the Board.

Because Petitioner makes no effort to “mitigate[] any concerns of duplicative efforts between the district court and the Board,” or “of potentially conflicting decisions,” Factor 4 weighs heavily in favor of discretionary denial. *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 19 (PTAB Dec. 1, 2020); *Google LLC v. EcoFactor, Inc.*, IPR2021-00454, Paper 9 at 12-14 (PTAB July 22, 2021).

E. Factor 5: Both Parties Are Parties In The Parallel Litigation

Factor 5—the overlap of the parties between the petition and the parallel litigation—suggests denial because Petitioner is a defendant in the parallel litigation and, as such, will have a full, fair opportunity to litigate its invalidity contentions. Under *Fintiv*, “[i]f a petitioner is unrelated to a defendant in an earlier court proceeding, the Board has weighed this fact against exercising discretion to deny institution.” *Fintiv*, IPR2020-00019, Paper 11 at 13-14. That is not the case here because Petitioner is a defendant in the litigation. Accordingly, the circumstances raise no fairness concerns that denial would deprive Petitioner of its “day in court.” *See Vizio, Inc. v. Maxell, Ltd.*, IPR2022-01459, Paper 7 at 21-22 (PTAB Apr. 11, 2023) (“Because Petitioner is the litigation defendant, factor 5 weighs in favor of discretionary denial”); *Nokia of Am. Corp. v. Godo Kaisha IP Bridge*, IPR2022-00755, Paper 9 at 13 (PTAB Nov. 2, 2022) (holding that Factor 5 weighed for

discretionary denial where Petitioner was defendant in parallel proceeding). This factor weighs in favor of discretionary denial.

F. Factor 6: The Petition Does Not Present “Compelling Evidence Of Unpatentability”

Factor 6—the merits of the petition—also weighs against institution because, as detailed below, the petition fails to show even a “reasonable likelihood” that Petitioner would prevail on any challenged claim. *See* 35 U.S.C. § 314(a). In particular, Petitioner’s references do not disclose or render obvious a reputation vector constructed using a “security history,” as required by every challenged claim. Petitioner also fails to articulate its proposed combination of Hubbard-495, Hubbard-174, and Alperovitch with adequate clarity. For example, Petitioner fails to explain *how* a POSITA would have combined the teachings of Hubbard-495, Hubbard-174, and Alperovitch, or *why* a POSITA would have combined particular teachings from these references. Section IV, *infra*.

Even if the petition did have a “reasonable likelihood” of succeeding (it does not), it certainly would not pass the higher threshold of a “compelling” unpatentability challenge that could preclude discretionary denial. Guidance at 4. “[T]he compelling merits standard is a higher standard than the standard for institution set by statute.” *Commscope Techs. v. Dali Wireless, Inc.*, IPR 2022-01242, Paper 23, 3 (PTAB Feb. 27, 2023). That higher standard requires determining

that Petitioner is “*highly likely*” to succeed on the merits. *Id.* at 4. The opposite is true here.

* * *

In sum, all six factors weigh for discretionary denial. Accordingly, Patent Owner respectfully requests that the Board exercise its discretion to deny institution.

III. THE '386 PATENT

A. Inadequacy Of The Prior Art And The Need For Improved Internet Access Control

The vast amount of information exchanged on the internet makes it a target for wrongdoing. (EX-2001 ¶¶25-26.) Hackers use internet communications to attack computers and other devices through the transmission of malicious data. (*Id.* at ¶26) For instance, a data packet received from one computer may contain malicious data that can provide access to sensitive information stored on another computer, or otherwise force the computer to operate in ways not intended by the computer's operator. (*Id.*)

There were various systems and methods for combatting these attempted exploits. For instance, internet security providers combatted these security threats by examining files, web page content, or other internet resources to discover known patterns or signatures associated with malicious content. (*Id.* at ¶27) Prior art approaches included determining whether a particular file or web page included

known malicious code, or whether the file or web page fell within with a specified category. (*Id.*)

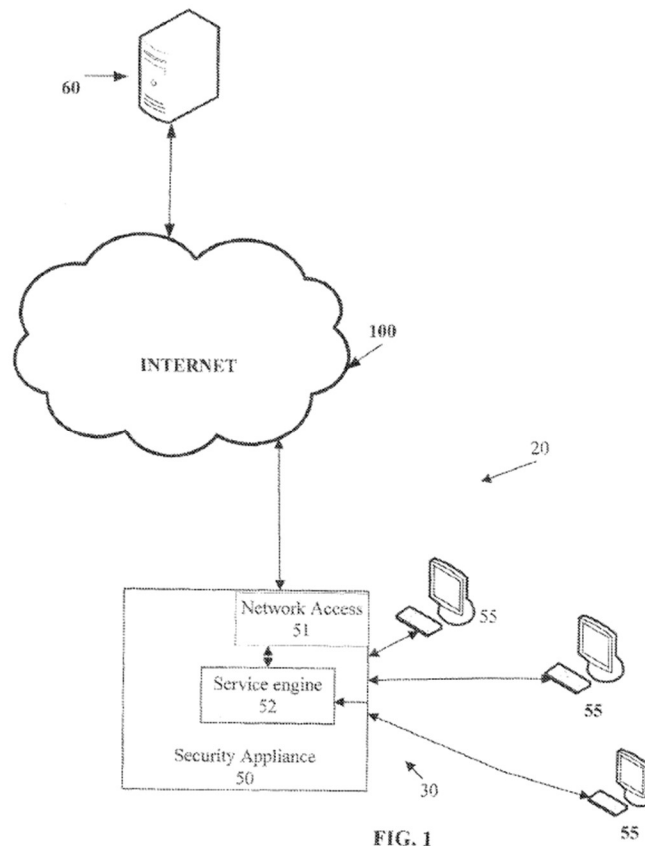
One prior art approach is referred to as “content filtering,” in which websites “are organized into categories and requests for Web content are matched against per-category policies and either allowed or blocked.” (*Id.*) These prior art systems failed to address a fundamental problem in malware detection and internet access control – lack of precision and means for preventing malicious data from reaching a computer before that malicious data has previously exploited a vulnerability and made itself known. (*Id.*) As such, there was a need to assess “zero-day threats,” and determine whether an internet resource contains malicious content in a more predictive and flexible manner. (*Id.* at ¶28)

B. Innovations Of The '386 Patent

The '386 patent is entitled “System and Method for Developing a Risk Profile for an Internet Service,” was filed on February 21, 2010, and was issued on May 7, 2013. (EX-1001.) The systems and methods described and claimed in the '386 patent are generally directed to improved techniques for identifying a potentially malicious internet resource. (*Id.* at Abstract.) These techniques involve assessing an internet resource's reputation to determine the likelihood that the internet resource may contain malicious or inappropriate content. (*Id.*)

The '386 patent describes computer networks, such as a local area network ("LAN"), through which multiple client computers access the internet. (EX-2001 ¶31.) The techniques described and claimed in the '386 patent improve over traditional networks because, for example and as described in the '386 patent, they employ "a predictive approach based on a statistical model built on broad sampling of Internet resources with varying degrees of risk. [Such embodiments] focus[] on the reputation of a Web site, or any Internet-based service or resource." (EX-2001 ¶¶30-31; EX-1001 4:34-38.)

An example of this novel technique is illustrated in Figure 1 of the '386 patent, which shows multiple client-side devices 55 on a local area network 30 connecting to the internet 100 to access an internet resource stored on a remote server 60. (EX-2001 ¶31; EX-1001 FIG. 1.) Requests from a client-side device 55 to download the internet resource may be sent to a security appliance 50. (EX-2001 ¶31; EX-1001 FIG. 1.) The security appliance 50 may assess a reputation for the requested internet resource by determining a reputation index, which may in turn be used to determine whether the request should be transmitted over the internet so that the internet resource may be provided to the requesting client-side device 55. (EX-2001 ¶¶31-32; EX-1001 FIG. 1.)



(EX-1001 FIG. 1.)

The reputation index for the requested internet resource is determined using a reputation vector. (EX-2001 ¶¶32, 38.) A reputation vector may be constructed using a variety of factors, including “security history,” “legitimacy,” “behavior,” “associations,” and “location.” (*Id.* ¶32.)

“Security history” refers to a history of security events for an internet resource. (EX-1001 12:8-10; EX-2001 ¶33.) For instance, the security history may include the number of malware infections inflicted upon an internet resource over a given period of time. (EX-1001 12:8-10; EX-2001 ¶33.) As the ’386 patent notes,

for example, “the occurrence of a single security breach (the site gets hacked and is a danger to visitors) does not dramatically lower the reputation of a site. Repeated occurrences over time, however, will destroy the reputation of the site.” (EX-1001 8:63-67; EX-2001 ¶33.)

“Legitimacy” refers to qualities of an internet resource that are generally indicative of reputable internet resources. For instance, legitimacy may be “determined by the top-level domain, the investment in the internet resource (virtual hosting with non-affiliated sites, multiple hosting and SSL security), the traffic volume, the category age[,] the popularity rank. . . the consistency between the registering and hosting city region or country; and city, region or country associated with the IP address.” (EX-2001 ¶34 (*citing* EX-1001 9:8-18).) Legitimacy may involve an assessment of other internet resources that are closely related to the requested internet resource. For example, an internet resource having a reputable top-level domain (*e.g.*, google.com) may have a higher reputation than an internet resource having a top-level domain that has been determined to be non-reputable (*e.g.*, g00g1e.com). (EX-2001 ¶34) As another example, an internet resource having SSL security (*e.g.*, SSL certificates for HTTPS access schemes) would increase the legitimacy of the resource. (*Id.*; *see also* EX-1001 9:8-15 (“Legitimacy is determined by . . . the investment in the Internet resource (. . . SSL security).”))

“Behavior” may include run-time behaviors exhibited by the internet resource, such as “the use of popup ads, browser hijacking and the use of auto-redirecting.” (EX-2001 ¶35; EX-1001 9:19-20.)

“Associations” may include how the requested internet resource interacts with other resources on the internet. For instance, associations may involve “the number of sites linking into the site, the reputations of the linked in sites and the reputations of the linked-to sites.” (EX-2001 ¶36; EX-1001 9:20-22.)

“Location” refers to geographical factors associated with an internet resource, such as “the hosting country, the registration country, the region[,] the city[,] . . . [and] the consistency between the registering and hosting country and the country associated with the IP address.” (EX-2001 ¶37; EX-1001 9:15-18.)

The table below provides exemplary features that constitute factors used to construct the claimed reputation vector:

TABLE ONE

Attribute	Description
Country	2-letter code, 3-letter code or full name of country based on IP block
Top-level Domain	.com, .biz, .org, .gov, etc.
Domain Age	Number of months in existence on zone lists, or no less than the classification age
Database Age	Months since Authority was entered into database
Classification	Months that the Authority has held its current classification
Age	Number of IP's associated with the Authority
Hosts	T/F if the other authorities share associated IP's
Virtually Hosted	T/F if the page opens new browser windows on its own
Popups	T/F does the default page alter the browser configuration
Hijack	Count of <SCRIPT> blocks in default pages
JavaScript	T/F does the authorities download executables to client
Executables	Count of pictures on default page
Pictures	

TABLE ONE-continued

Attribute	Description
Latency	Number of milliseconds to return default page
Rank	Numerical ranking, used as T if <2,000,000, F otherwise in modeling
Infected	T/F were infected download files found by AV tools during site analysis
Security Trend	Number of malware infections in past 12 months
Total Security	Total number of malware infections known
Count	
Redirect	Authority redirects to another Authority
IP Address	Analysis of IP address for known threat sources, reserved IP ranges, and legacy IP address assignments
ISP	Internet service provider
City	
Region	

(EX-1001 11:50-12:16.)

The reputation vector may be fed into a machine learning classifier, allowing the classifier to identify how these factors are indicative of a good or bad reputation. (*Id.* ¶39) Once the machine learning classifier is trained using a plurality of reputation vectors including these factors, the system “uses the reputation vector for a requested Internet service to evaluate its reputation index, a score which can be used with empirically developed threshold values to block access where the reputation index is deemed too low to be safe.” (EX-2001 ¶39; EX-1001 9:30-41.) Threshold values may be established for different local area networks based on the needs and tolerances of a particular network. (*Id.*)

C. Claim Construction

On March 16, 2023, in parallel district court litigation, the Court construed the term “security appliance” as having its plain and ordinary meaning. (EX-2010 8.) Neither party proposed constructions for any other claim terms. (*Id.*)

Here, Petitioner does not offer a construction for any claim term, and purports to apply the ordinary and customary meaning of the claim terms as understood by a person having ordinary skill in the art (“POSITA”). *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). However, Petitioner’s analysis deviates from the plain and ordinary meaning of the claim language for at least the term “security

history.” (EX-2001 ¶43.) Accordingly, Patent Owner proposes a construction for that term that is consistent with its plain and ordinary meaning as understood by a POSITA.

1. “Security History”

Consistent with its plain and ordinary meaning, “security history” refers to “a history of security events for an internet resource.”

The '386 patent specification indicates that the claim term “security history” refers to a history of security events for an internet resource. The specification describes past instances (or a pattern) of security breaches for a particular internet site, such as when a website gets hacked, and discloses that too many past security events may lower the reputation of the site:

While security threats are transitory since they come up suddenly and are mitigated as quickly as possible, reputation is built up over a period of time and is a more enduring quality. ***Reputation can be lost, or become bad, over a period of time with repeated security events***, bad associations, and bad behavior. ***For that reason, the occurrence of a single security breach (the site gets hacked and is a danger to visitors) does not dramatically lower the reputation of a site. Repeated occurrences over time, however, will destroy the reputation of the site.***

(EX-1001 8:58-67 (emphasis added).) A POSITA would understand from this passage that the “security history” refers to a history of security events (e.g., breaches) of an internet site and that this history of security events is used in determining the reputation of that site. (EX-2001 ¶ 45) The specification further

describes a “Security Trend” attribute as the “[n]umber of malware infections in the past 12 months” and a “Total Security Count” attribute as the “[t]otal number of malware infections known. (EX-1001 12:8.) A POSITA would understand that these disclosures refer to past security events (*e.g.*, malware infections) for an internet resource whose reputation is being determined. (EX-2001 ¶¶46-47.)

Accordingly, the term “security history” should be construed as a history of security events for an internet resource.

D. Level Of Ordinary Skill In The Art

A POSITA at the time of the invention of the '386 patent had a bachelor's degree in an accredited program of electrical engineering, computer engineering, or computer science, or a similar discipline, and have 2-3 years of practical work experience in the general fields of electrical engineering, computer science, networking, communications, and/or device and network security. (EX-2001 ¶50.) More advanced degrees and/or training in a related discipline can compensate for shorter work experience. (*Id.*) Although PO's PHOSITA definition differs slightly from Petitioner's, PO's positions and arguments do not change based on which PHOSITA definition the Board applies. (*Id.* at 52-53)

IV. THE PETITION IS NOT REASONABLY LIKELY TO SUCCEED

Petitioner presents two obviousness grounds challenging certain claims of the '386 patent:

Ground 1	Section 103(a)	Obvious over Hubbard-495 and Hubbard-174	Claims 1-13, 15, 16, and 18
Ground 2	Section 103(a)	Obvious over Hubbard-495, Hubbard-174, and Alperovitch	Claims 1-13, 15, 16, and 18

For the reasons below, Petitioner fails to establish a reasonable likelihood of prevailing on either ground as to any challenged claim.³

A. Petitioner's Cited Prior Art References

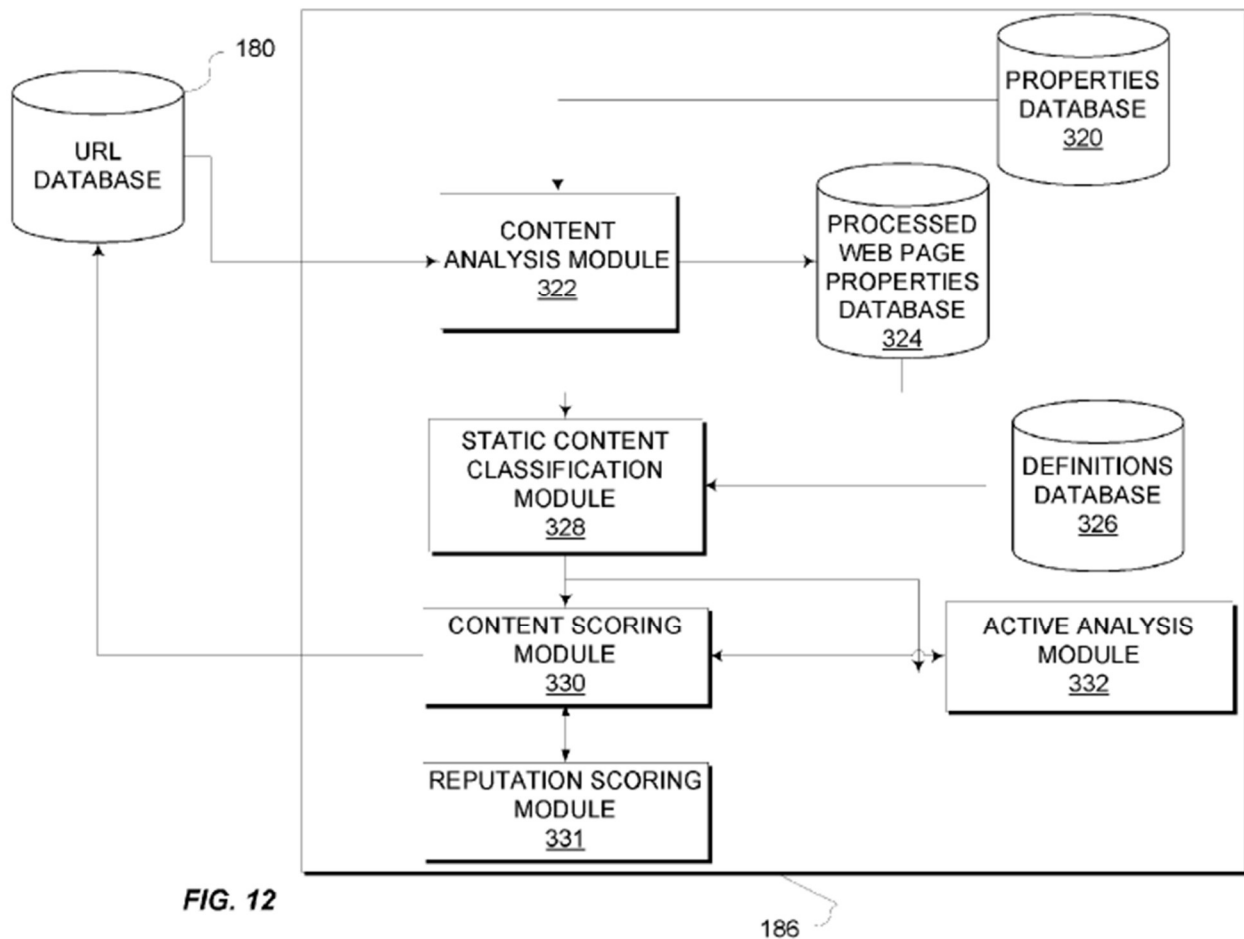
1. Hubbard-495

Hubbard-495 is directed to a “system and method . . . for identifying active content in websites on a network.” (EX-1004 Abstract.) Hubbard-495 discloses that

³ As this is a preliminary response, Patent Owner does not address every limitation of every claim. However, this in no way indicates that other limitations and claims are disclosed or rendered obvious by the prior art; indeed, they are not.

when a user requests access to a website, a database of categorized URLs is used to determine whether that request should be granted. (EX-1004 6:53-7.)

If the URL is not in the database of categorized URLs (*i.e.*, it is uncategorized), the system employs a reputation scoring module 331 “that generates a score or other data representative of a reputation of the URL.” (EX-1004 9:29-33.)



(EX-1004 FIG. 12.)

“One embodiment may include a method of generating a score indicative of the reputation, or likelihood that a website associated with an uncategorized URL contains active or other targeted content based on an analysis of the URL.” (EX-1004 Abstract, 9:25-33.)

Hubbard-495 discloses that if a user requests access to an uncategorized URL, Hubbard-495 may employ an *ad hoc* process for categorizing the URL in order to determine if the user's request should be allowed in accordance with the policies stored in the URL Access Policy Database. In this *ad hoc* categorization process, Hubbard-495 discloses that “URL analysis module 149 may comprise a reputation scoring module (such as an embodiment of the reputation scoring module 331 of FIG. 12) that generates a score of other data representative of the URL.” (EX-1004 9:29-33.)

The *ad hoc* process disclosed in Hubbard-495 involves applying a large number of rules using one or more criteria from a list. (EX-1004 18:53-19:22) For example, Hubbard-495 analyzes URL strings, searches through various databases that involve a URL's host, and parses through the content of the webpage located at the URL. *Id.* These rules then collectively generate a reputation score. *Id.* at 19:22-25.

2. Hubbard-174

Hubbard-174 discloses systems and methods for removing objectionable content from webpages. Hubbard-174 attempts to address the issues of “Google-bombing” or “Spamdexing,” wherein “operators of websites having undesirable or malicious content may utilize misleading techniques with the purpose of having their malicious content included in the web feeds” or search engine results. (EX-1005 1:13-26.)

Rather than determine whether or not to block a user's request for a webpage based on a categorization of a URL, Hubbard-174 discloses “removing certain portions of the data such as malicious or otherwise objectionable content.” (EX-1005 Abstract.) Hubbard-174 seeks to accomplish this goal by using a “policy module including instructions for modifying content based on the category of the content, and a content filtering module configured to modify at least some of the content based at least in part on the instructions.” (EX-1005 2:5-9.)

Hubbard-174 describes a content filtering module 149 that may remove content from webpages located at those URLs. The content filtering module 149 performs this filtering by utilizing a link analysis chart 250, which identifies content that should be removed from a webpage being accessed by a user:

250

ITEM TYPE	URL	ACTION TAKEN	CATEGORY	CODE
a,href	http://www.coolscreensavers.com/	Allow	Search Engines	76
a,href	http://www.verycoolscreensavers.com/	Allow	Search Engines	76
a,href	http://www.verycoolscreensaver.com/	Observe	Free Software	99
a,href	http://www.somewhatcoolscreensavers.com/	Allow	Search Engines	76
a,href	http://www.downloadacoolscreensaver.com/	Observe	Free Software	99
img,src	http://www.adultcoolscreensavers.com/sample.gif	Block	Adult Content	66
a,href	http://www.thebestscreensavers.com/	Allow	Search Engines	76
a,href	http://www.artisticscreensavers.com/	Allow	Search Engines	76
img,src	http://www.verycoolscreensavers.com/save.jpg	Allow	Search Engines	76
a,href	http://www.trickyscreensavers.com/	Block	Spyware	154
a,href	http://www.basicscreensavers.com/	Observe	Free Software	99

252 254 256 258 260

FIG. 11B

(EX-1005 FIG. 11B.)

As shown in FIG. 11B, Hubbard-174 discloses that certain types of content, such as hyperlinks and image files, are removed from a webpage requested by a user. The result is the requested webpage with some of its content removed, as shown in FIG. 12B below.

3. Alperovitch

Alperovitch is directed to systems and methods for improved spam filters for messaging systems, such as emails and instant messages. To improve such filters,

Alperovitch discloses identifying spam communications, namely emails, by assigning reputations to certain “communications entities,” such as email addresses.

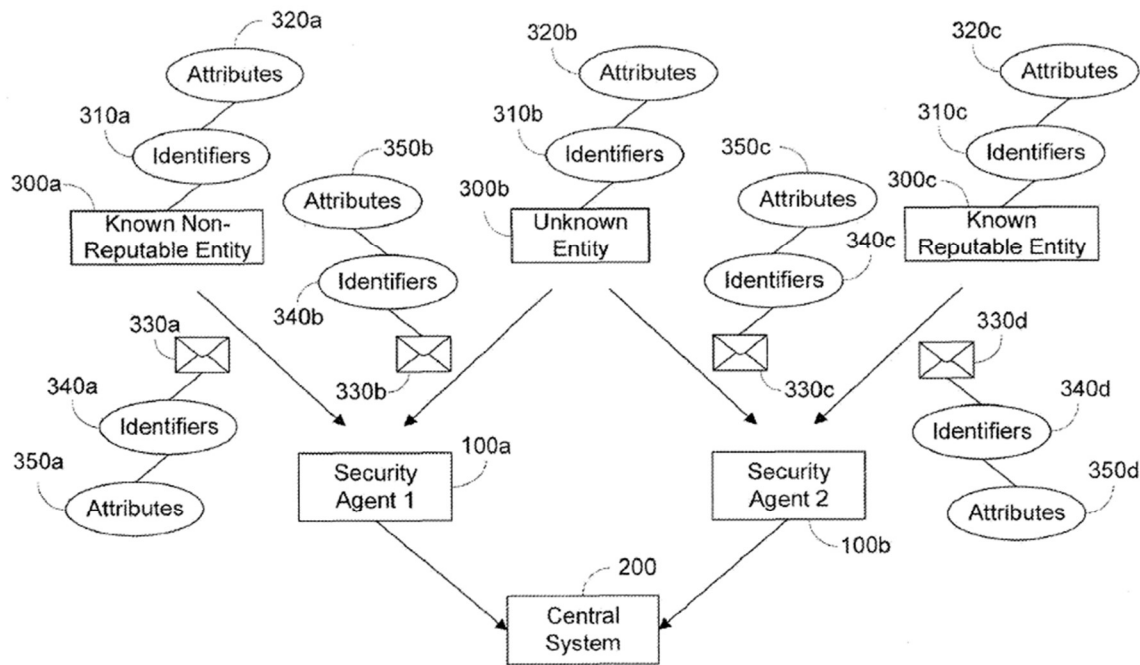


FIG. 3

(EX-1006 FIG. 3.)

Alperovitch discloses that a communication entity's reputation may be based on its observed behavior. (EX-1006 [0045].) Such behavior may include “a specific set of sending patterns, blacklist events, or specific attributes of the evidentiary data.” (EX-1006 [0048].) Alperovitch does not explain what a “blacklist event” is or how it is used.. (*Id.*)

B. Ground 1: Petitioner Fails To Establish That The Combination Of Hubbard-495 And Hubbard-174 Renders Obvious The “Security History” Factor Limitation In All Challenged Claims

Petitioner’s first ground relies on a combination of Hubbard-495 and Hubbard-174. (Petition 24–26, 52, 58.) Petitioner asserts that Hubbard-495 alone teaches a reputation vector that includes a “security history” factor. It does not, for the reasons discussed below.

Each challenged independent claim recites a “reputation vector” that includes a plurality of factors, including “security history,” “legitimacy,” “behavior,” “associations,” and “location”:

Claim limitation	Claim Language
1[c2]	“the reputation vector comprising a plurality of factors for the Internet resource comprising <i>security history</i> , legitimacy, behavior, associations and location”
7[e3]	“the reputation vector comprising a plurality of factors for the Internet resource comprising <i>security history</i> , legitimacy, behavior, associations and location”
11[c2]	“a reputation vector for the Internet resource comprising <i>security history</i> , legitimacy, behavior, associations and location”

13[c2]	“the reputation vector comprising a plurality of factors for the Internet resource comprising <i>security history</i> , legitimacy, behavior, associations and location”
--------	---

Each challenged claim requires (1) a “security history” for the internet resource whose reputation index is being determined and (2) a reputation vector that uses the internet resource’s “security history” as a factor in determining the reputation index of the internet resource. (EX-1001 cls. 1, 7, 11, 13.)

First, each challenged claim recites a “security history” for the internet resource whose reputation index is being determined. (*Id.*) As discussed above, the term “security history” refers to a history of security events for an internet resource. *See*, Section III.C, *supra*. The claim language also requires that the claimed “security history” is for the same internet resource whose reputation is being determined. For example, claim 1 recites a “method for controlling access to an Internet resource” that includes the step of “determining if a reputation index for the Internet resource is at or above a threshold value . . .” where the reputation index is generated from a reputation vector for the Internet resource that includes “a plurality of factors for the Internet resource,” with one of those enumerated factors being the Internet resource’s “security history.” EX-1001 (claim 1, 15:66-16:14). This claim

language identifies “security history” as a factor “*for the Internet resource*” and requires that “*the internet resource*” is the same internet resource whose reputation index is generated using the reputation vector. Each challenged independent claim includes similar language. (EX-1001 (cl. 7, 16:63-17:1 “the reputation vector comprising a plurality of factors for the Internet resource comprising security history...”), claim 11, 17:28-39 “accessing a reputation index for the Internet resource, the reputation index based on a reputation vector for the Internet resource comprising security history...”), *id.* cl. 13, 18:1-20 (“constructing a reputation vector for the Internet resource...the reputation vector comprising a plurality of factors for the Internet resource comprising security history...”).)

Second, the claims recite that “security history” is a factor used in a reputation vector that determines the reputation index of the internet resource whose reputation index is being determined. As shown in the table above, the challenged claims require that the reputation vector includes “a plurality of factors for the Internet resource,” with one of those enumerated factors being the internet resource’s “security history.” (EX-2001 ¶¶69-70) The challenged claims further state that the claimed “reputation index” is generated from the “reputation vector.” (EX-1001 cl.1; *see also* cl. 7 (“generating a reputation index for the Web site from the reputation vector, the reputation vector comprising a plurality of factors for the Internet

resource comprising security history..."); cl. 11 (17:28-39 "accessing a reputation index for the Internet resource, the reputation index based on a reputation vector for the Internet resource comprising security history...").)

A POSITA would understand that the claimed "security history" is included as a factor in the reputation vector so that the reputation index of the internet resource may take its security history into account. (EX-2001 ¶70) Indeed, as discussed above, the specification explains that the reputation of an internet resource may be lowered when there are too many security breaches. (EX-1001 8:58-67)

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

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

First, Petitioner incorrectly argues that Hubbard’s reference to “[c]ertificate details associated with the URL (e.g., for secure (such as HTTPS) access schemes)” discloses the “security history” limitation. (Petition 25.) These criteria do not teach the claimed “security history” factor and, at most, relate to “legitimacy” of an internet resource, which all challenged claims recite as a factor distinct from the “security history” factor. (EX-2001 ¶73.)

“Certificate details” for secure access schemes such as HTTPS provide information that indicates whether a particular URL is currently secured via a security protocol known as Secure Sockets Layer (SSL). (EX-2001 ¶73.). Being secured via the SSL protocol increases the likelihood that an internet resource has a

high legitimacy—hence the certificate. (*Id.*) The '386 patent identifies SSL Security as one of the factors that determines legitimacy: “[l]egitimacy is determined by the top-level domain, the investment in the Internet resource (virtual hosting with non-affiliated sites, multiple hosting and **SSL security**).” (EX-1001 9:10-14 (emphasis added).) Thus, the “certificate details” criteria in Hubbard-495 would at most relate to the claimed “legitimacy” factor (and a *current* state of the URL, not its history), not the “security history” factor.

Second, Petitioner cites Hubbard-495’s reference to “active content previously identified with reference to the host, the hosts’ domain, or the URL path” (Petition 25.) These criteria also do not disclose or render obvious the claimed “security history” factor. Hubbard-495’s “active content previously identified” is not “security history.” According to Hubbard-495, “[a]ctive content” is simply content in a webpage that provides interactive or dynamic qualities to the website. (EX-1004 1:34-52.) “Active content” includes GIFs, JavaScript, and streaming audio and/or video. (EX-2001 ¶75.) This “active content” does not include any information about “security,” much less a history of security events, for an internet resource. (*Id.* ¶¶75-76) Indeed, the '386 patent specification distinguishes website **content** from past malware infections reflected in the security history:

Security solutions, such as anti-virus products, examine file or Web page content to discover known patterns or signatures that represent

security threats to users, computers, or corporate networks. *These focus not on the subject matter of a site [content], but look for viruses and other malware that are currently infecting the site.*

(EX-1001 1:41-46 (emphasis added).) A POSITA would not understand, and Petitioner fails to explain, how a general reference to the active content for a website resource could be used as a “security history” factor in a reputation vector used to determine a reputation index for an internet resource. (EX-2001 ¶¶74-76.)

Third, Petitioner cites Hubbard-495's reference to a “fingerprint,” but this reference does not disclose or render obvious the claimed “security history” factor. (Petition 26.) Hubbard-495 includes only one reference to a “fingerprint” in its list of scoring criteria: “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).” (EX-1004 19:13-17.) Hubbard-495's “fingerprint,” like the “active content” discussed above, relates to the *content* of a webpage located at a URL, and whether the content of the page being analyzed has the same fingerprint as previously analyzed URLs. (EX-2001 ¶77) Petitioner fails to explain, and a POSITA would not understand, how this reference to a fingerprint provides information about the extent and frequency of prior malware infections that could

be used as a “security history” factor to generate a reputation index for the internet resource. (EX-2001 ¶77.)

Accordingly, because Hubbard-495 does not teach the claimed “security history” factor, and because Petitioner does not assert that Hubbard-174 teaches this limitation, the combination of the two Hubbard references does not render any challenged '386 patent claim obvious. Petitioner's first ground therefore fails.

C. Ground 2: Petitioner Fails To Establish That The Combination Of Hubbard-495, Hubbard-174, And Alperovitch Renders Obvious The “Security History” Limitation In All Challenged Claims

In its second ground, Petitioner argues that Alperovitch discloses the “security history” factor recited in claim elements 1[c2], 7[e3], 11[c2], and 13[c2]. (Petition at 72-73.) Petitioner's argument fails because Alperovitch does not teach this limitation and because Petitioner has not shown adequate motivation to combine Alperovitch with the two Hubbard references.

1. Alperovitch Does Not Disclose or Render Obvious the Claimed “Security History” Factor

Petitioner relies on Alperovitch's reference to a “behavioral profile” as allegedly disclosing the “security history” factor recited in all challenged claims of the '386 patent. Petition at 73. As discussed above in Section IV.B, the claims require (1) a “security history” for the internet resource whose reputation index is being determined and (2) a reputation vector that uses the internet resource's

“security history” as a factor in determining the reputation index of the internet resource.

Alperovitch's behavioral profile does not disclose or render obvious these requirements of the “security history” factor. First, Petitioner states that Alperovitch discloses that its “behavioral profile” may include “a specific set of sending patterns” and “blacklist events.” Petition at 73. Neither discloses or renders obvious the claimed “security history” factor. (EX-2001 ¶81) For example, “sending patterns” and “blacklist events” are, at most, only part of a larger “behavioral profile.” Alperovitch's “behavioral profile” is not even limited to historical data and does not describe a history security events. (EX-2001 ¶82; EX-1006 [0048]) Petitioner does not explain, and Alperovitch does not disclose, how a behavioral profile constitutes a history of security events for the internet resource whose reputation is being determined. (EX-2001 ¶82) Nor does Petitioner explain, or Alperovitch describe, how a “behavioral profile” is used as a factor to generate the reputation index of a particular internet resource to account for the extent of that resource's historical security events. (EX-2001 ¶82)

In particular, Alperovitch's reference to “blacklist events” does not disclose a “security history” for an internet resource being analyzed. (EX-2001 ¶82.) Petitioner does not show, and Alperovitch does not describe, how Alperovitch's “blacklist

events” might be used as a factor in a reputation vector so that the reputation index of the internet resource. (*Id.*)

Second, Petitioner's reliance on Alperovitch's reference to a “behavioral profile” conflates two separate factors of the claimed reputation vector. As discussed above, the challenged claims of the '386 patent all require a reputation vector that includes five specific factors—“security history, legitimacy, **behavior**, associations and location.” (*See* Section IV.B, *supra*; EX-2001 ¶84.) Petitioner's reliance on Alperovitch's “behavioral profile” and “behavioral events relevant to defining the disposition of an entity matching the profile” at best might have suggested the “behavior” factor for assessing reputation, but not the separate “security history” factor. (EX-1001 9:8-27.)

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

vulnerabilities, or how often these exploits occur. (EX-2001 ¶85.) Rather, a specific set of sending patterns pertains to behavior of the individual or entity sending the messages, particularly behavioral patterns. (EX-2001 ¶85.)

Accordingly, Petitioner has failed to establish that Alperovitch discloses or renders obvious the claimed “security history” factor. Petitioner’s second ground therefore fails.

2. There Was No Motivation to Combine Hubbard-495 and Hubbard-174 with Alperovitch

A POSITA would not have been motivated to combine Hubbard-495 and Hubbard-174 with Alperovitch because these references are not analogous art and are not in the same field of endeavor, and because Petitioner provides no guidance as to how these references would have been combined or modified.

Alperovitch is not analogous to or reasonably pertinent to the ’386 patent, as it seeks to solve different problems from those of the ’386 patent. For example, the ’386 patent seeks to prevent users in a network seeking access to internet resources with malicious or inappropriate content from being granted access to those resources. In contrast, Alperovitch seeks to identify individuals send message recipients malicious or inappropriate content. The vulnerabilities, vectors for exploitation, and communication protocols are not the same (*e.g.*, Alperovitch’s “sending patterns” and criteria for generating a “behavioral profile” are different

from concerns involving users visiting webpages and other internet resources, such as popularity rank of the resource), and a POSITA would not have looked to systems for monitoring email, VoIP, instant message, or other messaging systems to identify dangerous internet resources such as webpages or files requested by users. (EX-2001, ¶¶90-92.)

Further, Petitioner does not explain how a POSITA would have combined the teachings of these references. (*Id.*) Hubbard-495 relates to categorizing webpages and websites. Hubbard-174 is directed to filtering active content from webpages, namely search engine results. (*Id.* ¶88) Unlike the two Hubbard references, Alperovitch is directed to securing messaging systems, such as emails and instant messages, by identifying messaging accounts that exhibit malicious behavior. (*Id.*)

In fact, rather than focusing on websites as Hubbard-495 and Hubbard-174 do, Alperovitch is entirely focused on protecting against disreputable individuals that may send messages (*e.g.*, VoIP calls, e-mails, instant messages, etc.), which is why Alperovitch's disclosure relates to "behavioral profiles." (*Id.* ¶90-92; EX-1006 [0032], [0048]) Petitioner does not explain how a POSITA would have reconciled these differences.

Petitioner oversimplifies Alperovitch in arguing that both it and the Hubbard references "determine conditions under which access to an Internet resource is

allowed.” (Petition at 71 (citing EX-1006 [0073])) In the passage cited by Petitioner, Alperovitch describes throttling communications between telephonic devices attempting to establish a real-time VoIP connection. (EX-1006 [0071]-[0072]) Specifically, Alperovitch describes the time-sensitive nature of initiating VoIP connections. (EX-1006 [0072]). Accordingly, Alperovitch describes assessing a reputation of a communications account in order to determine whether a real-time connection should be established. (*Id.* at [0073])

Alperovitch explains that this would involve assessing the behavioral profile of a message sender, as opposed to the factors involved in assessing a reputation of a webpage as described in Hubbard-495. This difference is evident from the passage from Alperovitch that Petitioner relies on for the “security history” limitation, which is not consistent with the webpages described in Hubbard-495 or Hubbard-174. (Petition 73-74; EX-1002 ¶215 (citing EX-1006 [0048]) For example, Alperovitch describes “sending patterns” (which is consistent with someone making calls or sending emails, as opposed to a webpage visited by a user) and vaguely referenced “blacklist events” (which neither Hubbard-495, Hubbard-174, nor Alperovitch define) and other “behavioral events relevant to defining the disposition of an entity matching the profile.” (EX-2001 ¶ 89; EX-1006 [0048])

Alperovitch identifies the following attributes as relevant to the behavior of an account sending outgoing messages: “a specific set of sending patterns, blacklist events, or specific attributes of the evidentiary data. Some examples include: Sender/Receiver Identification; Time Interval and sending patterns; Severity and disposition of the payload; Message construction; Message quality; Protocols and related signatures; Communications medium.” (EX-1006 [0048]) These factors not consistent with the webpages/URLs described in Hubbard-495 and Hubbard-174. (*See, e.g.*, EX-1004 18:53-19:61; *see generally* EX-1005 (lacking any reference to reputation analysis)). In light of these inconsistencies and differences, Petitioner does not explain how a POSITA would have modified Hubbard-495 and Hubbard-174, or otherwise combined Alperovitch's “communications entity” behavioral profile with the URL reputation analysis module disclosed in Hubbard-495.

Modifying or combining these references would have been impractical. While Alperovitch states that “hackers often attempt to use various network-type applications (*e.g.*, e-mail, web, instant messaging (IM) etc.), Alperovitch does not disclose how to address web-based threats. (EX-1006 [0032]) At most, Alperovitch discloses identifying e-mail and instant messaging accounts for entry on a blacklist, but does not teach identifying risks associated with webpages described in Hubbard-495 or Hubbard-174. (EX-2001 ¶91) For instance, Hubbard-495 and Hubbard-174

focus on identifying risk factors associated with a URL host. (EX-2001 ¶¶90.) A POSITA would understand that such risk factors would not be useful to Alperovitch's method, because wrongdoers using Gmail accounts would have higher reputations merely for using a known, reputable email server to send suspicious or dangerous emails. (*Id.*) Conversely, a large number of wrongdoers would negatively affect Gmail's reputation index, thereby lowering the reputation scores of every other Gmail account. (*Id.*) Similarly, Alperovitch's behavioral profile for messaging system would not be useful to the methods of Hubbard-495 or Hubbard-174, because the examples described in Alperovitch are not relevant to the URLs referenced in the Hubbard references. (*Id.* at ¶¶91-93) By Petitioner's logic, any system or method involving cybersecurity or reputation would have been obvious to a POSITA to combine, regardless of their field of endeavor, teachings, and goals for improvement over the art. (*Id.*)

Based on the above, there was no motivation to combine Alperovitch with Hubbard-495 or Hubbard-174. Alperovitch is neither in the same field of endeavor nor reasonably pertinent to the particular problem with which the inventors of the '386 patent were involved. Further, Alperovitch is non-analogous art to the '386 patent, Hubbard-495, and Hubbard-174, and thus cannot serve as a reference for Petitioner's second obviousness ground.

V. PETITIONER'S GROUNDS FAIL TO ANTICIPATE OR RENDER OBVIOUS ALL DEPENDENT CLAIMS

Because Petitioner has fails to establish that any of its grounds render obvious all limitations of independent claims 1, 7, 11, and 13, Petitioner cannot show that such grounds render obvious dependent claims 2-6, 8-10, 12, 15, 16, and 18.

VI. OTHER LIMITATIONS NOT ADDRESSED

At this preliminary stage, Patent Owner addresses those deficiencies in the prior art which clearly show a lack of reasonable likelihood of the petition's success. Patent Owner's decision not to address certain limitations at this preliminary stage in no way reflects Patent Owner's agreement with the petition or lack of dispute as to these additional limitations.

VII. SECONDARY OBJECTIVE INDICIA OF NONOBVIOUSNESS

In determining obviousness of the claimed invention, objective evidence of secondary considerations pertaining to nonobviousness must be considered, including long-felt but unsolved needs, failure of others, commercial success, etc. *In re Huang*, 100 F.3d 135, 139 (Fed. Cir. 1996) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966)). These indicia constitute independent evidence of nonobviousness that can be the most probative evidence in that regard "in avoiding the trap of hindsight when reviewing, what otherwise seems like, a combination of

known elements.” *Leo Pharm. Prods., Ltd. v. Rea*, 726 F.3d 1346, 1358 (Fed. Cir. 2013).

The Board has repeatedly cautioned “that known evidence of secondary considerations should be addressed in the petition.” *See, e.g., Robert Bosch Tool Corp. v. SD3, LLC*, IPR2016-01751, (PTAB March 22, 2017) (Paper 15 at 23) (collecting prior Board decisions that deny institution based, at least in part, on a petitioner’s failure to address known evidence of secondary considerations of non-obviousness). Despite Patent Owner providing evidence regarding the long-felt, unmet need for the invention and commercial success in its district court complaint against Petitioner, Petitioner fails to address or consider any such evidence in its petition; thus, institution should be denied.

As discussed above, a long-felt and persistent need existed to improve malicious content identification and internet access control before the invention of the ’386 patent. (*See* Section III.A, *supra*; EX-2001 ¶98.) Prior attempts to develop real-time malware protection failed to consider various factors necessary to assess the likelihood that an internet resource contained malicious or inappropriate content and employed broad, inflexible systems, making them insufficient to identify and address the threats faced by modern computer networks. (*See* Section III.A, *supra*;

EX-2001 ¶98.) Where others failed, the inventors of the '386 patent succeeded. (See Section III.B, *supra*; EX-2001 ¶¶97-99.)

Patent Owner currently accuses Petitioner of infringing the technology claimed in the '386 patent, demonstrating the critical need and widespread industry reliance on these novel methods. Petitioner, in particular, markets and provides the Forcepoint ONE Secure Web Gateway, Advanced Classification Engine, and ThreatSeeker Intelligence, the components of which practice the system and methods claimed in the '386 patent. (See EX-2012.)

VIII. CONCLUSION

For the foregoing reasons, the challenged claims of the '386 patent are patentable and the Board should decline to institute IPR.

Date: August 17, 2023

Respectfully submitted,

KING & SPALDING LLP

BY: /Brian Eutermoser/
Brian Eutermoser
Registration No. 64,058

*Attorney for Patent Owner
Open Text Inc.*

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PATENT OWNER PRELIMINARY RESPONSE** specified in 37 C.F.R. § 42.24 have 10,130 words, in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24. This word count was prepared using Microsoft Word 365 V.2022.

Date: August 17, 2023

Respectfully submitted,

KING & SPALDING LLP

BY: /Brian Eutermoser/
Brian Eutermoser
Registration No. 64,058

*Attorney for Patent Owner
Open Text Inc.*

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER'S PRELIMINARY RESPONSE** and all supporting **EXHIBITS 2001-2012** were served by filing the documents through the Patent Trial and Appeal Case Tracking System (P-TACTS) on August 17, 2023 and courtesy copies were also served via electronic mail, in their entireties on the following:

Kat Li
Reg. No. 64,857
kat.li@kirkland.com
Forcepoint_Webroot_IPR@kirk-
land.com
KIRKLAND & ELLIS LLP
401 Congress Avenue
Austin, TX 78701
Telephone: (512) 678-9100
Facsimile: (512) 678-9101

*Counsel for Petitioner
Forcepoint LLC*

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

Nadia E. Haghighatian (pro hac vice to
be filed)
nadia.haghighatian@kirkland.com
KIRKLAND & ELLIS LLP
401 Congress Avenue
Austin, TX 78701
Telephone: (512) 678-9100
Facsimile: (512) 678-9101

Date: August 17, 2023

KING & SPALDING LLP

BY: /Brian Eutermoser/

Brian Eutermoser
Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.