

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Sophos Ltd. and Sophos Inc.,
Petitioners,

v.

Webroot Inc.,
Patent Owner.

Case No. IPR2023-00633

U.S. Patent No. 8,726,389

Petition for *Inter Partes* Review of U.S. Patent No. 8,726,389

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

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. MANDATORY NOTICES	2
A. Real Parties-in-Interest 37 C.F.R. §42.8(b)(1)	2
B. Related Matters Under 37 C.F.R. §42.8(b)(2)	2
1. Current Litigation.....	2
2. Administrative Proceedings	2
C. Lead and Back-Up Counsel.....	3
D. Service of Information Under 37 C.F.R. §42.8(b)(4)	4
III. PAYMENT OF FEES	4
IV. REQUIREMENTS OF <i>INTER PARTES</i> REVIEW	4
A. Standing.....	5
B. Identification of Challenge and Relief Requested	5
C. How the Challenged Claims Are to Be Construed Under 37 C.F.R. §42.104(b)(3)	7
D. How the Challenged Claims Are Unpatentable Under 37 C.F.R. § 42.104(b)(4).....	8
E. Supporting Evidence Under 37 C.F.R. §42.104(b)(5)	8
V. THRESHOLD REQUIREMENT FOR <i>INTER PARTES</i> REVIEW	9
VI. PERSON OF ORDINARY SKILL IN THE ART	9
VII. STATE OF THE ART	10
A. Malware.....	10
B. Malware Detection Software.....	10
VIII. OVERVIEW OF THE '389 PATENT	11
IX. DETAILED CHALLENGE	14

TABLE OF CONTENTS

(continued)

	<u>Page</u>
A. Ground 1: Halperin Renders Obvious Claims 1-6, 8-13, 15-20, 22-27, 29, 30.....	14
1. Prior Art Overview.....	14
2. Analysis.....	16
B. Ground 2: Halperin in View of Kirby Renders Obvious Claims 3, 5, 7, 9–13, 17, 19, 21, 23–27	43
1. Prior Art Overview.....	43
2. Motivation to Combine and Reasonable Expectation of Success	44
3. Analysis.....	45
C. Ground 3: Halperin in View of Kirby and Mankins Renders Obvious Claims 14 and 28	56
1. Prior Art Overview.....	56
2. Motivation to Combine and Reasonable Expectation of Success	57
3. Analysis.....	60
X. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION.....	66
A. PTAB Should Not Exercise Its Discretion to Deny Institution Under <i>Fintiv</i>	66
1. Factor 1: Likelihood of Stay	67
2. Factor 2: District Court Schedule	67
3. Factor 3: Petitioners’ Investment in IPR Outweighs Forced Investment in Litigation to Date	70
4. Factor 4: The Petition Raises Unique Issues	71

TABLE OF CONTENTS

(continued)

	<u>Page</u>
5. Factor 5: Institution Will Provide the Board an Opportunity to Invalidate Claims That Later Could Be Reasserted Against Others	72
6. Factor 6: Other Circumstances Support Institution	73
B. PTAB Should Not Exercise its Discretion To Deny Institution Under <i>Becton</i> and <i>Advanced Bionics</i>	73
XI. CONCLUSION.....	75
XII. CERTIFICATE OF WORD COUNT	75

TABLE OF AUTHORITIES

	<u>Page(s)</u>
Cases	
<i>10X Genomics, Inc. v. Bio-Rad Labs., Inc.</i> , IPR2020-00086, Paper 8 (Apr. 27, 2020).....	7
<i>Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH</i> , IPR2019-01469, Paper 6 (Feb. 13, 2020).....	73
<i>Amperex Tech. Ltd. v. Maxell, Ltd.</i> , IPR2021-0142, Paper 16 (Apr. 12, 2022).....	74
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR 2020-00019, Paper 15 (May 13, 2020).....	72
<i>Apple Inc. v. Seven Networks</i> , IPR2020-00255, Paper 13 (July 28, 2020)	71
<i>Becton, Dickinson & Co. v. B. Braun Melsungen AG</i> , IPR2017-01586, Paper 8 (Dec. 15, 2017)	73
<i>Cizion, LLC v. Kerr Machine Co.</i> , PGR2020-00065, Paper 10 (Dec. 3, 2020).....	68, 69
<i>Crowdstrike, Inc. v. Webroot Inc.</i> , IPR2023-00556, Paper 1 (Feb. 17, 2023).....	2
<i>DJI Europe B.V. v. Textron Innovations, Inc.</i> , IPR2022-00453, Paper 10 (Aug. 3, 2022).....	74
<i>HTC Corp. v. Cellular Communications Equip., LLC</i> , 877 F.3d 1361 (Fed. Cir. 2017)	7
<i>KSR Int’l Corp. v. Teleflex, Inc.</i> , 550 U.S. 398 (2007).....	58, 60

*Petition for Inter Partes Review
of U.S. Patent No. 8,726,389*

<i>Micron Tech., Inc. v. Godo Kaisha IP Bridge 1,</i> IPR2020-01008, Paper 10 (Dec. 7, 2020)	68
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.,</i> 868 F.3d 1013 (Fed. Cir. 2017)	8
<i>Oticon Medical AB v. Cochlear Ltd.,</i> IPR2019-00975 Paper 15, 20 (Oct. 16, 2019)	75
<i>REG Synthetic Fuels, LLC v. Neste Oil, Oyj,</i> IPR2018-01375, Paper 11 (Feb. 19, 2019)	74
<i>Sand Revolution II, LLC v. Continental Intermodal Grp.,</i> IPR2019-01393, Paper 24 (June 16, 2020)	67, 71
<i>Samsung Elec. 's Co., Ltd. v. Staton Techniya, LLC,</i> IPR2022-00302, Paper 13, 10 (July 11, 2022)	69
<i>Tianma Microelectronics Co. Ltd. v. Japan Display Inc.,</i> IPR2021-01028, Paper 14 (Dec. 14, 2021)	74
<i>Volkswagen Grp. of Am., Inc. v. Arigna Tech. Ltd.,</i> IPR2021-01321, Paper 10 (Feb. 15, 2022)	67
<i>Webroot Inc, et al. v. Sophos Ltd.,</i> No. 6:22-cv-240 (W.D. Tex.)	2
<i>Webroot, Inc. et al. v. AO Kaspersky Lab,</i> No. 6:22-cv-243 (W.D. Tex.)	2
<i>Webroot, Inc. et al. v. CrowdStrike Holdings, Inc. et al.,</i> No. 6:22-cv-241 (W.D. Tex.)	2
<i>Webroot, Inc. et al. v. Forcepoint LLC,</i> No. 6:22-cv-00342-ADA-DTG (W.D. Tex.)	2
<i>Webroot, Inc. et al. v. Sophos Ltd.,</i> No. 6:22-cv-00240-ADA-DTG (W.D. Tex.)	72

*Petition for Inter Partes Review
of U.S. Patent No. 8,726,389*

<i>Webroot, Inc. et al. v. Trend Micro, Inc.,</i> No. 6:22-cv-239 (W.D. Tex.)	2
<i>Western Digital Corp. v. Kuster,</i> IPR2020-01391, Paper 10 (Feb. 16, 2021)	67
<i>Western Digital Corp. v. SPEX Techs., Inc.,</i> IPR2018-00082, Paper 11 (Apr. 25, 2018)	7

Statutes

35 U.S.C. § 102	5, 6
-----------------------	------

Other Authorities

Katherine K. Vidal, <i>Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings With Parallel District Court Litigation,</i> https://www.uspto.gov/sites/default/files/documents/interim_proc_ discretionary_denials_aia_parallel_district_court_litigation_memo_ _20220621_.pdf	69
---	----

*Petition for Inter Partes Review
of U.S. Patent No. 8,726,389*

TABLE OF EXHIBITS

Ex. No.	Document
1001	U.S. Patent No. 8,726,389 (“the ’389 Patent”)
1002	File History for U.S. Patent No. 8,726,389
1003	Complaint, <i>Webroot Inc, et al. v. Sophos Ltd.</i> , No. 6:22-cv-240 (W.D. Tex.)
1004	Declaration of Dr. Richard Newman
1005	Curriculum Vitae of Dr. Richard Newman
1006	U.S. Patent Pub. No. 2004/0111632 to Halperin (“Halperin”)
1007	U.S. Patent No. 7,694,150 to Kirby (“Kirby”)
1008	U.S. Patent No. 7,900,194 to Mankins (“Mankins”)
1009	Stipulation Waiving IPR Claims in District Court Litigation
1010	Sophos Central Admin, Threat Graphs, SOPHOS LTD., https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/ThreatAnalysisCenter/ThreatGraphs/index.html (last visited Feb. 15, 2023)
1011	Sophos Central Admin, Threat Graph Analysis, SOPHOS LTD., https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/ThreatAnalysisCenter/ThreatGraphs/ThreatAnalysisDetails/index.html (last visited Feb. 15, 2023)
1012	Excerpt from Transcript of Motions Hearing in <i>Webroot, Inc., et al. v. AO Kaspersky Lab</i> , No. 6:22-cv-00243-ADA-DTG (W.D. Tex.) (Dec. 9, 2022)
1013	Order Granting Fourth Amended Scheduling Order, Dkt. 160, <i>Webroot, Inc., et al. v. AO Kaspersky Lab</i> , No. 6:22-cv-00243-ADA-DTG (W.D. Tex.) (Jan. 22, 2023)

I. INTRODUCTION

Sophos Ltd. and Sophos Inc. petition for *inter partes* review (“IPR”), seeking cancellation of claims 1-30 of U.S. Patent No. 8,726,389 (the “’389 Patent,” EX-1001). This Petition demonstrates there is at least a reasonable likelihood Petitioners will prevail on at least one of the challenged claims based upon prior art references the USPTO did not have before it during prosecution.

The ’389 patent describes and claims a purportedly novel system in which computer objects are examined to determine whether or not they are, and should be classified as, malware. Among other things, the patent describes multiple remote computers that transmit data about a computer object to a base computer, which correlates the data and determines whether the computer object should be classified as malware.

None of this was new. As demonstrated below, at the time of the purported invention, it was well known in malware detection to receive data about a computer object from first and second remote computers, correlate the received data, and compare the correlated data to another object or entity to identify malware. Therefore, claims 1-30 should be canceled as unpatentable under 35 U.S.C. § 103 over the prior-art references identified in this Petition.

II. MANDATORY NOTICES

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

Sophos Ltd., and Sophos Inc. are the real parties-in-interest.

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

1. Current Litigation

The '389 Patent is the subject of litigation in five suits brought by Patent Owner against Petitioner Sophos Ltd. and four other defendants in: *Webroot Inc, et al. v. Sophos Ltd.*, No. 6:22-cv-240 (W.D. Tex.) (EX-1003); *Webroot, Inc. et al. v. Trend Micro, Inc.*, No. 6:22-cv-239, (the “Trend Micro Action”); *Webroot, Inc. et al. v. CrowdStrike Holdings, Inc. et al.*, No. 6:22-cv-241, (the “CrowdStrike Action”); *Webroot, Inc. et al. v. Forcepoint LLC*, No. 6:22-cv-00342-ADA-DTG (W.D. Tex.)(the “Forcepoint Action”); and *Webroot, Inc. et al. v. AO Kaspersky Lab*, No. 6:22-cv-243, (the “Kaspersky Action”). These cases are consolidated in Case No. 6:22-cv-00243-ADA-DTG (W.D. Tex.).

2. Administrative Proceedings

On February 17, 2023, CrowdStrike, Inc. filed a petition for *inter partes* review challenging all claims of the '389 patent. *See Crowdstrike, Inc. v. Webroot Inc.*, IPR2023-00556.

C. Lead and Back-Up Counsel

Petitioners provide the following designation of counsel:

Lead Counsel	Backup Counsel
Ryan Iwahashi (Reg. No. 63,378) Gibson, Dunn & Crutcher LLP 1881 Page Mill Road Palo Alto, CA 94304-1211 Tel: (650) 849-5367 RIwahashi@gibsondunn.com	Josh Krevitt (<i>pro hac vice</i> motion requested) Gibson, Dunn & Crutcher LLP 1881 Page Mill Road Palo Alto, CA 94304-1211 Tel: (212) 351-2490 JKrevitt@gibsondunn.com
	Brian A. Rosenthal (<i>pro hac vice</i> motion requested) Gibson, Dunn & Crutcher LLP 200 Park Avenue New York, NY 10166-0193 Tel: (212) 351-2339 BRosenthal@gibsondunn.com
	Timothy P. Best (<i>pro hac vice</i> motion requested) Gibson, Dunn & Crutcher LLP 333 South Grand Avenue Los Angeles, California 90071-1504 Tel: (213) 229-7659 TBest@gibsondunn.com

Petitioners respectfully request authorization to file motions for Josh Krevitt, Brian Rosenthal, and Timothy Best to appear before the USPTO *pro hac vice*. Mr. Krevitt, Mr. Rosenthal, and Mr. Best are experienced litigating attorneys and

*Petition for Inter Partes Review
of U.S. Patent No. 8,726,389*

are currently serving as lead counsel for Petitioners in the District Court Action. Each has established familiarity with the subject matter at issue in this proceeding. Petitioners intend to file a motion to appear *pro hac vice* under 37 C.F.R. § 42.10. Pursuant to 37 C.F.R. § 42.10(b), powers of attorney accompany this petition.

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

Service of any documents via hand delivery may be made at the mailing address of lead and backup counsel designated above. Petitioners also hereby consent to electronic service, and service via electronic mail may be made at the email addresses provided above for the lead and backup counsel.

III. PAYMENT OF FEES

Pursuant to 37 C.F.R. §§42.103 and 42.15(a), the required fee was submitted, but the Office is authorized to charge any fee deficiency, or credit overpayment, to Deposit Account 50-1408, including additional fees due in connection with this Petition.

IV. REQUIREMENTS OF INTER PARTES REVIEW

Pursuant to 37 C.F.R. §42.104, each requirement for *inter partes* review of the '389 Patent is satisfied.

A. Standing

Pursuant to 37 C.F.R. § 42.104(a), Petitioners certify the '389 patent is available for IPR and Petitioners are not barred or estopped from requesting IPR of the claims on the ground identified herein. Specifically, Petitioners certify: Petitioners have not filed a civil action challenging the validity of the '389 patent; this Petition is filed not more than one year from March 11, 2022, the date on which Sophos Ltd. was served with the Complaint by Petitioners, alleging infringement of the '389 patent; the estoppel provisions of 35 U.S.C. § 315(e)(1) do not prohibit this *inter partes* review; and this petition is filed after the later of (a) the date that is nine months after the date of the grant of the '389 patent or (b) the termination of any post-grant review of the '389 patent.

B. Identification of Challenge and Relief Requested

Pursuant to 37 C.F.R. §42.104(b), Petitioners request the Board institute *inter partes* review of claims 1-30 of the '389 Patent on one or more grounds under pre-AIA 35 U.S.C. §§102 and/or 103. Petitioners request that claims 1-30 be canceled in view of the following prior-art references:

*Petition for Inter Partes Review
of U.S. Patent No. 8,726,389*

Patent/ Publication	Filing/ Priority Date	Date of Publication	Exhibit No.
Halperin	May 5, 2003	June 10, 2004	EX-1006
Kirby	June 22, 2004	April 6, 2010	EX-1007
Mankins	March 25, 2004	March 1, 2011	EX-1008

The '389 Patent is a U.S. Patent resulting from application No. 13/543,866, filed June 8, 2012, a continuation of application No. 11/477,807, filed June 30, 2006, which claims priority to foreign patent GB 0513375.6, filed June 30, 2005. Claims 1-30 of the '389 Patent are entitled to a priority date no earlier than June 30, 2005.¹ Accordingly, Halperin qualifies as prior art at least under 35 U.S.C. §102(b), and Kirby and Mankins qualify as prior art at least under 35 U.S.C. §102(e).² Halperin, Kirby, and Mankins were not cited during the '389 Patent's prosecution.

In this *inter partes* review, Petitioners apply the above references and assert the following grounds of rejection under 35 U.S.C. §103:

¹Petitioners assume for purposes of this Petition a priority date of June 30, 2005. Petitioners do not concede any claim of the '389 Patent is entitled to that or any earlier priority date. The Board need not resolve any priority issues for the purposes of this Petition.

²Unless specifically noted, all references to Title 35 of the United States Code refer to code pre-America Invents Act. *See, e.g.*, 35 U.S.C. § 102 (2011).

*Petition for Inter Partes Review
of U.S. Patent No. 8,726,389*

Ground	Claims	Proposed Statutory Rejections
1	1-6, 8-13, 15-20, 22-27, 29, 30	Obvious under 35 U.S.C. §103 over Halperin
2	3, 5, 7, 9-13, 17, 19, 21, 23-27	Obvious under 35 U.S.C. §103 over Halperin in view of Kirby
3	14, 28	Obvious under 35 U.S.C. §103 over Halperin in view of Kirby and Mankins

C. How the Challenged Claims Are to Be Construed Under 37 C.F.R. §42.104(b)(3)

Petitioners do not believe any constructions affect the invalidity analyses set forth herein. *See HTC Corp. v. Cellular Communications Equip., LLC*, 877 F.3d 1361, 1367–68 (Fed. Cir. 2017) (affirming the Board’s application, absent an express construction of a term). Although Petitioners and Patent Owner disagree over the construction of certain terms in the parallel district-court litigation, for the purpose of this Petition, Petitioners rely on Patent Owner’s proposed constructions (plain and ordinary meaning). *See 10X Genomics, Inc. v. Bio-Rad Labs., Inc.*, IPR2020-00086, Paper 8 at 17–22 (PTAB Apr. 27, 2020) (a Petitioner need only identify “[h]ow the challenged claim is to be construed” for purposes of the petition, and “judicial efficiency will be enhanced by allowing Petitioner to rely upon a claim construction that Patent Owner is relying upon in the related district court litigation

to assert infringement of the challenged patent”); *see also Western Digital Corp. v. SPEX Techs., Inc.*, IPR2018-00082, Paper 11 at 12 (PTAB Apr. 25, 2018).

Moreover, the Board “need only construe terms ‘that are in controversy, and only 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) (citation omitted). Because Petitioners base this Petition on constructions *Patent Owner* has advocated, the Petition presents no controversy over claim meaning and the Board need not construe any terms. *Nidec*, 868 F.3d at 1017. Petitioners maintain the Challenged Claims would have been obvious under any reasonable construction.

D. How the Challenged Claims Are Unpatentable Under 37 C.F.R. § 42.104(b)(4)

An explanation of how the Challenged Claims are unpatentable, including the identification of where each element of the claim is found in the prior-art patents or printed publications, is provided below.

E. Supporting Evidence Under 37 C.F.R. §42.104(b)(5)

The exhibit numbers of the supporting evidence relied upon and the relevance of the evidence to the challenged claims, including an identification of specific portions of the evidence supporting the challenge, are provided above. A list identifying the exhibits is also included. The Expert Declaration of Dr. Richard

Newman (EX-1004) further supports the Petition’s technical evidence and grounds for rejection.

V. THRESHOLD REQUIREMENT FOR INTER PARTES REVIEW

Under 35 U.S.C. §314(a), institution of *inter partes* review requires “a reasonable likelihood that the petitioners would prevail with respect to at least one of the claims challenged in the petition.” This Petition meets this threshold for each of the asserted grounds.

VI. PERSON OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (“POSITA”) in June 2005 would have had at least a Bachelor’s degree in Computer Science, Computer Engineering, Electrical Engineering, or an equivalent discipline, and at least two years’ worth of experience developing dynamic malware detection and computer networking or network architecture, or a Master’s degree in a related field. EX-1004 ¶17. Alternatively, a POSITA could have four or more years of work experience in computer networking and in the development of client-server systems. *Id.* A POSITA would either have six months’ experience as a network or system administrator, or have taken two advanced computer-security courses. *Id.*

VII. STATE OF THE ART

All concepts in this section were well known and widely used by POSTAs at least as of June 30, 2005.

A. Malware

Malware (malicious software) refers to software developed to modify, steal, or destroy data on a computer or a computer network. EX-1004 ¶32-33. Malware is often introduced into a computer or computer network through the Internet or an external storage device. *Id.* ¶34.

B. Malware Detection Software

Traditional malware detection software relies on signature-matching to identify malicious code. EX-1004 ¶35. A signature is a sequence of bytes that uniquely identify a computer object based on characteristics such as the content or metadata of the object. *Id.* When a new computer object is introduced into a user's computer, the malware-detection software generates one or more signatures for that object and searches a malware-detection-software provider's database for a match. *Id.* If the generated signature is found in the database, the object can be classified as malware and isolated. *Id.*

Although the use of signatures is effective, it has well-known, significant disadvantages. EX-1004 ¶36. Signatures can be written only after the malware-detection provider has seen a malware sample, so new and sufficiently different malicious code that is may spread before the provider can add a signature for that new code into the database. *Id.*

Another method of malware detection that was known in the art is behavior analysis, which evaluates the actions or intended actions of a computer object. EX-1004 ¶38-39. Behavior-based analysis does not require the computer object to be previously known because it examines the actual or expected behavior of a computer object. *Id.* Often, behavior-based antivirus software includes policies that define the actions an object can or cannot do. *Id.* ¶39-40. If an object performs or tries to perform an action that is considered malicious or not known to be safe, the object may be classified as malware. *Id.*

VIII. OVERVIEW OF THE '389 PATENT

The '389 Patent purports to describe a “method of classifying a computer object as malware, includ[ing] receiving at a base computer data about a computer object from each of plural remote computers.” EX-1001, Abstract. According to the patent, prior-art anti-malware programs often used databases of “signatures in

the object that are known to be indicative of the presence of a virus,” but “[h]euristic methods have also been employed” to detect malware. *Id.* at 1:23–34. The patent asserts that delay between new pieces of malware coming into existence and the generation and release of signature updates to service providers’ databases left users at risk. *Id.* at 1:35–42. Further, “malware writers use obfuscation techniques in order to attempt to hide the signature or signature base data of the virus code from detection.” *Id.* at 1:42–47.

According to the patent, an anti-malware program using data about the same or similar computer object from “different remote computers to determine whether or not a particular object should be classed as good or as malware”, *id.* at 3:16–18, can overcome these vulnerabilities. The claimed system is depicted in Figure 1 (reproduced below):

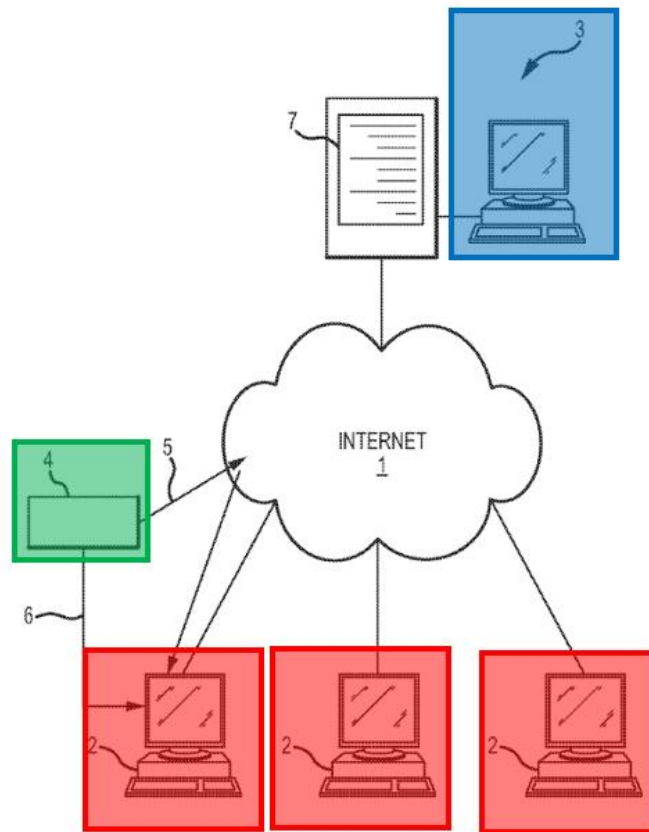


FIG.1

The '389 Patent explains that a plurality of **remote computers 2** are in communication with a **base or central computer 3**. *Id.* at 7:59-8:1. When an unknown **computer object 4** is discovered on a **remote computer 2**, the **remote computer 2** sends data representing that **computer object 4** to the **base computer 3**. *Id.* at 8:47-53. The **base computer 3** receives data from multiple **remote**

computers 2 and correlates the data. *Id.* at 10:43-46. The correlated data can then be compared to data corresponding to another object or entity. The unknown computer object may be classified as malware on the basis of that comparison. *Id.* at 3:37-39, 10:51-11:4.

IX. DETAILED CHALLENGE

A. Ground 1: Halperin Renders Obvious Claims 1-6, 8-13, 15-20, 22-27, 29, 30

Halperin discloses “a computer virus detection and containment system,” EX-1006, [0021], that classifies an object as malware by correlating data about that object received from plural remote computers:

After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers.

Ex. 1006, [0047].

1. Prior Art Overview

Like the '389 Patent, Halperin discloses “detecting malicious activity in a computer network,” EX-1006, Abstract, “by correlating behavior and/or data from different computers.” EX-1006, [0037]. Halperin proposes a solution “that

overcomes disadvantages of the prior art,” EX-1006, [0007], which Halperin describes as “virus scanners [that] operate by searching a computer for tell-tale byte sequences known as ‘signatures’ that exist in known viruses,” EX-1006, [0005], and “antivirus software that employs heuristic techniques to identify typical virus behavior...and then identifying any deviation from such behavior.” EX-1006, [0006]. Figure 5 of Halperin (shown below) is “a simplified conceptual illustration” of Halperin’s disclosure:

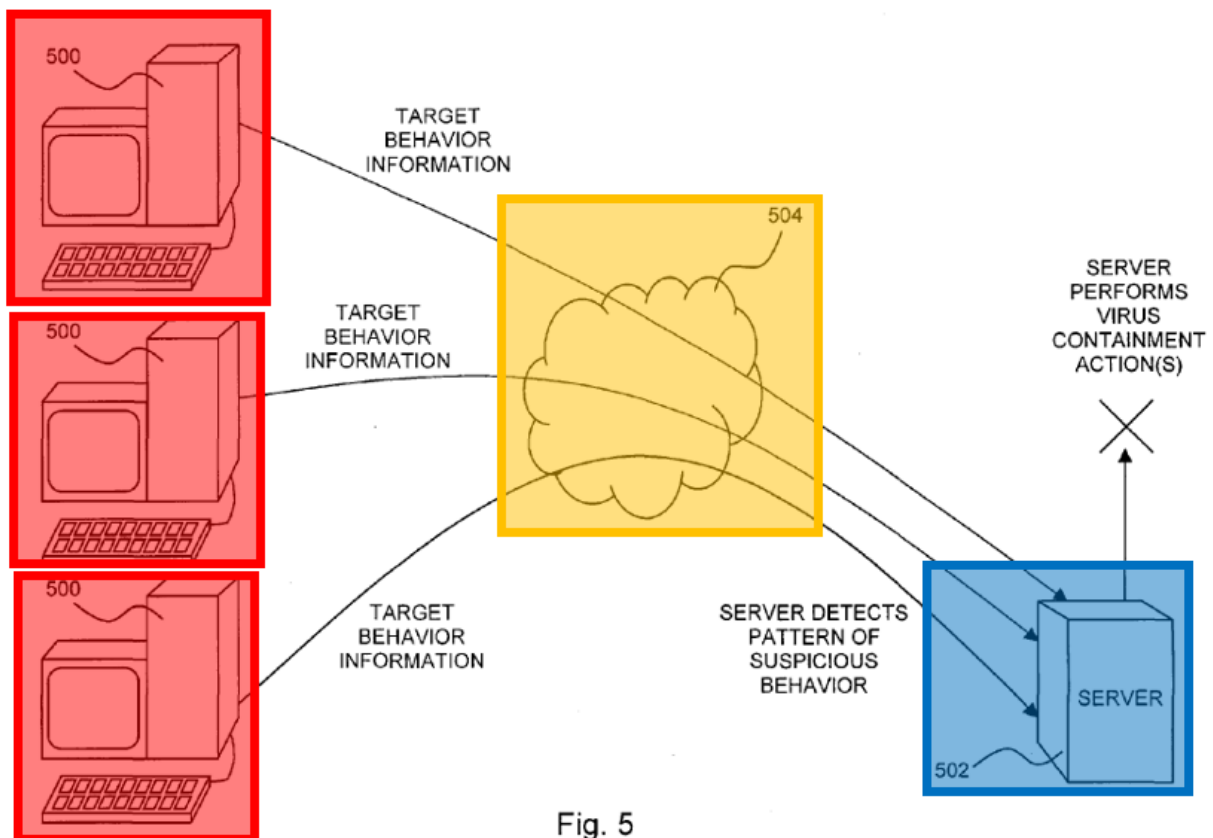


Fig. 5

“In the system of Figure 5 one or more **computers 500** are shown, being configured to communicate with a **server 502** via a **network 504**, such as the Internet.” EX-1006, [0036]. **Server 502** “may be configured with such target behavior profiles and may detect associated target behavior at **computers 500** using conventional techniques.” *Id.*, [0047]. “After collecting information regarding target behavior detected at two or more of **computers 500**, **server 502** may then correlate the presence of target behavior detected at two or more of **computers 500** in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern.” *Id.*, [0047]. Halperin then compares the correlated data to another object or entity, specifically a “predefined suspicious behavior pattern of target behavior.” *Id.*, [0038]. Based on the comparison between the correlated data and the “predefined suspicious behavior pattern of target behavior,” Halperin may determine that “malicious software has been identified.” *Id.*, [0047], [0073].

2. Analysis

Halperin discloses and renders obvious all features of claims 1-6, 8-13, 15-20, 22-27, 29, and 30 of the '389 Patent.

a) Independent Claim 1

[1P]: A method of classifying a computer object as malware, the method comprising:

To the extent the preamble is claim-limiting, Halperin discloses [1P]. EX-1004 ¶62. Halperin discloses a system and method of “detection and prevention of malicious computer programs.” EX-1006, [0002]. Halperin discloses “malicious software detection algorithms” *id.* [0074], *i.e.*, methods for classifying software (“a computer object”) as malware, such that “when malicious software has been identified . . . it is possible to isolate the mechanism that has been spreading the malicious software,” *id.* [0073]. Thus, a POSITA would understand Halperin’s disclosure of methods for detecting and identifying software as “malicious” as disclosing a “method of classifying a computer object as malware.”

[1A]: at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored,

Halperin discloses [1A]. EX-1004 ¶63-68. For example, in Figure 5, Halperin discloses a base computer (**server 502**) and a first remote computer (one of **computers 500**). EX-1006, Fig. 5, [0047]. Halperin discloses the base computer (**server 502**) receiving data about a computer object—e.g., “target behavior

information” (Fig. 5) associated with a potential “**virus**”—from a first remote computer (one of **computers 500**). EX-1006, Fig. 5, [0036]-[0037], [0047].

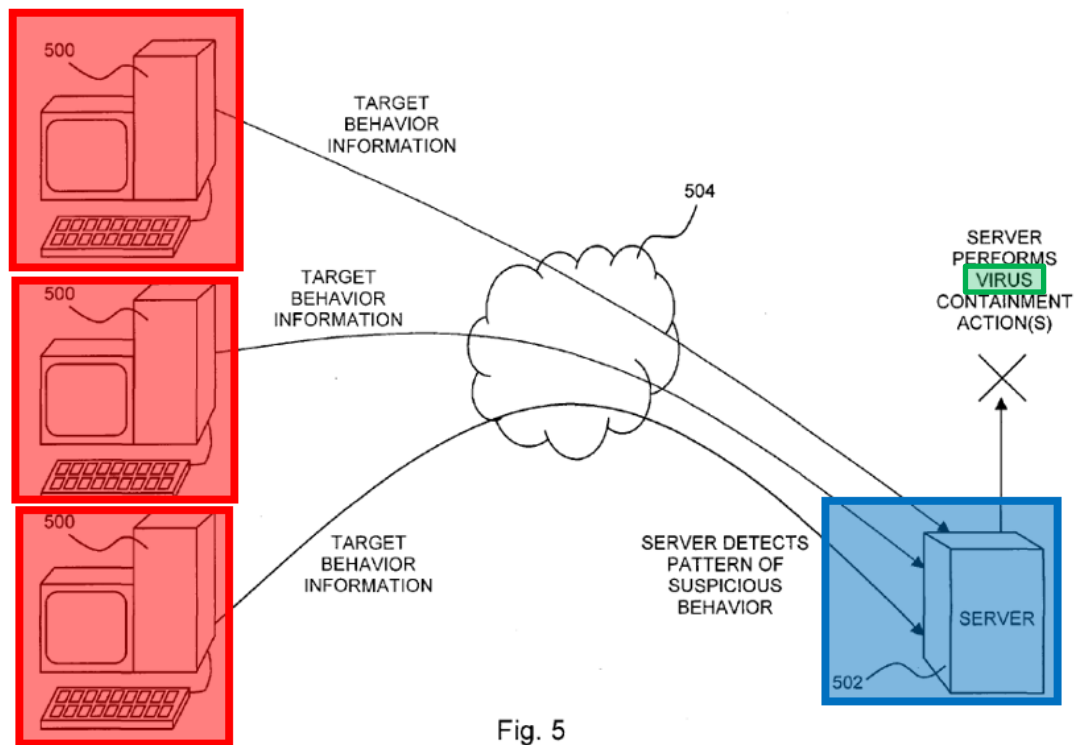


Fig. 5

Halperin discloses “target behavior profiles are defined for **computers 500**. Each target behavior profile describes behavior that should be the subject of correlation analysis.” *Id.*, [0038]. Thus, **computers 500** can “detect associated target behavior and notify **server 502** accordingly” and **server 502** “collect[s] information regarding target behavior detected at two or more of **computers 500**.” *Id.*, [0047]; EX-1004 ¶65. Further, with reference to “the embodiments described

hereinabove” (*i.e.*, including the Figure 5 embodiment), Halperin discloses “each computer” logging “any predefined suspicious event that takes place” and discloses “[t]hat information is logged in a central database,” *i.e.*, at the base computer. EX-1006, [0086]. A POSITA would have understood the “target behavior” and the “predefined suspicious event[s]” detected by the computers and received by the base computer to be data about a computer object (*i.e.*, a potential **virus**) or similar computer objects stored on at least one of **computers 500**, as Halperin’s purpose is to determine whether “a computer virus may have infected those computers.” *Id.* [0047]; EX-1004 ¶66. Thus, Halperin discloses “at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored.”

[1B]: wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;

Halperin discloses [1B]. EX-1004 ¶69-74. Halperin discloses eight examples of “target behavior” detected on the remote computers “that should be the subject of correlation analysis” by the base computer. EX-1006, [0038]-[0046]. Halperin also refers to these as “predefined suspicious event[s].” *Id.*, [0086]. One example is

“[m]odifying operating system files such as the Microsoft Windows® registry.” *Id.*, [0041]; *see also id.*, [0086]. A POSITA would understand Halperin’s “target behavior” and “predefined suspicious event[s]” from one of the computers in Halperin (the “first remote computer”) are events initiated by or involving the computer object (*i.e.*, potential virus) when it is created, configured, or runs on the first remote computer. EX-1004 ¶70.

Halperin further discloses the information received at the base computer including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed. EX-1004 ¶71. Halperin discloses that logging each “predefined suspicious event” includes “the *type of event*, time of event and *on which computer it took place*.” EX-1006, [0086]; *id.* [0090] (“The logging preferably includes the *type of event*, the time it occurred and *on which computer it occurred* (if relevant)”).³ Moreover, a POSITA would understand from Halperin’s registry-edit example that the information received at the base computer would include the event type (registry edit), and the identity of the entity on which the event is being performed (the

³ All emphases added, unless otherwise noted.

Microsoft Windows® Registry). EX-1004 ¶72. Thus, Halperin discloses “said information including at least . . . the event type, and an identity of an . . . entity on which the event is being performed.” *Id.*

Halperin also discloses the information received at the base computer including at least an identity of an object initiating the event. For example, Halperin discloses a “characteristic code may be generated” for an “e-mail attachment that when activated causes the malicious software to spread,” such as by “using well known ‘checksum’ algorithms.” EX-1006, [0073]. Halperin explains the “checksum may then be sent to neighboring computers . . . which may then use the checksum to identify suspicious malicious software upon arrival at these computers.” *Id.* Thus, a POSITA would understand Halperin’s “predefined suspicious event” information includes “at least an identity of an object initiating the event,” which can be determined by checksum. EX-1004 ¶74. Moreover, a POSITA would understand the identity of the object initiating the event necessarily must be collected to perform the correlation analysis Halperin discloses and ultimately to determine whether the object is malware. *Id.* At a minimum, it would have been obvious to include an identity of an object initiating the event, e.g., the checksum of

the email attachment Halperin discloses, in the suspicious-event information logged in the central database in Halperin. *Id.*

[1C]: at a base computer, receiving data about the computer object from a second remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured, or runs on the second remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;

Halperin discloses [1C]. EX-1004 ¶75-77. Halperin explains:

[C]omputer viruses typically infect a computer system by moving from one computer to another within a computer network A computer virus can thus be detected by correlating behavior and/or data from different computers. Activity that cannot be confidently attributed to a virus when observed on one computer can be clearly identified as such when observed on several computers in a network.

Ex. 1006, [0037]. Accordingly, Halperin discloses server 502 “collecting information regarding target behavior [of a potential virus] detected **at two or more computers 500.**” EX-1006, [0047]. Halperin discloses “*each computer*” in the system logs “any predefined suspicious event that takes place” and the “information is logged in a central database . . . for *each event.*” *Id.*, [0086]; *id.*, [0090] (“the system logs *every event* of a sensor identifying a suspicious behavior”). Thus, the “two or more computers 500” include the first and second remote computers, and each provides to the base computer the information described in step [1B].

EX-1004, ¶77. That is, Halperin discloses the same information as in [1B] is received from a second remote computer. And because, as explained regarding [1D] below, Halperin discloses “correlat[ing]” the data received from the two or more computers 500, EX-1006, [0047], and a POSITA would have known such correlation would require the information describe the “computer object or similar computer objects.” As such, Halperin discloses [1C].

[1D]: storing, at the base computer, said data received from the first and second remote computers;

Halperin discloses [1D]. EX-1004 ¶78-79. Halperin states the information received from the remote computers “is logged in a central database.” EX-1006, [0086]. A POSITA would understand this logging requires storing the received data. EX-1004 ¶79. Moreover, Halperin discloses “correlat[ing]” the data received from the two or more computers 500. EX-1006, [0047]. A POSITA would understand the act of correlating data necessarily requires storing the data. EX-1004 ¶79.

[1E]: correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;

Halperin discloses [1E]. EX-1004 ¶80-83. Halperin explains “[a]ctivity that cannot be confidently attributed to a virus when observed on one computer can be

clearly identified as such when observed on several computers in a network.” EX-1006, [0037]. Thus, “[a]fter collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern.” EX-1006, [0047]. Halperin explains “any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers.” EX-1006, [0047]; EX-1004 ¶81. Halperin’s “two or more of computers 500” constitute the first and second remote computers, and Halperin discloses correlating at least some of the data about the computer object (potential virus) received from each. Therefore, Halperin discloses [1E]. EX-1004 ¶81.

[1F]: comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and

Halperin discloses [1F]. EX-1004 ¶84-87. Once Halperin’s base computer correlates the data received from the first and second computers, the base computer

compares the correlated data to another computer object or entity, *i.e.*, a “predefined suspicious behavior pattern of target behavior.” EX-1006, [0047]–[0056]. Specifically, Halperin teaches “determin[ing] whether the correlated target behavior *corresponds* to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers.” EX-1006, [0047]. A POSITA would understand that a “predefined suspicious behavior pattern of target behavior” is data about the behavior of malicious code. EX-1006, [0047]–[0056]; EX-1004 ¶86. Thus, by determining whether the “correlated target behavior” “corresponds” to the “predefined suspicious behavior pattern of target behavior,” Halperin discloses comparing the correlated data to another object or entity (*i.e.*, data about the behavior of malicious code). EX-1004 ¶86.

Moreover, for its infringement allegations, Patent Owner asserts this limitation is met when the data uploaded from an endpoint is checked against a set of rules. Although Petitioner disputes Patent Owner’s infringement allegations, under Patent Owner’s apparent interpretation, Halperin discloses this limitation because it discloses comparing the data received from the first and second remote computers to one or more rules that trigger “containment actions” (e.g., if correlated data shows “[a] certain percentage of the computers in the network sending more

than 10 messages per minute in the last 5 minutes”). EX-1006, [0048]-[0057]; EX-1004 ¶87.

[1G]: classifying, by the base computer, the computer object as malware on the basis of said comparison.

Halperin discloses [1G]. EX-1004 ¶88-90. Halperin explains if the base computer determines “the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior,” it classifies the computer object as malware (*e.g.*, a “computer virus”). See EX-1006, [0047], [0057], [0073], [0074], ; *id.* [0087] (“The proposed system works in two phases to identify malicious code (from here on referred to as ‘viruses.’)”; *id.* [0061] (“[T]he identification of virus activity may include automatic identification of suspicious activity by a server or a combination of automatic identification and a notification of a system operator and approval by that operator that the suspicious activity is truly a virus, before notifying other servers.”). EX-1004 ¶89. Thus, by comparing the correlated data about a computer object to another object or entity, Halperin determines whether that computer object is malware and classifies it as such. *Id.* ¶90. A POSITA would further understand from Halperin that when the disclosed computer system responds to the detection of a virus (*e.g.* by “activat[ing] a virus alarm” or “initiat[ing] virus

containment actions,” EX-1006 [0090]), it is because the system has classified the computer object as malware. EX-1004 ¶90.

b) Independent Claim 15

Claim 15 has the same limitations as Claim 1, except that it claims an apparatus comprising “a base computer constructed and arranged to” perform the steps of Claim 1. As discussed in Section IX.IX.A.2.a) above, Halperin discloses a base computer (server 502) performing the steps recited in claim 1 and therefore also is “constructed and arranged to” perform the identical functions set out in claim 15. Halperin, therefore, also renders claim 15 obvious. EX-1004 ¶91.

c) Dependent Claims 2 and 16

Claim 2 depends from claim 1 and further requires “wherein the relationship is between objects related directly, or between objects related via other objects.” In its infringement contentions in the District Court, Patent Owner asserts this limitation is met by “Threat Graphs” that allow a user to “find out where an attack started, how it spread, and which processes or files it has affected,” EX-1010, *see also* EX-1011, and by identifying the root cause of a suspicious process. Halperin discloses the same: “For example, where malicious software is spread by e-mail, the e-mail attachment that when activated causes the malicious software to spread may

be identified.” EX-1006, [0073]. Moreover, Halperin further discloses identifying when, e.g., a “certain percentage of computers in the network” have deleted “a file by the same name,” or sent “the same file attachment,” file attachments where “each of the files includes the same string of bits,” or files with “the same or similar data.” *Id.* [0051]-[0056]. Thus, under Patent Owner’s reading, Halperin discloses this element, and renders the claim obvious. EX-1004 ¶¶92-94.

Claim 16 is the apparatus version of Claim 2, and is therefore disclosed by Halperin for the same reasons as Claim 2. EX-1004 ¶96.

d) Dependent Claims 3 and 17

Claim 3 depends from claim 1 and further requires “wherein where an object and other objects are found to have a relationship, monitoring those related objects as a homogenous entity and identifying a common object of the homogenous entity as a malware object.” Halperin discloses email objects may be found to have a relationship because “[i]n most cases, viruses are spread when computer users send infected files to other computer users via electronic mail (e-mail).” EX-1006, [003]. Halperin discloses monitoring email “as a homogenous entity,” because, e.g., a “virus may attach itself to otherwise innocuous e-mail messages.” *Id.*, [004].

Halperin further discloses identifying a common object (a malicious email attachment) as malware: “For example, where malicious software is spread by e-mail, the e-mail attachment that when activated causes the malicious software to spread may be identified.” EX-1006, [0073]. A “characteristic code may be generated for the attachment that distinguishes it from other such attachments.” EX-1006, [0073]. This code “may then be sent to neighboring computers within the group and to computers within neighboring groups which may then use the checksum to identify suspicious malicious software upon arrival at these computers.” EX-1006, [0073]; EX-1004 ¶97. Thus, Halperin renders claim 3 obvious. EX-1004 ¶98.

Claim 17 is the apparatus version of Claim 3, and is therefore obvious over Halperin for the same reasons as Claim 3. EX-1004 ¶98.

e) Dependent Claims 4 and 18

Claim 4 depends from claim 1 and further requires “comprising deducing an object to be malware based on the behavior of a related object.” Halperin discloses this element. EX-1004 ¶99-101. As previously discussed, Halperin teaches using a “known ‘checksum’ algorithm[]” to generate a “characteristic code” for an “e-mail attachment that when activated causes the malicious software to spread.” EX-1006,

[0073]. The “checksum may then be sent . . . to identify suspicious malicious software upon arrival at” other computers. EX-1006, [0073]. A POSITA would know the email attachment for which the characteristic code was generated is an object related to malicious software, and this email attachment is deduced to be malware based on the behavior of its child object. EX-1004 ¶99. Moreover, “[i]n order to anticipate the propagation path of malicious software within and between groups 800, the behavior of previous malicious software may be studied.” EX-1006, [0076]. Halperin describes ways objects’ behavior may indicate objects are malware. *Id.* And Halperin explains when a virus is detected based on its behavior, “neighboring groups [of computing devices] may be notified,” *id.* A POSITA would have known that notifying neighboring groups allows for classification and isolation of related objects. EX-1004 ¶101. Claim 4 is, thus, obvious over Halperin.

Claim 18 is the apparatus version of Claim 4, and is therefore obvious over Halperin for the same reasons as Claim 4. EX-1004 ¶102.

f) Dependent Claims 5 and 19

Claim 5 depends from claim 1 and further requires “wherein if at least one other object to which said computer object is related is classed as malware, then classifying said computer object as malware.” Halperin discloses this element. As

described regarding Claim 3, Halperin discloses identifying the “e-mail attachment that when activated causes the malicious software to spread.” EX-1006, [0073]. Halperin further discloses a “checksum” may be “generated for the attachment” and “sent to neighboring computers . . . which may then use the checksum to identify suspicious malicious software.” EX-1006, [0073]. Thus, because the checksum is “for the attachment” and is used to “identify suspicious malicious software,” Halperin discloses classifying the attachment as malware if it is related to at least one other object classed as malware (the “malicious software” that spreads when the attachment is “activated”). EX-1004 ¶103-104. Claim 5 is obvious over Halperin. *Id.* ¶103.

Claim 19 is the apparatus version of Claim 5, and is therefore obvious over Halperin for the same reasons as Claim 5. EX-1004 ¶105.

Moreover, to the extent not expressly disclosed, it would have been obvious to a POSITA to modify Halperin, and a POSITA would have been motivated to do so, such that if the correlated data about a computer object matches the data of known malware, the system would automatically classify the computer object as malware. Halperin recognizes that a specific object may create malware. Halperin would be able to classify an object as malware more quickly if the correlated data about a

computer object indicates that it is related to malware. EX-1004 ¶106. A POSITA would have had a reasonable expectation of successfully modifying Halperin in this manner. *Id.*

g) Dependent Claims 6 and 20

Claim 6 depends from Claim 1 and further requires “wherein said other objects include the object or similar objects stored on at least one of the first and second remote computers.” In its infringement contentions in the District Court, Patent Owner asserts this limitation is met by “Threat Graphs,” as discussed regarding Claim 2, which Patent owner asserts identify suspicious processes and similar/related processes, and by the ability to query devices in the network for data about objects from endpoints connected to the network. Halperin discloses the same, including, for example, “[a] certain percentage of the computers in the network sending file attachments via one or more messages in the last hour where each of the files includes ***the same string of bits.***” EX-1006, [0047], [0055]. A POSITA would understand that “the same string of bits” is a string of bits in the virus (“the object”) itself. EX-1004 ¶107-108. Thus, under Patent Owner’s reading, Halperin discloses the limitation of claim 6. Claim 6 is therefore obvious over Halperin. *Id.*

Claim 20 is the apparatus version of Claim 6, and is therefore obvious over Halperin for the same reasons as Claim 6. EX-1004 ¶109.

h) Dependent Claims 8 and 22

Claim 8 depends from Claim 1 and further requires “wherein the data about the computer object that is sent from the respective remote computer to the base computer and that is used in the comparison includes one or more of . . . the current name of the computer object.” Halperin discloses this element. One Halperin embodiment identifies malware by detecting “computers in the network sending the same file attachment via a message in the last 15 minutes.” EX-1006, [0054]. A common way to determine if two file attachments are the same is to compare file names. EX-1004 ¶110. A POSITA would have known that the current name of the computer objects must be sent to the base computer. *Id.* Halperin, thus, renders claim 8 obvious. Claim 22 is the apparatus version of Claim 8, and is therefore obvious over Halperin for the same reasons as Claim 8. *Id.* ¶110.

i) Dependent Claims 9 and 23

Claim 9 recites a “method according to claim 1, wherein the data is sent in the form of a key that is obtained by a hashing process carried out in respect of the objects on the respective remote computer.” Halperin discloses this element. As

described above regarding Claims 3 and 17, Halperin discloses generating a “characteristic code” identifying “the e-mail attachment that when activated causes the malicious software to spread” (*i.e.*, the computer object) “using well known ‘checksum’ algorithms.” EX-1006, [0073]. A POSITA would have known that a checksum identifying an attachment that, when activated, causes the object to spread, constitutes a key “obtained by a hashing process” carried out in respect of the objects on the respective remote computer. EX-1004 ¶112. Halperin, thus, renders claim 9 obvious. *Id.*

Moreover, to the extent not expressly disclosed, a POSITA would have found it obvious to modify Halperin to use any of the “well known ‘checksum’ algorithms” Halperin discloses, EX-1006, [0073], to send the “target behavior” Halperin discloses sending from the remote computers to the base computer (*e.g.*, *id.* [0038]) in the form of a key obtained by a hashing process carried out in respect of the objects on the respective remote computer. EX-1004 ¶113. Halperin discloses “[t]arget behavior may be any and all computer activity,” including information that would allow the base computer to identify “repeating patterns of data within the memories of two or more computers,” whether multiple computers have sent “the same file attachment,” and whether multiple computers have sent file attachments with “the

same string of bits.” EX-1006, [0038], [0047], [0054], [0055]. A POSITA would have understood these examples would require sending either the object itself (e.g., the email attachment) or, for example, a key obtained by a hashing process carried out in respect of the object. EX-1004 ¶113.

A POSITA would have been motivated to send this data from the remote computers to the base computer as a key, just as Halperin teaches regarding email attachments that have been identified as malicious (Ex. 1006 [0073]). EX-1004 ¶114. It was commonly known that a key representing an object is typically physically smaller than the object itself, and that smaller amounts of data are transmitted faster than larger amounts of data. *Id.* It therefore would have been obvious to a POSITA to send the data Halperin discloses sending from the remote computers to the base computer in the form of a key obtained by a hashing process carried out in respect of the objects on the respective remote computer. *Id.*

Claim 23 is the apparatus version of Claim 9, and is therefore obvious over Halperin for the same reasons as Claim 9. EX-1004 ¶115.

j) Dependent Claims 10 and 24

Claim 10 recites a “method according to claim 9, wherein the key has at least one component that represents executable instructions contained within or

constituted by the computer object.” As discussed regarding Claim 9 above, Halperin discloses generating a key identifying “the e-mail attachment that when activated causes the malicious software to spread” (*i.e.*, the computer object) “using well known ‘checksum’ algorithms.” EX-1006, [0073]. Because the key is obtained using a “checksum” algorithm run with respect to the attachment that, when activated, causes the computer object to spread, a POSITA would understand that the key would represent executable instructions contained within or constituted by the computer object. EX-1004 ¶116-17. Halperin, thus, renders Claim 10 obvious. *Id.*

As discussed with respect to Claim 9 above, to the extent not expressly disclosed, it would have been obvious to a POSITA to modify Halperin such that the remote computers send target behavior to the base computer in the form of a key, including wherein the key has at least one component that represents executable instructions contained within or constituted by the computer object. EX-1004 ¶119. Doing so would enable the base computer to conduct the analyses Halperin discloses, such as whether the object is “the same file attachment” sent by multiple remote computers or whether it contains “the same string of bits” (Ex. 1006, [0054], [0055]), while sending smaller amounts of data and therefore improving

transmission speed. EX-1004 ¶119. It therefore would have been obvious to a POSITA to send data including the executable instructions contained within or constituted by the object itself, as a key, and Halperin renders Claim 10 obvious for this additional reason. *Id.*

Moreover, for purposes of its infringement allegations, Patent Owner asserts that sending a SHA256 hash meets this limitation, without specifying what the hash contains. Halperin meets this limitation under Patent Owner’s own interpretation because Halperin sends data about the computer object in the form of a key that is obtained by a hashing process. EX-1004 ¶121.

Claim 24 is the apparatus version of Claim 10, and is therefore obvious over Halperin for the same reasons as Claim 10. EX-1004 ¶122.

k) Dependent Claims 11 and 25

Claim 11 recites a “method according to claim 9, wherein the key has at least one component that represents data about said computer object.” Halperin discloses this element. *See* IX.IX.A.2.j). An identification of “the e-mail attachment that when activated causes the malicious software” (i.e., the computer object) “to spread,” EX-1006, [0073], constitutes “data about said computer object.” EX-1004 ¶123. Moreover, the key Halperin discloses (the “checksum”) represents

the email attachment. Thus, a POSITA would understand that the key Halperin discloses has at least one component that represents data about the computer object, and thus Halperin renders claim 11 obvious. *Id.* ¶123.

To the extent not expressly disclosed, it would have been obvious to a POSITA to modify Halperin such that the data sent from the remote computers is in the form of a key, including at least one component that represents data about the computer object, for the same reasons discussed with respect to Claims 9 and 10. *See* Sections IX.IX.A.2.i)-j)); EX-1004 ¶124. Halperin, thus, renders Claim 11 obvious. *See* IX.A.2.j)); EX-1004 ¶124.

Claim 25 is the apparatus version of claim 11, and is therefore obvious over Halperin for the same reasons as claim 11. EX-1004 ¶125.

l) Dependent Claims 12 and 26

Claim 12 recites:

A method according to claim 11, wherein said data about said computer object includes at least one of:

the current name of the computer object;

the physical and folder location of the computer object on disk;

the original name of the computer object;

the creation and modification dates of the computer object;
vendor, product and version and any other information stored
within the computer object;
the computer object header or header held by the respective
remote computer; and,
events initiated by or involving the computer object when the
computer object is created, configured or runs on the respective
remote computers.

Halperin discloses this element. As discussed regarding Claims 9-11 above, it would have been obvious to a POSITA to send the data Halperin discloses sending about the computer object from the remote computers to the base computer in the form of a key representing data about the computer object. *See IX.IX.A.2.i)-k); EX-1004 ¶127.*

Moreover, a POSITA would understand from Halperin that the data represented in the key would include at least one of the items recited in Claim 12. For example, for the base computer to determine whether the computer object found on the remote computers is “the same file attachment,” as Halperin teaches (EX-1006, [0054]), it would be obvious for the data about the computer object to

include any or all of the information recited in Claim 12. EX-1004 ¶128. In addition, a POSITA would understand that for the base computer to correlate information about registry edits on the remote computers, as Halperin teaches (Ex. 1006 [0053]), the data represented by the key would necessarily include events initiated by or involving the computer object when the computer object is created or configured, or runs, on the respective remote computers. *See* Section IX.IX.A.2.a) (element [1B]); EX-1004 ¶131. Halperin, thus, renders claim 12 obvious. EX-1004 ¶131.

Claim 26 is the apparatus version of claim 12, and is therefore obvious over Halperin for the same reasons as claim 12. EX-1004 ¶132.

m) Dependent Claims 13 and 27

Claim 13 recites a “method according to claim 9, wherein the key has at least one component that represents the physical size of the computer object.” Halperin discloses this element. As discussed regarding Claims 10 and 11 above, Halperin discloses or renders obvious transmitting data about an object in the form of a key with at least one component representing data about the object itself (e.g., its executable instructions contained within or constituted by the malicious software). *See supra* IX.IX.A.2.j)-k); EX-1004 ¶134. To the extent not expressly disclosed, a POSITA would have known that metadata about the computer object, including its

physical size, could be used to help determine whether it was legitimate or likely malware. EX-1004 ¶134. For example, if an object purports to be a known, legitimate object, comparing its characteristics like physical size to the known characteristics of the object it purports to be can help identify whether the object is malware. *Id.* Thus, it would have been obvious to a POSITA to include in a key representing data about the computer object at least one component that represents the physical size of the computer object. Halperin, thus, renders claim 13 obvious. *Id.*

Claim 27 is the apparatus version of Claim 13, and is therefore obvious over Halperin for the same reasons as Claim 13. EX-1004 ¶135.

n) Dependent Claim 29

Claim 29 depends from Claim 1 and further requires a “computer program recorded on non-transitory computer readable medium comprising program instructions for causing a computer to perform the method of claim 1.” Halperin discloses this element: “While the methods and apparatus disclosed herein may or may not have been described with reference to specific hardware or software, it is appreciated that the methods and apparatus described herein may be readily implemented in hardware or software using conventional techniques.”

EX-1006, [0092]. A POSITA would understand at least hardware implementation to require using a non-transitory computer-readable medium, and Halperin therefore renders Claim 29 obvious. EX-1004 ¶137-38.

o) Dependent Claim 30

Claim 30 depends from Claim 1 and further requires “wherein the data received about the computer object from the first remote computer is different than the data received about the computer object from the second remote computer.” Halperin discloses this element. In the example above related to Claims 6 and 20, Halperin states that “‘polymorphic viruses’ may change their name as they move from one computer to another.” EX-1006, [0056]. As a result, the computer object (polymorphic virus) on the first remote computer may “not [] have the same name” as the same object stored on the second remote computer. EX-1006, [0056]. Halperin teaches identifying such viruses by “identify[ing] attachments that have the same or similar data, whether or not they have the same name.” EX-1006, [0056]. In this example, Halperin uses “similar” (i.e., not the same, different) data received from the two remote computers to determine the computer object is a virus. EX-1004 ¶139-40. Halperin, consequently, renders claim 30 obvious. *Id.* ¶140.

B. Ground 2: Halperin in View of Kirby Renders Obvious Claims 3, 5, 7, 9–13, 17, 19, 21, 23–27

1. Prior Art Overview

Kirby discloses a method and apparatus for virus detection. EX-1007, Abstract. Kirby purports to “overcome[] the above described shortcomings of the signature approach alone by providing an integrated approach which applies features of both the behavioral and signature approach in a parallel and complementary manner.” EX-1007, 2:56-62. Kirby’s behavior-based approach monitors actions performed by computer objects “to determine if the detected actions correspond to the suspicious behavioral actions of the behavior heuristic 112.” EX-1007, 10:54-60. If they do, the object is classified as “undesirable activity” (malware). EX-1007, 10:63–11:6; *see also id.* at 15:7–20. In addition, Kirby discloses that when the behavioral actions indicate an object is malware, the computer on which the object is found creates a “hash signature” of the object, “therefore enabling a signature based (immediate) prevention mechanism against subsequent occurrences of the malware on this or other computers.” *Id.* at 15:15-20.

2. Motivation to Combine and Reasonable Expectation of Success

Both Halperin and Kirby are directed to malware-detection systems and processes that use behavioral monitoring to address the “day zero” problem of traditional signature approaches. See EX-1004 ¶142; EX-1006 at [0005], [0007]; EX-1007 at 1:62-2:7, 2:12-25 (“Embodiments of the invention provide a behavioral approach to virus detection and processing of other malicious processing activity, that in contrast to conventional techniques, exhibits a substantial departure from the conventional day Zero problem.”). Kirby, in particular, focuses on combining behavioral and signature-matching approaches. EX-1007 at 2:56-62. A POSITA would have been motivated to combine the teachings of Halperin and Kirby for multiple reasons, including to produce the obvious, beneficial, and predictable result of incorporating Kirby’s signature-matching techniques to aid in the classification of malware. EX-1004 ¶143. Kirby would have been a natural place for a POSITA to look because Kirby’s system of classifying an object as malware using integrated behavioral analysis and signature-matching was known as an effective way to detect malware that would speed up the detection process. *Id.*

Further, a POSITA would have been motivated to use Kirby's teachings regarding identifying as malware objects that "touch" malware. EX-1004 ¶144. As Halperin discloses, viruses are "designed to infiltrate computer files and other sensitive areas on the computer." EX-1006 at [0003]. Thus, viruses modify existing programs or files to include viral code. EX-1004 ¶144. A POSITA would understand that, as a result, an object modified by a virus is likely to be malware itself. *Id.* Thus, a POSITA would have been motivated to modify Halperin by incorporating Kirby's teachings on classifying as malware objects that "touch," or have interacted with known malware. *Id.* ¶144; *see also* EX-1007 at 5:48-53.

3. Analysis

a) Halperin in View of Kirby Renders Obvious Claims 3 and 17 of the '389 Patent

Claim 3 recites the "method according to claim 1, wherein where an object and other objects are found to have a relationship, monitoring those related objects as a homogeneous entity and identifying a common object of the homogenous entity as a malware object." Petitioners submit under Ground 1 that Halperin alone renders obvious Claim 3. *See* Sections IX.IX.A.2.a), d). The combination of Halperin and Kirby also renders Claim 3 obvious.

Kirby teaches a method wherein an object and other objects are found to have a relationship: “For example, an incoming email attachment file may be deemed as ‘untrusted.’ A process reading the file and writing another file creates another untrusted file . . . any process or file which ‘touches’ an untrusted file may ‘inherit’ an untrustworthy trait” EX-1007 at 5:48–53; EX-1004 ¶147. Kirby further teaches monitoring those related objects as a homogeneous entity and identifying a common object of the homogenous entity as a malware object when “the pattern indicates a correspondence with undesirable . . . behavior.” EX-1007, at 5:54-55. As Kirby explains, “the security agent 110 employs the heuristic 112 in an ongoing manner, in which ‘untrusted’ objects and ‘suspect’ activities *are observed* and inherited by other processes and objects which interact. At some point, the heuristic 112 *identifies a complementary object* associated with the actions which is *likely the conveyance of malware*.” EX-1007, 15:8-13. A POSITA would understand from this disclosure the “complementary object” is a common object of the homogenous entity being “observed” (i.e., monitored) and that it is identified as malware to protect “against subsequent occurrences of the malware on this or other computers.” EX-1007, 15:10-20; EX-1004 ¶147.

As explained above, a POSITA would have been motivated to combine the teachings of Kirby with Halperin to improve the detection process. *See* Section IX.B.2; EX-1004 ¶148. A POSITA reviewing Halperin would have been motivated to seek a disclosure providing a method for detecting subsequent instances of detected malware. EX-1004 ¶148. Since Kirby and Halperin are both directed to malware-detection systems and processes, Kirby would have been a natural place for a POSITA to look. *Id.* A POSITA would have had a reasonable expectation of modifying Halperin to incorporate this aspect of Kirby as described above. *Id.* As such, the disclosures in Halperin and Kirby render claim 3 obvious. *Id.*

Claim 17 is the apparatus version of Claim 3, and is therefore rendered obvious by Halperin and Kirby for the same reasons as Claim 3. EX-1004 ¶149.

b) Halperin in View of Kirby Renders Obvious Claims 5 and 19 of the '389 Patent

Claim 5 recites the “method according to claim 1, wherein if at least one other object to which said computer object is related is classed as malware, then classifying said computer object as malware.” Petitioners submit under Ground 1 that Halperin alone renders obvious Claim 5. *See* Sections IX.IX.A.2.a), IX.A.2.f). The combination of Halperin and Kirby also renders Claim 5 obvious.

As discussed regarding Claim 3, Kirby teaches that “any process or file which ‘touches’ an untrusted file” (i.e., malware) “may ‘inherit’ an untrustworthy trait, which may then be passed on until the pattern indicates a correspondence with undesirable, and hence, preventable, behavior.” EX-1007, at 5:52-55. Kirby further discloses “‘untrusted’ objects and ‘suspect’ activities are observed and . . . the heuristic 112 identifies a complementary object associated with the actions” as “malware.” EX-1007, 15:8-20. A POSITA would understand these disclosures to teach that if at least one other object to which a computer object is related is classed as malware, then classifying the computer object as malware. EX-1004 ¶151. As explained above, a POSITA would have been motivated to combine the teachings of Kirby with Halperin, and would have reasonably expected this combination to be successful. *See* IX.B.2 Thus, Halperin and Kirby render Claim 5 obvious. EX-1004 ¶151.

Claim 19 is the apparatus version of Claim 3, and is therefore rendered obvious by Halperin and Kirby for the same reasons as Claim 3. EX-1004 ¶152.

**c) Halperin in View of Kirby Renders Obvious Claims 7
and 21**

Claim 7 recites the “method according to claim 1, wherein said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said computer object.” Petitioners submit under Ground 1 that Halperin alone renders obvious independent Claim 1. *See supra* Section IX.IX.A.2.a). The combination of Halperin with Kirby also renders Claim 7 obvious.

Kirby explains that “the invention focuses on the subject actor of suspect operations, such as the process writing or executing a file . . . the behavioral approach analyzes the actions performed and the provenance of the data used.” EX-1007, 2:25-30. A POSITA would have understood that by “executing a file,” an object creates another file, or a child object. EX-1004 ¶154-55. Thus, Kirby’s invention is concerned with identifying the object that executes a file that exhibits bad behavior, or the parent object to malware. *Id.* ¶155.

In addition, Kirby teaches “the security agent 110 employs the heuristic 112 in an ongoing manner, in which ‘untrusted’ objects and ‘suspect’ activities are observed and inherited by other processes and objects which interact.” EX-1007,

15:8–11. Thus, a computer object that is classified as “untrusted” (or malware) will pass down its “untrusted” (or malware) classification to “other processes and objects” (a child object) . EX-1004 ¶156.

As explained above, a POSITA would have been motivated to combine the teachings of Kirby with Halperin, and would have reasonably expected this combination to be successful. *See* IX.B.2. Thus, the disclosures in Halperin and Kirby render Claim 7 obvious. Claim 21 is the apparatus version of Claim 3, and is therefore rendered obvious by Halperin and Kirby for the same reasons as Claim 3. EX-1004 ¶158.

d) Halperin in View of Kirby Renders Obvious Claims 9 and 23

Claim 9 recites “the method according to claim 1, wherein the data is sent in the form of a key that is obtained by a hashing process carried out in respect of the objects on the respective remote computer.” Petitioners submit under Ground 1 that Halperin alone renders obvious Claim 9. *See* IX.IX.A.2.a), IX.A.2.i). The combination of Halperin with Kirby also renders Claim 9 obvious.

Kirby teaches a two-tiered virus-detection system that scans for viruses and monitors objects’ behavior. Kirby teaches that a “security agent” on the host

computer (*i.e.*, remote computer) includes “a scanner/extractor 124 for parsing objects such as files and delivering byte sequences to the signature generator 114 for computing a signature or hash.” EX-1007, 11:11–16. Kirby further discloses that the signature generated by the remote computer “is an identifier such as a hash, *i.e.* MD4, MD5, or SHA to name several known in the art, which are rapidly computable,” and that “other hashes or computations which are smaller than the entity they represent yet highly unlikely to be duplicated by a dissimilar entity” could be used. EX-1007, 12:37–43. Further, Kirby teaches the remote computer calculating the hash on the objects stored on the remote computers and transmitting it to the base computer, to give the base computer data about the computer objects. EX-1007 at 9:66-10:4, 15:21-26; EX-1004 ¶160-61. Modifying Halperin’s disclosures of sending data about a computer object to a base computer by sending the data in the form of a key obtained by a hashing process carried out in respect of the objects on the respective remote computers, as Kirby teaches, would have been an obvious combination of prior-art elements according to known methods to yield predictable results. EX-1004 ¶161. Thus, the combination of Halperin with Kirby also renders Claim 9 obvious. *Id.* ¶162. Claim 23 is the apparatus version of

Claim 9, and is therefore obvious over Halperin in view of Kirby for the same reasons as Claim 9. *Id.*

e) Halperin in View of Kirby Renders Obvious Claims 10 and 24

Claim 10 recites a “method according to claim 9, wherein the key has at least one component that represents executable instructions contained within or constituted by the computer object.” As discussed regarding Claim 9 above, Kirby discloses sending data about computer objects to a base computer (or AV server) in the form of a hash. Kirby further teaches “the signature is computed from the associated object (e.g. infected email attachment) of the behavioral actions and operable to indicate subsequent undesirable activity.” EX-1007 at 12:23-26. A POSITA would understand one way Kirby’s signature would be “operable to indicate subsequent undesirable activity” would be to include a component representing executable instructions contained within or constituted by the malware (i.e., the computer object), and it would have been obvious to a POSITA to include that component to improve detection. EX-1004 ¶163.

As discussed in Ground 1 above, Patent Owner asserts that sending a SHA256 hash meets this limitation. *See supra*, IX.IX.A.2.j). Kirby expressly discloses

sending a “SHA” hash. EX-1007 at 12:38-19. Thus, Kirby discloses this element under Patent Owner’s interpretation. EX-1004 ¶164.

Further, as explained regarding Claim 9 above, it would have been obvious to combine Halperin with Kirby’s key. EX-1004 ¶165. Thus, the combination of Halperin with Kirby also renders Claim 10 obvious. *Id.* Claim 24 is the apparatus version of Claim 10, and is therefore obvious over Halperin in view of Kirby for the same reasons as Claim 10. *Id.*

**f) Halperin in View of Kirby Renders Obvious Claims
11 and 25**

Claim 11 recites a “method according to claim 9, wherein the key has at least one component that represents data about said computer object.” As discussed regarding Claim 10 above, Kirby discloses generating a key “computed from the associated object (e.g. infected email attachment) of the behavioral actions,” *i.e.*, computed from the malware object. EX-1007 at 12:23-26. A POSITA would accordingly understand that the key Kirby discloses has at least one component that represents data about the computer object. EX-1004 ¶166. As further explained regarding Claim 10 above, it would have been obvious to a POSITA to modify Halperin with the key disclosed by Kirby. Thus, the combination of Halperin with

Kirby also renders claim 11 obvious. *Id.* Claim 25 is the apparatus version of Claim 11, and is therefore obvious over Halperin in view of Kirby for the same reasons as Claim 11. *Id.*

**g) Halperin in View of Kirby Renders Obvious Claims
12 and 26**

Claim 12 recites:

A method according to claim 11, wherein said data about said computer object includes at least one of:

- the current name of the computer object;
- the physical and folder location of the computer object on disk;
- the original name of the computer object;
- the creation and modification dates of the computer object;
- vendor, product and version and any other information stored within the computer object;
- the computer object header or header held by the respective remote computer; and,

events initiated by or involving the computer object when the computer object is created, configured or runs on the respective remote computers.

As discussed regarding Claim 11 above, Kirby discloses generating a key “computed from” the computer object. A POSITA would have known that a key computed from the computer object could include any of the information recited in claim 12, and it would have been obvious to a POSITA to represent at least one of the items recited in claim 12 in order to improve detection. EX-1004 ¶168. Thus, for the reasons explained above with respect to Claims 9-11, the combination of Halperin with Kirby also renders Claim 12 obvious. *Id.* Claim 26 is the apparatus version of Claim 12, and is therefore obvious over Halperin in view of Kirby for the same reasons as Claim 12. *Id.*

h) Halperin in View of Kirby Renders Obvious Claims 13 and 27

Claim 13 recites a “method according to claim 9, wherein the key has at least one component that represents the physical size of the computer object.” As discussed regarding Claim 12 above, Kirby discloses generating a key “computed from” the computer object. A POSITA would have known that a key computed from

the computer object could include at least one component that represents the physical size of the computer object, and it would have been obvious to a POSITA to include that information in order to improve detection, as discussed in Ground 1 above. *See supra*, IX.IX.A.2.m); EX-1004 ¶169. Thus, the combination of Halperin with Kirby also renders Claim 13 obvious. EX-1004 ¶169. Claim 27 is the apparatus version of Claim 13, and is therefore obvious over Halperin in view of Kirby for the same reasons as Claim 13. *Id.*

C. Ground 3: Halperin in View of Kirby and Mankins Renders Obvious Claims 14 and 28

1. Prior Art Overview

Mankins describes a “system and method for kernel-based intrusion detection using Bloom filters.” EX-1008 at 3:18-19. Mankins explains that “normal (i.e., expected) system-call behavior is defined by monitoring system-call behavior during operation of the computer program under training conditions (e.g., when the computer program is not subject to intrusion attacks). EX-1008 at 3:37-40. “The intrusion detection system then uses a Bloom filter to generate a Bloom filter data object containing data representative of the normal system-call behavior.” EX-1008 at 3:40-43. “The predefined Bloom filter data is representative of ‘normal’ computer program behavior, which refers to behavior that is expected during operation of the

computer programs when not subject to intrusion attempts.” EX-1008 at 3:26-30. “Anomalous behavior is identified when the actual system-call behavior does not have a match in the Bloom filter data object.” EX-1008 at 3:53-55.

2. Motivation to Combine and Reasonable Expectation of Success

It would have been obvious to a POSITA to incorporate Mankins’s Bloom filter data object into Halperin’s and Kirby’s integrated approach to malware detection in order to augment the detection of malware-based intrusions using expected system-call behavior, in addition to (or in place of) Halperin’s and Kirby’s behavioral approaches. EX-1004 ¶171. Halperin monitors an object’s behavior for suspicious events, and both Kirby and Mankins relate to behavioral approaches that monitor the actions of a computer program and compare the behavior to known suspect behavior (in Kirby) or to known “normal” or acceptable behavior (in Mankins). *Id.* Further, although Halperin focuses on identifying behavior matching predefined malicious behavior patterns, Halperin discloses that “[a]nother approach involves using . . . heuristic techniques to identify typical virus behavior by *characterizing legitimate software behavior* and then *identifying any deviation* from such behavior.” EX-1006, [0006]. A POSITA would have known that anomaly

detection was another useful way to detect and classify malware, and would have looked to systems like Mankins that detect deviations from legitimate software behavior. EX-1004 ¶171. And, for the reasons explained in Section IX.B.2, a POSITA would have been motivated to combine Kirby with Halperin.

As explained by Petitioners' expert, intrusion detection using sequences of system calls was known in the art as early as the mid-1990s. EX-1004 ¶173. Accordingly, incorporating Mankins's Bloom filter data object into Halperin's and Kirby's integrated approach to malware detection would have been nothing more than a predictable use of a prior-art element according to its established function. *KSR Int'l Corp. v. Teleflex, Inc.*, 550 U.S. 398, 417 (2007).

It would have been obvious to a POSITA to add Mankins's Bloom filter approach into Halperin and Kirby, and a POSITA would have recognized that Mankins's Bloom filter data object could be incorporated at either a remote computer or a base computer using the system architectures described in Halperin and Kirby. See EX-1007 at 4:11-20, Fig. 1; EX-1004 ¶174. For example, because each remote computer in Halperin's system monitors the "target behavior" of objects and sends it to a "central database," which "logs" the monitored behavior for comparison against predefined patterns, it would be an obvious modification to

collect system-call sequences as part of the data and compare them against a Bloom filter data object stored there. EX-1004 ¶174. Indeed, Mankins teaches that its “intrusion detection system 100 may be implemented *in a distributed fashion over a network of computing devices.*” EX-1008 at 4:29-30; *see also id.*, 4:50-52.

Alternatively, it would have been obvious to a POSITA that the combined system could log the sequence of system calls made by the object in the kernel and maintain the Bloom filter at each remote computer, as in the preferred embodiment in Mankins. EX-1004 ¶176. Mankins explains that because “the amount of memory required by a particular Bloom filter data object 180 (e.g., 3 KB) will be a small memory outlay,” it “may easily fit in the process structure of the OS kernel 120.” EX-1008 at 10:48-51. Kirby likewise teaches monitoring behavior locally at a remote computer. EX-1007 at 8:15-16 (“[T]he environment 100 includes one or more security agents 110 on a host computer 120.”).

In either implementation, if the system does not identify malware based on the behavioral data received from remote computers 500, Mankins’s process would begin. EX-1004, ¶177. Whether at each remote computer or in the base computer, the system would follow Mankins’ teaching to: (i) use the monitored behavior containing the “normal” system call patterns to generate a (or update an existing)

Bloom filter data object for that program; and (ii) monitor the behavior of the program (*e.g.*, by monitoring system-call sequences) and compare the behavior to the Bloom filter data object directly at the remote computer, or, alternatively, transmit the information for comparison against the Bloom filter data object stored at base computer. *Id.* ¶177.

Adding these additional steps from Mankins would optimize the system's ability to identify unknown malware, and, as explained by Dr. Newman, the benefits of this addition would not be offset by any cost. EX-1004, ¶178. Ultimately, a POSITA would have understood that the chosen configuration is an obvious matter of system design. *Id.*

3. Analysis

As stated above, Petitioners submit under Ground 1 that Halperin alone renders obvious independent claims 1 and 15 of the '389 patent. *See* IXA.2. Claim 14 depends from Claim 1 and further requires “initially classifying a computer object as not malware, generating a mask for said computer object that defines acceptable behaviour for the computer object, monitoring an operation of the computer object on at least one of the first and second remote computers and reclassifying the computer object as malware if the actual monitored behaviour extends beyond that

permitted by the mask.” As set forth below, Halperin in view of Kirby and in further view of Mankins renders this claim obvious. EX-1004 ¶179.

[14A]: initially classifying a computer object as not malware,

Kirby discloses “[i]f the pattern matcher concludes that a content based check against the baseline of previously stored realtime signatures in the signature database indicates a *benign transmission*, then the behavior monitor evaluates the actions performed by, on behalf of or as a result of the incoming transmission, based on the operations exhibited.” EX-1007 at 7:65-8:4. A POSITA would understand that by determining the object is benign, Kirby discloses classifying that object as not malware. EX-1004 ¶180.

[14B]: generating a mask for said computer object that defines acceptable behaviour for the computer object,

Mankins discloses [14B]. EX-1004 ¶181-82. Mankins “uses a Bloom filter to generate a Bloom filter data object containing data representative of normal system-call behavior” of a computer program. EX-1007 at 3:40–43. Mankins explains that the “predefined Bloom filter data is representative of ‘normal’ computer program behavior that is expected during operation of the computer programs when not subject to intrusion attempts.” *Id.* at 3:26–30. The “Bloom filter

data object 180 is built from the monitored behavior” of the computer object. A POSITA would know that Mankins’s “Bloom filter data object,” which is “representative of ‘normal’ computer program behavior” (Ex. 1006 at 3:40–43) is a “mask . . . that defines acceptable behaviour for the computer object.” EX-1004 ¶182.

[14C]: monitoring an operation of the computer object on at least one of the first and second remote computers and

Mankins discloses [14C]. EX-1004 ¶183. Mankins’s Figure 3, reproduced below, is a flowchart that illustrates “an example process for detecting intrusion attempts by monitoring system-call behavior”:

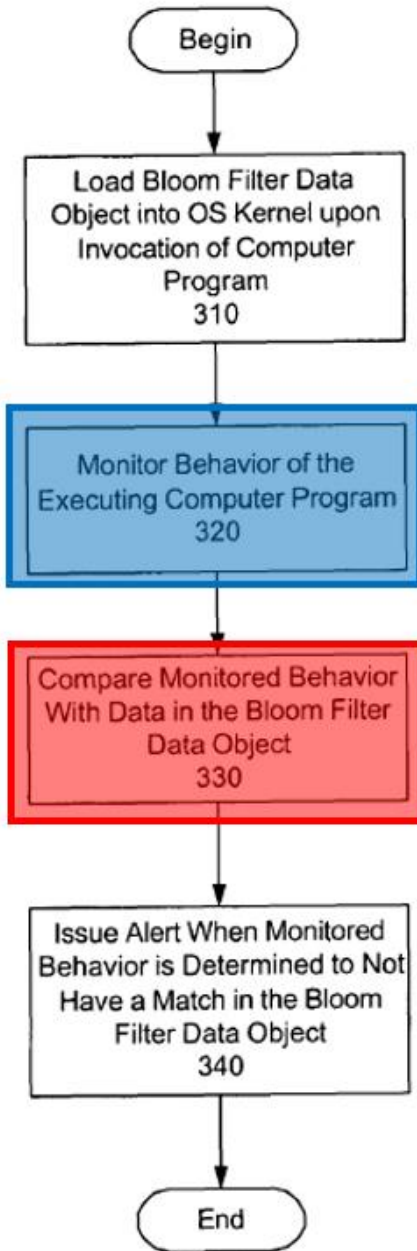


FIG. 3

Ex. 1008, 11:50–52, Fig. 3. At **step 320** of Figure 3, “behavior of the computer program is monitored as it is executed by the computer 110.” *Id.*, 11:63–65. At **step 330**, “the monitored behavior is compared with data in the Bloom filter data object,” which “may be performed by the monitoring subsystem 150, which may use the Bloom filter 175 to search the Bloom filter data object 180 to determine whether a match exists for any particular set of monitored behavior (e.g., a system-call sequence).” *Id.*, 12:1–6.

As explained above with respect to element [14B], it would have been obvious to a POSITA to incorporate the Mankins Bloom filter data object into the Kirby integrated malware-detection approach. EX-1004 ¶184. And, in such a combination, Kirby’s host computers 120 would monitor the behavior of an executing computer program (*i.e.*, step 320 of Mankins’s Figure 3) and compare the behavior with the Bloom filter data object associated with the monitored object to determine whether a match exists. *Id.*; *see also* EX-1008, 4:29–31 (“[T]he intrusion detection system 100 may be implemented in a distributed fashion over a network of computing devices.”).

[14D]: reclassifying the computer object as malware if the actual monitored behaviour extends beyond that permitted by the mask.

Mankins and Kirby disclose [14D]. In Mankins, “[a]t step 340, an alert is issued in response to a determination that the Bloom filter data object 180 does not contain a match for the monitor[ed] behavior.” EX-1008 at 12:11-9. A POSITA would have known that in case of a mismatch between monitored behavior and the Bloom filter data object, that means the behavior is beyond that allowed by the mask, and the system could monitor for mismatches. EX-1004 ¶187. And in Mankins, “[a]ny appropriate predefined action may be performed in response to the alert.” EX-1008 at 12:13-14. A POSITA would know that reclassifying the object as malware is an example of an “appropriate predefined action.” EX-1004 ¶187. As an example, Mankins states “the report subsystem 170 may be configured to automatically invoke predetermined actions designed to protect the computer 110 or to analyze the nature and/or source of the detected intrusion.” EX 1008 at 11:8-11. A POSITA would know that reclassifying an object as malware would be an action designed to protect the computer. EX-1004 ¶187.

Kirby classifies a computer object as not malware (specifically, “benign”) if the computer object passes the signature check. Kirby explains that the “signature

check . . . generally occurs immediately upon introduction of a new entity (e.g. file or object).” EX-1007 at 14:30-33. Kirby continues “the behavioral monitoring and prevention, which occurs as an ongoing monitoring effort.” EX-1007 at 14:30-33. The behavioral monitoring step is, therefore, performed after the computer object is classified as not malware (benign). EX-1004 ¶186. A combination of Mankins’s Bloom filter data object into Kirby would monitor a computer object that has passed the signature step (and thereby has been classified as not malware) using the Mankins Bloom filter. *Id.* As described above, when the behavioral monitoring step determines that the behavior is beyond the mask of the Mankins Bloom filter, it would reclassifies that computer object as malware. *Id.* ¶186.

Claim 28 is the apparatus version of Claim 14, and is therefore obvious over Halperin in view of Kirby and in further view of Mankins for the same reasons as Claim 14. EX-1004 ¶188.

X. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. PTAB Should Not Exercise Its Discretion to Deny Institution Under *Fintiv*

Consistent with congressional intent and the goals of *NHK/Fintiv*, Petitioners took all possible steps to promote the Board’s efficiency and fairness objectives. Petitioners initiated this petition with diligence, filed a single, focused petition, and

served a stipulation (EX-1009) identical to one the Board previously found mitigated concerns of duplicative efforts between the district court and the Board and potentially conflicting decisions. *Sand Revolution II, LLC v. Continental Intermodal Grp.*, IPR2019-01393, Paper 24 (June 16, 2020). These facts, along with the merits of Grounds 1-3, strongly favor institution.

1. Factor 1: Likelihood of Stay

Institution will enable the Board to resolve the issue of validity, and a finding of invalidity will relieve the District Court of the need to thereafter continue with the litigation. The District Court has made clear in prior cases that a motion to stay prior to institution of an IPR would be premature, and the Board recently “decline[d] to speculate on the likelihood of Judge Albright entering a stay after institution” and thus found Factor 1 neutral. *Western Digital Corp. v. Kuster*, IPR2020-01391, Paper 10 at 9 (Feb. 16, 2021); *see also Volkswagen Grp. of Am., Inc. v. Arigna Tech. Ltd.*, IPR2021-01321, Paper 10 at 3 (Feb. 15, 2022) (declining to speculate about the likelihood of a stay). Thus, this factor is at worst neutral.

2. Factor 2: District Court Schedule

The District Court schedule weighs in favor of institution. Pursuant to the District Court’s amended scheduling order on January 22, 2023 (Dkt. 160), the trial

*Petition for Inter Partes Review
of U.S. Patent No. 8,726,389*

in this case will not begin until August 19, 2024. EX-1013, 6. Based on an 18-month IPR schedule, even if the trial began exactly as currently projected, a Final Written Decision (“FWD”) arising from this petition would still be likely to issue before trial.

Even if that were not the case, uncertainty about the trial date and the high likelihood of further delay weigh against discretionary denial. In general, District Court patent-validity litigation schedules are uncertain. Indeed, the Board has held that this factor was “neutral” even in cases where the projected trial date was before the Board’s statutory final-decision deadline because it has recognized that projected trial dates are uncertain, especially when projected in the early stages of litigation. In *Cizion, LLC v. Kerr Machine Co.*, for instance, trial was set “three months prior to [the Board’s] (anticipated) deadline for a final written decision.” PGR2020-00065, Paper 10 at 26 (Dec. 3, 2020). The Board explained that “[a]lthough the current schedule [in *Cizion*] indicates that trial will commence a few months prior to the statutory due date to issue a final written decision in this proceeding, evidence in the record cited by the Petitioner does indicate that the actual trial date is uncertain.” *Id.*; see also *Micron Tech., Inc. v. Godo Kaisha IP Bridge 1*, IPR2020-01008, Paper 10 at 14 (Dec. 7, 2020) (“Accordingly, even if we consider the Texas

*Petition for Inter Partes Review
of U.S. Patent No. 8,726,389*

court to have set a formal trial date for a few months before the final written decision, due to the uncertainty as to this trial date, this factor is, at most, neutral to whether we should exercise our discretion to deny the Petition.”).

Of particular relevance here, the *Cizion* Board credited the Petitioner’s evidence that “in the Western District of Texas, 70% of trial dates have slipped following PTAB discretionary denials.” PGR2020-00065, Paper 10 at 26 (Dec. 3, 2020). The Board further noted that the evidence included “multiple proceedings with trial dates close to the” same trial date. *Id.* The same is true here, where the District Court has set a single trial date for five separate litigations with dozens of asserted patents. EX-1013.

Thus, the general uncertainty of District Court patent-validity actions, and the high likelihood that this litigation will extend beyond its projections, weighs in favor of institution. Indeed, recent Interim Guidance⁴ dictates that because scheduled trial dates “are unreliable and often change,” a scheduled trial date “is not by itself a good indicator of whether the district court trial will occur before the statutory deadline

⁴ https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf

for a [FWD].” *Samsung Elec. ’s Co., Ltd. v. Staton Techniya, LLC*, IPR2022-00302, Paper 13, 10 (PTAB July 11, 2022).

Finally, trial is more likely to get pushed further back in this case because the litigation is especially complex. Patent Owner originally asserted nine patents against five defendants, including the ’389 Patent, and recently moved to assert five more patents against Sophos Ltd. and other defendants. In granting Patent Owner’s motion to amend, the Court acknowledged that this case is “about as complicated as you’re going to get with patent cases” and said it would be “amenable to adjusting the schedule” by “granting more time to address things.” EX-1012, 2. Because this multi-defendant consolidated case is exceptionally complicated, it is unlikely that the District Court will dispose of the dispute over the ’389 Patent before a FWD would issue.

Thus this factor weighs strongly against discretionary denial.

3. Factor 3: Petitioners’ Investment in IPR Outweighs Forced Investment in Litigation to Date

Petitioners’ substantial investment in these IPR proceedings should counterbalance—if not outweigh—the resources invested in the co-pending litigation. It would be unjust to consider resources expended in the District Court

(equally by both parties), without considering Petitioners’ resources expended to prepare this IPR petition that would be irretrievably lost without consideration on the merits, in addition to the extensive expenses that may be foregone through institution of this petition and that will otherwise certainly follow in co-pending litigation for which significant milestones exist. *See, e.g., Apple v. Seven Networks*, IPR2020-00255, Paper 13 at 12–15 (July 28, 2020) (declining to exercise discretionary denial on petitions filed nine months after the commencement of co-pending litigation where a large number of patents were included in the litigation, and a large number of claims from each patent were challenged in the petitions).

In *Sand Revolution*, even after invalidity contentions and the *Markman* hearing, the Board found that this factor weighed “only marginally, if at all, in favor of exercising discretion.” *Sand Revolution*, IPR2019-01393, Paper 24 at 11. Given Petitioners’ diligence and significant investment in filing this petition, especially this early in the litigation, this factor should weigh against a discretionary denial.

4. Factor 4: The Petition Raises Unique Issues

Factor 4 strongly supports institution. Consistent with *Fintiv*, Petitioners ask the Board to consider the unique challenges raised in the petition. Petitioners have stipulated that, if the Board institutes the present petition, Petitioners will not assert

that the challenged claims are invalid on the instituted grounds in the related litigation, nor any other possible prior art printed publication grounds based on the references in Grounds 1–4. *Webroot, Inc. et al. v. Sophos Ltd.*, No. 6:22-cv-00240-ADA-DTG (W.D. Tex.). This stipulation is similar to the stipulation in *Sand Revolution* and therefore this factor strongly supports institution. *Sand Revolution*, Paper 24 at 11.

5. **Factor 5: Institution Will Provide the Board an Opportunity to Invalidate Claims That Later Could Be Reasserted Against Others**

In the District Court litigation, as noted above, Patent Owner has asserted 15 patents against five defendants. Of those 15 patents, five are asserted against all five defendants; five are asserted against four defendants; and the average patent is asserted against 3.6 defendants. In fact, Patent Owners asserted the '389 Patent against all other co-defendants. *See Forcepoint Action, CrowdStrike Action, Trend Micro Action, and Kaspersky Action.* In other words, Patent Owner has a demonstrated history of asserting claims against multiple defendants, and the Board has an opportunity to invalidate some of those claims here. Factor 5 weighs in favor of institution.

6. Factor 6: Other Circumstances Support Institution

As explained above, the merits of the unpatentability grounds are particularly strong, weighing in favor of institution. See *Fintiv*, at 14–15. And the effect on “the economy [and] the integrity of the patent system” further supports institution. PTAB Consolidated Trial Practice Guide, 56. The claims of the ’389 Patent are very broad and purport to cover receiving, determining, and storing information about potential malware, which was already disclosed several years prior to even the earliest priority date of the patent. The Board should consider and invalidate the claims such that they may not be asserted against other entities in the future.

B. PTAB Should Not Exercise its Discretion To Deny Institution Under *Becton* and *Advanced Bionics*

Institution should not be denied under the framework set forth in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (Dec. 15, 2017) (precedential as to § III.C.5, first paragraph) and *Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH*, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (precedential). Neither Halperin⁵, Kirby, nor Mankins was before the

⁵ This Petition presents U.S. Patent App. Pub. No. 2004/011632 to Halperin (“Halperin”), which was not mentioned by the patentee during prosecution, nor otherwise cited by the Examiner during prosecution. Halperin has a similar specification to an earlier-filed, abandoned U.S. Patent App. Pub. No. 2002/0194490

Examiner during prosecution. Therefore, the arguments presented in this Petition are not the same as, or substantially similar to, arguments previously presented to the Office. Thus, the first prong of the *Advanced Bionics* framework is not met.

to Halperin and Almogy (the “’490 Application”), which was cited in the final Information Disclosure Statement (“IDS”) submitted at the end of the prosecution of the ’389 Patent. However, review of the file history shows that the Examiner did not use the ’490 Application for any rejection or consider that application during prosecution. In fact, Patentee had not submitted the IDS citing the ’490 Application until after submitting its November 12, 2013 Request for Continued Examination and Arguments and Remarks made in response to the Examiner’s Final Rejection. The addition of the independent claims’ “correlation” step was included for the first time in the November 12 Amendment. The Examiner did not cite the ’490 Application or otherwise offer any substantive explanation of her decision to allow the claims over any prior art in her December 26, 2013 Notice of Allowability.

The citation of the ’490 Application in the final IDS is not sufficient for discretionary denial. The PTAB has held that “the mere listing of a reference...on an information disclosure statement...does not amount to substantive consideration of that reference by the Examiner.” *REG Synthetic Fuels, LLC v. Neste Oil, Oyj*, IPR2018-01375, 13 (PTAB February 19, 2019) (Paper 11) (collecting cases). See also *DJI Europe B.V. v. Textron Innovations, Inc.*, IPR2022-00453, 11–12 (PTAB August 3, 2022) (Paper 10) (instituting IPR that relied on prior art cited in an information disclosure statement, finding Examiner erred by failing to substantively consider that reference, where the Examiner did not use that reference for any rejections and the notice of allowability simply stated the prior art of record did not teach the claims without any substantive discussion of that reference); *Amperex Tech. Ltd. v. Maxell, Ltd.*, IPR2021-0142, 13–17 (PTAB April 12, 2022) (Paper 16) (instituting IPR that relied on prior art that was cited by the Examiner during prosecution); *Tianma Microelectronics Co. Ltd. v. Japan Display Inc., et al.*, IPR2021-01028, 15–17 (PTAB December 14, 2021) (Paper 14) (instituting IPR that relied on prior art cited by Examiner during prosecution).

And because the first prong is not met, there is no need to reach the second prong to resolve against discretionary denial under Section 325(d)—though in any event, there are no pending proceedings before the PTAB concerning the '389 Patent, so the second prong is not met either. *Oticon Medical AB v. Cochlear Ltd.*, IPR2019-00975 Paper 15, 20 (PTAB Oct. 16, 2019) (precedential).

XI. CONCLUSION

The cited prior art references in this Petition provide new, noncumulative technological teachings which indicate a reasonable likelihood of success as to Petitioners' assertion that the Challenged Claims of the '389 Patent are not patentable pursuant to the grounds presented in this Petition. Accordingly, Petitioners respectfully request that this Petition be granted, that *inter partes* review be instituted, and that claims 1-30 of the '389 Patent be found unpatentable and canceled.

XII. CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24, the undersigned attorney for the Petitioners declares that the argument section of this Petition (Sections I, III-XI) has a total of 13,914 words, according to the word count tool in Microsoft Word™.

*Petition for Inter Partes Review
of U.S. Patent No. 8,726,389*

Dated: March 3, 2023

Respectfully submitted,

/s/ Ryan Iwahashi

Ryan Iwahashi

(Reg. No. 63,378)

Gibson, Dunn & Crutcher LLP

1881 Page Mill Road

Palo Alto, CA 94304-1211

Tel: (650) 849-5367

RIwahashi@gibsondunn.com

CERTIFICATE OF SERVICE

The undersigned certifies service pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(a), (b) on the Patent Owner via FedEx overnight mail of a copy of this Petition for *Inter Partes* Review and supporting materials at the Patent Owner at the correspondence address of record for the '389 Patent:

Assignee:

Webroot Inc.
385 Interlocken Crescent
Suite 800
Broomfield, CO 80021

Counsel of Record:

Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN
United States

DATED: March 3, 2023

By: /s/ Ryan Iwahashi
Ryan Iwahashi
(Reg. No. 63,378)
Gibson, Dunn & Crutcher LLP
1881 Page Mill Road
Palo Alto, CA 94304-1211
Tel: (650) 849-5367
RIwahashi@gibsondunn.com