

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.,

Petitioner,

v.

TAASERA LICENSING LLC,

Patent Owner.

Patent No. 8,850,517

Filing Date: June 15, 2013

Issue Date: September 30, 2014

Inventor: Srinivas Kumar

Title: RUNTIME RISK DETECTION BASED ON USER, APPLICATION, AND
SYSTEM ACTION SEQUENCE CORRELATION

PATENT OWNER'S PRELIMINARY RESPONSE

Case No. IPR2023-00798

TABLE OF CONTENTS

	<u>Page(s)</u>
I. INTRODUCTION	1
II. THE '517 PATENT	2
III. THE ALLEGED PRIOR ART	6
A. Wright.....	6
B. Daswani	10
IV. CLAIM CONSTRUCTION	11
V. LEVEL OF ORDINARY SKILL IN THE ART	12
VI. PETITIONER HAS NOT DEMONSTRATED A REASONABLE LIKELIHOOD OF SUCCESS FOR THE GROUNDS ADVANCED IN THE PETITION, AND THE PETITION SHOULD BE DENIED	13
A. Claim 1 is Not Obvious Over Wright in Combination With Daswani	15
1. Wright in Combination with Daswani Does Not Disclose “storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence,” as Required by Claim 1	15
2. Wright in Combination with Daswani Does Not Disclose “storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules,” as Required by Claim 1	17
3. Wright in Combination with Daswani Does Not Disclose “identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application,” as Required by Claim 1	19

4.	Wright in Combination with Daswani Does Not Disclose “identifying, by a runtime monitor including a processing device, a behavior score for the application program that executes on the device based on the identified runtime risk,” as Required by Claim 1	20
B.	Claims 2-24 are Not Obvious Over Wright in Combination With Daswani	24
VII.	THE PETITION SHOULD BE DENIED IN THE DISCRETION OF THE DIRECTOR UNDER 35 U.S.C. § 314(A)	25
A.	The Parallel District Court Proceeding and the Petition Involve the Same Parties	26
B.	Proximity of The District Court’s Trial Date	27
C.	Significant Investment and Petitioner’s Delay in Filing the Petition.....	29
D.	No Stay of the Parallel District Court Litigation	29
E.	Other Factors Favor Discretionary Denial	31
VIII.	PETITIONER’S EXPERT DECLARATION SHOULD NOT BE CONSIDERED.....	ERROR! BOOKMARK NOT DEFINED.
IX.	THE BOARD SHOULD REJECT ANY LATE SOTERA STIPULATION	32
X.	CONCLUSION.....	33

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020)	25, 33
<i>Apple, Inc. v. Contentguard Holdings, Inc.</i> , IPR2015-00355, Decision Denying Institution of <i>Inter Partes</i> Review, Paper 9 at 9-10 (P.T.A.B. June 26, 2015)	13
<i>Broadcom Corp. v. Emulex Corp.</i> , 732 F.3d 1325 (Fed. Cir. 2013)	14
<i>Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.</i> , IPR2020-00122, Paper 15 (P.T.A.B. May 15, 2020)	27, 28
<i>Edward LifeSciences Corp. v. Evalve, Inc.</i> , IPR2019-01479, Paper 7 (P.T.A.B. Feb. 26, 2020).....	28
<i>Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha</i> , IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017).....	26
<i>Graham v. John Deere Co. of Kansas City</i> , 383 U.S. 1 (1966).....	13
<i>Innogenetics, N.V. v. Abbott Lab 'ys.</i> , 512 F.3d 1363 (Fed. Cir. 2008)	15
<i>Intell. Ventures II v. FedEx Corp.</i> , No. 2:16-cv-00980-JRG, Dkt. 141 (E.D. Tex. Oct. 24, 2017)	30, 31
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	14
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	13

<i>Lennon Image Techs., LLC v. Macy’s Retail Holdings, Inc.</i> , 2:13-CV-00235-JRG, 2014 WL 4652117 (E.D. Tex. Sept. 18, 2014)	30
<i>Los Angeles Biomedical Rsch. Inst. at Harbor-UCLA Med. Ctr. v. Eli Lilly & Co.</i> , 849 F.3d 1049 (Fed. Cir. 2017)	14
<i>Next Caller Inc. v. TrustID, Inc.</i> , IPR2019-00961, -00962, Paper 10, at 8-16 (P.T.A.B. Oct. 16, 2019)	28
<i>NHK Spring Co. v. Intri-Plex Techs., Inc.</i> , IPR2018-00752, Paper 8 (P.T.A.B. Sept. 12, 2018).....	26
<i>Pers. Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	14
<i>Samsung Elecs. Am., Inc. v. Uniloc 2017 LLC</i> , IPR2019-01218, Paper 7 (P.T.A.B. Jan. 7, 2020)	28
<i>Stratoflex, Inc. v. Aeroquip Corp.</i> , 713 F.2d 1530 (Fed. Cir. 1983)	13
<i>Supercell Oy v. Gree, Inc.</i> , IPR2020-00513, Paper 11 (P.T.A.B. June 24, 2020)	28
<i>Trend Micro, Inc., v. Taasera Licensing LLC</i> , IPR2023-00801, Paper 3 (P.T.A.B. April 27, 2023)	27
<i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG (E.D. Tex. Aug. 3, 2022).....	27, 28
<i>In re Van Os</i> , 844 F.3d 1359 (Fed. Cir. 2017)	14
Statutes	
35 U.S.C. § 314(a)	<i>passim</i>
35 U.S.C. § 314(b)(1).....	28
35 U.S.C. § 316(a)(11).....	28

Other Authorities

37 C.F.R. § 42.1(b)	32
---------------------------	----

LIST OF EXHIBITS

Exhibit No.	Description of Document
2001	Eighth Amended Docket Control Order, Dkt. 278, <i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG (E.D. Tex. Sept. 7, 2023)
2002	Defendants' Joint Patent L.R. 3-3 Invalidity Contentions and Subject Matter Ineligibility Contentions, <i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG, served March 28, 2023
2003	Joint Patent L.R. 4-5 Joint Claim Construction Chart, Dkt. No. 276-1, <i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG, filed September 1, 2023

I. INTRODUCTION

On April 5, 2023, Palo Alto Networks, Inc. (“Petitioner”) submitted a petition (Paper 2, “Petition” or “Pet.”) to institute *inter partes* review (“IPR”) of U.S. Patent No. 8,850,517 (Ex. 1001, “the ’517 Patent”), challenging claims 1-24 (the “Challenged Claims”). The Petition asserts that the Challenged Claims are obvious over U.S. Patent Publication No. 2011/0023115 A1 to Wright (Ex. 1005, “Wright”) in combination with U.S. Patent No. 8,806,647 to Daswani *et al.* (Ex. 1006, “Daswani”). Pet. at 2-3.

The Board should deny the Petition for at least two reasons: (1) the Petitioner fails to identify how certain elements of the Challenged Claims are obvious over Wright in combination with Daswani; and (2) the Board should exercise its discretion to deny the Petition under 35 U.S.C. § 314(a).

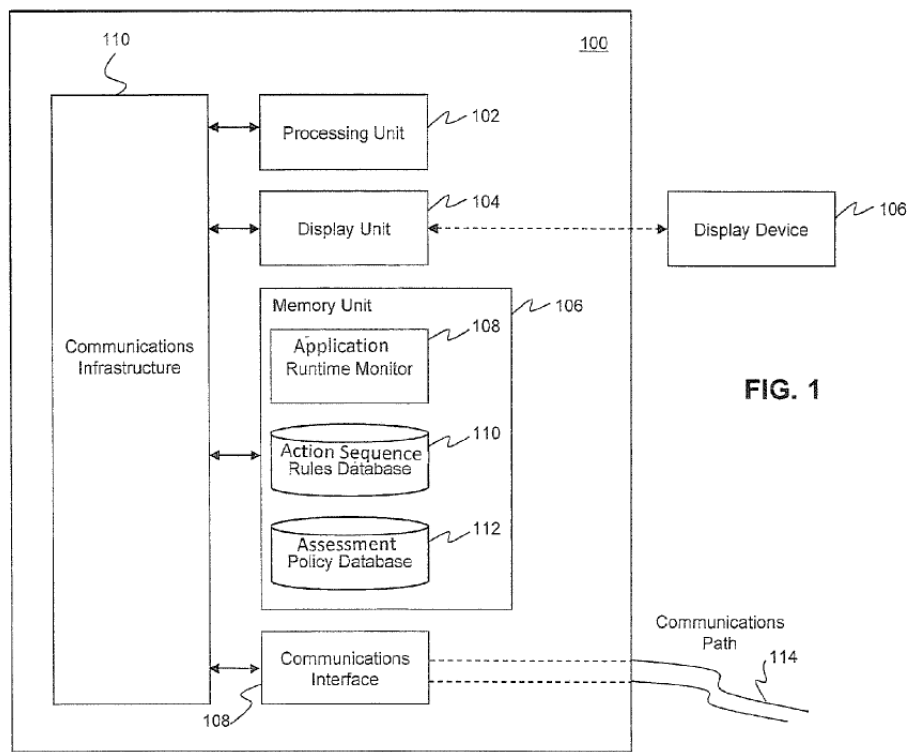
Wright is silent on rules that identify specific action sequences, as required by the claimed invention. Instead, Petitioner incorrectly conflates action sequences with rules, rendering the claim language redundant. Petitioner’s argument that Wright’s phenotype discloses the claimed “assessment policy” also fails because Wright’s phenotypes are simply collections of stored genes that do not perform any assessment of risk. Wright’s phenotypes also do not perform any assessment of risk because each phenotype is already predetermined to be associated with a known family of malware. Petitioner’s reliance on Wright in combination with Daswani to

show the claimed behavior score is similarly misguided because Petitioner's alleged disclosure of the behavior scores in each of Wright and Daswani exist prior to, and therefore cannot be based on, an identified runtime risk.

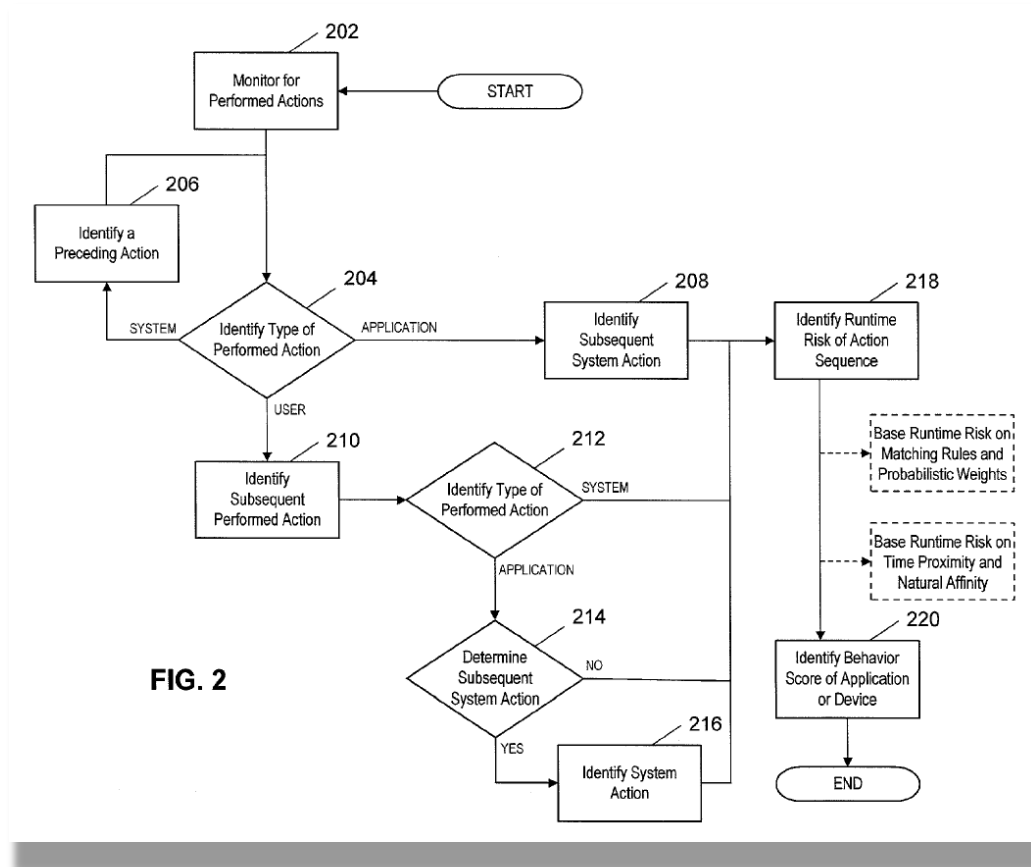
The Board should exercise its discretion to deny this Petition for at least the following reasons: (i) There exists a parallel District Court Litigation between the same parties or real-parties-in-interest; (ii) the District Court Litigation involves the same subject patent (the '517 Patent) with substantially the same claims; (iii) the District Court's trial will be almost *seven months before* the projected statutory deadline; (iv) the parties have heavily invested in the District Court proceeding since claim construction briefing is complete, fact discovery closes in approximately three months on November 6, 2023, and a trial date is set for April 15, 2024, which is only about seven months away; and (v) there is no stay of the parallel District Court Litigation.

II. THE '517 PATENT

The '517 Patent discloses and claims methods and systems “for assessing runtime risk for an application or device.” '517 Patent, Abstract. In particular, the methods and systems described in the '517 Patent identify an action sequence and assess a runtime risk and subsequent behavior score based on the identified action sequence, as shown in Figs. 1 and 2 reproduced below.



Id., Fig. 1.



Id. at Fig. 2.

The '517 Patent describes how assessing a runtime risk and subsequent behavior score based on an *identified action sequence* is an improvement over traditional methods and systems that evaluate individual actions or the application as a whole. An assessment based on an identified action sequence provides a greater level of scrutiny and accuracy and provides the added benefit of less processing:

The runtime monitor 108 may be further configured to identify the authenticity of the action sequence 308, such that an authentic action sequence may indicate that there is a forensic chain of events or a natural progression between the performed actions. In such an instance,

authenticating action sequences may enable the runtime monitor 108 to not consider action sequences that are purely circumstantial (e.g., where an application action 304 or system action 306 is not a result of the user action 302). ***This may result in more accurate scoring of behaviors and runtime risk, and also result in more efficient identification of runtime risks and behavior scores due to less processing required.***¹

Id. at 7:57-8:1.

The '517 Patent describes a relationship between rules, a rule database, policies, and a policy database in order to assess runtime risk based on at least one policy and provide the aforementioned benefit over traditional systems and methods:

The runtime risk may be identified using at least one assessment policy stored in the policy database 112. Each assessment policy may comprise one or more rules stored in the rules database 110 and may identify the runtime risk based on matching rules and probabilistic weights and scores.

Id. at 6:14-19.

The runtime monitor 108 may authenticate an action sequence 308 and determine the runtime risk using at least one assessment policy, which in turn includes at least one rule of the plurality of rules, based on the time proximity (e.g., as included in the action sequence) and natural affinity that may be logically inferred between the performed actions in the action sequence 308. For example, the modification of a file or a registry key value for the computing system 100 upon the opening of a document (e.g., PDF, Excel, PowerPoint, Word, etc.) attached to an e-mail without any user intervention may

¹ Emphasis added unless otherwise noted.

not be a natural progression for an action sequence, and
may therefore indicate a significant runtime risk.

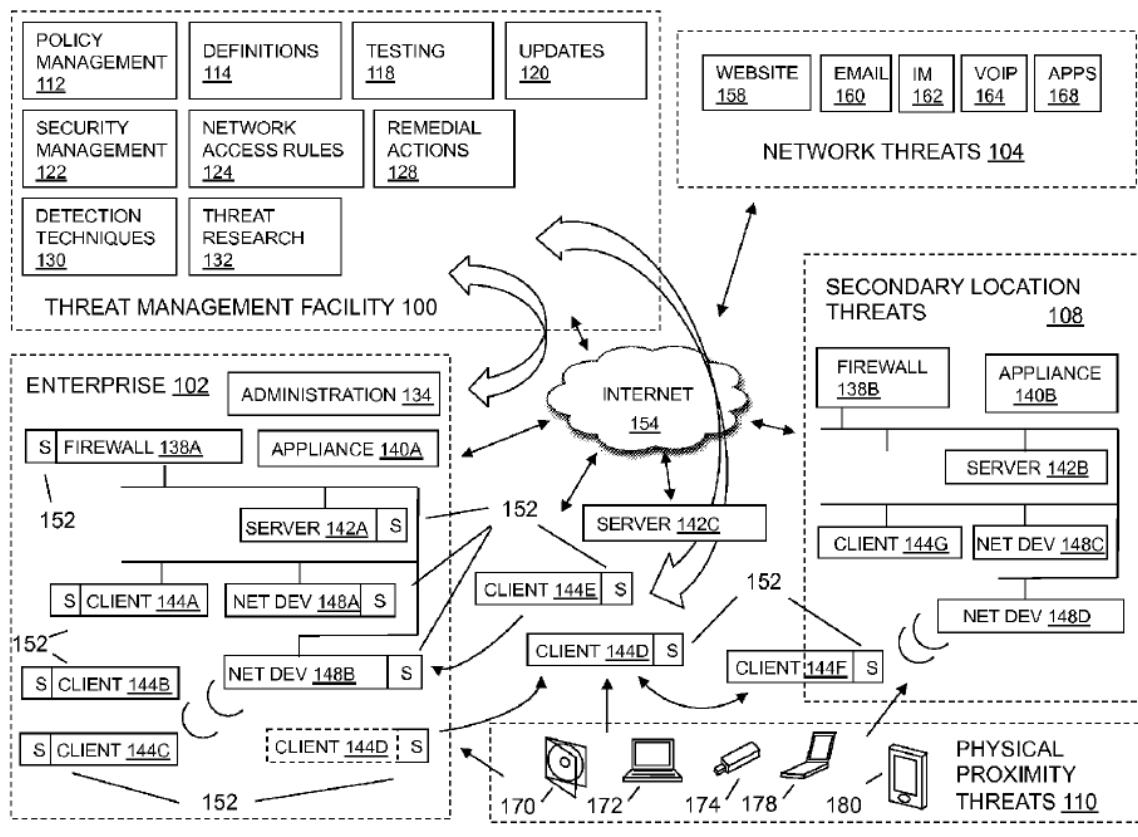
Id. at 8:10-12.

During prosecution, the claims of the '517 Patent were rejected over U.S. Patent App. Pub. No. 2013/0096980 to Basavapatna et al. ("Basavapatna"). Ex. 1002, 54-82, 106-128. The applicant was able to overcome this rejection by amending the claims to emphasize that "Basavapatna does not identify action sequences as part of the risk assessment, but instead uses countermeasures that have been deployed. Basavapatna also does not identify a risk or threat of the identified action sequence of the application, but instead assesses risk associated with known vulnerabilities." *Id.*, 140-141.

III. THE ALLEGED PRIOR ART

A. Wright

Wright is "related to behavioral-based threat detection." Ex. 1005, [0003]. Specifically, "[i]n embodiments of the present invention improved capabilities are described for threat detection using a behavioral-based host-intrusion prevention method and system for monitoring a user interaction with a computer, software application, operating system, graphic user interface, or some other component or client of a computer network, and performing an action to protect the computer network based at least in part on the user interaction and a computer code process executing during or in association with a computer usage session." *Id.*, Abstract.



Id. at Fig. 1.

Wright describes “rules” in the context of providing access permissions. For example, Wright discloses that:

[R]ules may provide a generic rule for the type of access that may be granted; the rules may be related to the policies of an enterprise facility 102 for access rights for the enterprise facility's 102 client facility 144. For example, there may be a rule that does not permit access to sporting websites.

Id., [0035].

Wright aggregates predetermined user behaviors or code behaviors in databases. *Id.*, [0007]-[0008] (“The indication of the user behavior may be a result of comparing the user interaction, or plurality of user interactions, with a predetermined behavior (hereinafter, a “behavioral gene”); “[T]he indication of the code operation may be a result of comparing on operation with a predetermined code behavior (hereinafter, a “code gene”)”).

Wright’s phenotypes are collections of stored genes that have some commonality:

A combination of one or more behavioral genes may be combined with one or more code genes and the combination compared to a predetermined collection of user behavior-code operation indications (“phenotypes”).

Id., [0008]. Each phenotype is already predetermined to be associated with a known family of malware:

A phenotype may be a predetermined collection of malicious behaviors which may include a grouping of specific genes that are typically present in a type or family of malicious code.

Id., [0069].

Wright discloses “policies” in the context of “access permissions associated with the network, applications, external computer devices, and the like:”

In an embodiment, a policy database may be a block list, a black list, an allowed list, a white list, or the like that may provide a list of enterprise facility 102 external network

locations/applications that may or may not be accessed by the client facility 144. The policy management facility 112 may include rules that may be interpreted with respect to an enterprise facility 102 network access request to determine if the request should be allowed.

Id., [0035].

Wright uses a behavior monitoring facility to “compar[e] a collection of observed user and code behaviors with the predetermined collections of known malicious user and code behaviors stored as phenotypes.” *Id.*, [0089].

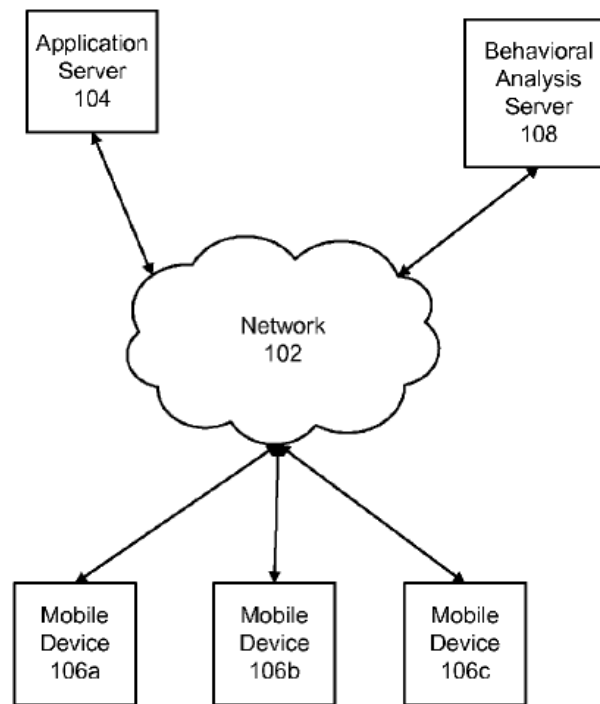
In the disclosure of Wright, behaviors comprising a phenotype are ranked ***prior to*** identifying “a known family of malware” (*i.e.*, determining a level of confidence that a known family of malware is being executed). *Id.*, [0069], [0169]. Wright describes that such behavior rankings are predetermined and the predetermined rankings are based on scaled analysis from a “threat research facility” or “threat management facility:”

Behavior-code ***phenotypes may capture a combination or a series of user and code behaviors that may be ranked*** to create increasing levels of confidence that the runtime object being monitored is executing a behavior pattern comparable to a known family of malware. The ***predetermined collections of behaviors, or phenotypes***, may be created based on suspicious or risky user behavior (e.g. downloading a file from a website, running an executable, opening a signed file with an unverifiable digital signature, or other potentially suspicious or risky behavior) and ***scaled analysis of families of malware in runtime, such as in a threat research facility 132 of a threat management facility 100.***

Id., [0089]. Therefore, Wright’s confidence level that a known family of malware is executed is based on Wright’s rankings of stored behaviors in a phenotype.

B. Daswani

Daswani “generally relates to the field of malware detection, in particular to detecting malware in computing applications.” Ex. 1006, 1:14-16. Daswani uses behavioral analysis of a mobile application that is performed to determine whether the application is malicious. *Id.* at Abstract.



Id., Fig. 1.

Daswani derives probabilities of maliciousness from an analysis module:

Similarly, analysis module 204 determines 504 observed soft signal behaviors and determines a probability of maliciousness for each of the soft signals.

Id., 8:14-16.

Daswani also describes that individual hard and soft signals have pre-existing probabilities of maliciousness *prior to* classifying an application as malicious:

In one embodiment, as previously discussed, individual hard signals have a probability of maliciousness high enough to classify the application as malicious. On the other hand, the probability of maliciousness for each of the observed soft signals is combined to calculate 506 a combined probability of maliciousness. If hard signal is observed, or if the combined probability of maliciousness exceeds a maliciousness threshold, the application is classified 508 as malicious. If no hard signal is observed, and if the combined probability of maliciousness fails to exceed the maliciousness threshold, the application is classified as non-malicious.

Id., 8:16-27.

IV. CLAIM CONSTRUCTION

For the purposes of this Preliminary Response only, Patent Owner believes that claim construction is not required to resolve any issues. While Petitioner notes that it believes that claim construction is not otherwise warranted, Patent Owner notes that both Petitioner and Patent Owner agreed to construe the term “runtime” in Claims 1, 10, 13, and 22 of the ’517 Patent as “the time the application is running.” *See* Pet. at 8; Ex. 2003 at 45-54. This, in addition to the plethora of other

outstanding issues that affect validity, weighs in favor of the Board using its discretion to deny institution of this Petition so that all validity issues could be resolved in the District Court Litigation.

V. LEVEL OF ORDINARY SKILL IN THE ART

For the purposes of this Preliminary Response only, Patent Owner utilizes Petitioner's proposed level of skill in the art: "a bachelor's degree in computer science, or a related field, or an equivalent technical degree or equivalent work experience, and an additional one or two years of education or experience in the field of computer security. More education can supplement practical experience and vice versa." Pet. at 7-8 (citations omitted).

**VI. PETITIONER HAS NOT DEMONSTRATED A REASONABLE
LIKELIHOOD OF SUCCESS FOR THE GROUNDS
ADVANCED IN THE PETITION, AND THE PETITION
SHOULD BE DENIED**

The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) so-called secondary considerations where in evidence. *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966); *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1537 (Fed. Cir. 1983).

The Board has held that a failure to identify the differences between the claimed subject matter and the prior art is fatal to an obviousness challenge. *See, Apple, Inc. v. Contentguard Holdings, Inc.*, IPR2015-00355, Decision Denying Institution of *Inter Partes* Review, Paper 9 at 9-10 (P.T.A.B. June 26, 2015) (denying institution for failure to identify the differences between the claimed subject matter and the prior art).

In arriving at an obviousness determination, the Board must sufficiently explain and support the conclusions that the prior-art references disclose all the

elements recited in the Challenged Claims and a relevant, skilled artisan not only could have made, but would have been motivated to combine all the prior art references in the way the patent claims and reasonably expected success. *Pers. Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017). That is, even if all the claim elements are found across a number of references, an obviousness determination must consider whether a person of ordinary skill in the art would have the motivation to combine those references. *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1368 (Fed. Cir. 2016); *Los Angeles Biomedical Rsch. Inst. at Harbor-UCLA Med. Ctr. v. Eli Lilly & Co.*, 849 F.3d 1049, 1067 (Fed. Cir. 2017) (vacating and remanding an obviousness determination, in part, because the Board did not make factual finding as to whether there was an apparent reason to combine all three prior art references to achieve the claimed invention and whether a person of skill in the art would have had a reasonable expectation of success from such a combination). This combinability determination, as supported by an articulated motivation to combine, requires a plausible rationale as to why those prior art references would have worked together. *Broadcom Corp. v. Emulex Corp.*, 732 F.3d 1325, 1335 (Fed. Cir. 2013). Absent some articulated rationale, a “common sense” finding is no different than the conclusory statement “would have been obvious.” *In re Van Os*, 844 F.3d 1359, 1361 (Fed. Cir. 2017). Of additional importance, “knowledge of a problem and motivation to solve it are entirely different

from motivation to combine particular references. . . .” *Innogenetics, N.V. v. Abbott Lab’ys.*, 512 F.3d 1363, 1373 (Fed. Cir. 2008).

A. Claim 1 is Not Obvious Over Wright in Combination With Daswani

1. Wright in Combination with Daswani Does Not Disclose “storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence,” as Required by Claim 1

Claim 1 of the ’517 Patent recites “storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence.” Wright does not render this claim limitation obvious, as Petitioner incorrectly asserts. Pet. at 18-25.

Wright fails to disclose the claimed “plurality of rules, wherein each rule identifies an action sequence.” Wright only mentions “rules” in the context of providing access permissions. For example, Wright discloses that:

[R]ules may provide a generic rule for the type of access that may be granted; the rules may be related to the policies of an enterprise facility 102 for access rights for the enterprise facility's 102 client facility 144. For example, there may be a rule that does not permit access to sporting websites.

Ex. 1005, [0035]. None of Wright’s rules identify an action sequence.

Because Wright does not disclose the claimed “rules, wherein each rule identifies an action sequence,” Wright also cannot disclose “storing, in a rules database, a plurality of rules.” The entries of Wright’s disclosed databases are user

behavior and code behavior genes, which are, at most, actions or events because Wright's databases aggregate predetermined user behaviors or code behaviors. Ex. 1005, [0007]-[0008] ("The indication of the user behavior may be a result of comparing the user interaction, or plurality of user interactions, with a predetermined behavior (hereinafter, a "behavioral gene")"; "[T]he indication of the code operation may be a result of comparing on operation with a predetermined code behavior (hereinafter, a "code gene)"). Petitioner fails to show how Wright's databases are rules databases when the entries are behaviors instead of rules that identify action sequences, as required by the claim.

As a result of interpreting the entries of Wright's "gene"/ behavior database as the claimed "rules," Petitioner improperly conflates Wright's "genes" with both the claimed "action sequences" and the claimed "rules." First, Petitioner argues that "Wright's user interactions (behavior genes) and code actions (code genes) encompass user actions, application actions, and system actions . . . A PHOSITA would understand these example actions correspond to the 'action sequences' recited." Pet. at 20. Second, Petitioner argues that "Wright discloses storing behavioral genes ('rules') in a code gene database and behavior gene database ('storing in a rules database'). Pet. at 22. By claiming that behavioral genes are both the claimed action sequences and the claimed rules, Petitioner effectively argues that

rules are action sequences and renders the claim language that “each rule identifies an action sequence” redundant because an action sequence cannot identify itself.

Petitioner fails to show that Wright in combination with Daswani renders this limitation obvious.

2. Wright in Combination with Daswani Does Not Disclose “storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules,” as Required by Claim 1

Claim 1 of the ’517 Patent recites “storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules.” Wright in combination with Daswani does not render this claim limitation obvious, as Petitioner asserts. Pet. at 25-27.

Since Petitioner fails to show how Wright discloses, teaches, or suggests “a rules database, a plurality of rules, wherein each rule identifies an action sequence,” it cannot now disclose, teach, or suggest “wherein each assessment policy includes at least one rule of the plurality of rules.” *See supra* Section VI.A.1.

Petitioner alleges that the claimed policy database is disclosed by Wright’s “phenotype database.” Pet. at 26. But Wright’s phenotypes are simply collections of stored genes that have some commonality. Ex. 1005, [0069]. As a mere collection of behaviors, each phenotype cannot be an assessment policy because a collection of behaviors (*i.e.*, phenotype) cannot perform an assessment of risk, let alone “a

runtime risk” as the subsequent claim limitation requires (“identifying, using at least one assessment policy, a runtime risk for an application program”):

A combination of one or more behavioral genes may be combined with one or more code genes and the combination compared to a *predetermined collection of user behavior-code operation indications* (“phenotypes”).

Ex. 1005, [0008]. Wright’s phenotypes do not perform any assessment of *runtime* risk because each phenotype is already *predetermined* to be associated with a known family of malware:

A phenotype may be a predetermined collection of malicious behaviors which may include a grouping of specific genes that are typically present in a type or family of malicious code.

Id., [0069].

Further, Wright only mentions “policies” in the context of “access permissions associated with the network, applications, external computer devices, and the like.”

In an embodiment, a policy database may be a block list, a black list, an allowed list, a white list, or the like that may provide a list of enterprise facility 102 external network locations/applications that may or may not be accessed by the client facility 144. The policy management facility 112 may include rules that may be interpreted with respect to an enterprise facility 102 network access request to determine if the request should be allowed.

Id., [0035]. Wright’s policies are not related to the claimed runtime risk assessment policies, and, therefore, Petitioner cannot meet its burden to show “storing, in a policy database, a plurality of assessment policies.”

Therefore, Petitioner fails to show that Wright in combination with Daswani renders this limitation obvious.

3. Wright in Combination with Daswani Does Not Disclose “identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application,” as Required by Claim 1

Claim 1 of the ’517 Patent recites “identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application.” Wright in combination with Daswani does not render this claim limitation obvious, as Petitioner asserts. Pet. at 28-31.

Since Petitioner fails to show how Wright discloses, teaches, or suggests “a plurality of assessment policies, wherein each assessment policy includes at least one rule,” it cannot now disclose, teach, or suggest “identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device.” *See supra* Section VI.A.2.

The language of this claim limitation recites “identifying, using at least one assessment policy, a runtime risk.” Even assuming that Wright’s phenotypes were the claimed policies, Petitioner’s own cited portions of Wright indicate that Wright’s phenotypes do not identify the runtime risk, as the claim limitation requires. Wright uses a behavior monitoring facility (*i.e.*, not a phenotype) to “compar[e] a collection of observed user and code behaviors with the predetermined collections of known malicious user and code behaviors stored as phenotypes.” Pet. at 30 (citing Ex. 1005, [0089]).

In contrast, the ’517 Patent describes that runtime risk can be identified based on matching multiple rules associated with a given policy.

The runtime risk may be identified using at least one assessment policy stored in the policy database 112. Each assessment policy may comprise one or more rules stored in the rules database 110 and may identify the runtime risk based on matching rules and probabilistic weights and scores.

’517 Patent, 6:14-19. As noted above and by Petitioner, Wright only uses comparisons of previously stored actions to runtime behaviors to determine threats or malware. Wright does not use policies that utilize rules to assess runtime risk.

Therefore, Petitioner fails to show that Wright in combination with Daswani renders this limitation obvious.

4. Wright in Combination with Daswani Does Not Disclose “identifying, by a runtime monitor including a processing

device, a behavior score for the application program that executes on the device based on the identified runtime risk,” as Required by Claim 1

Claim 1 of the '517 Patent recites “identifying, by a runtime monitor including a processing device, a behavior score for the application program that executes on the device based on the identified runtime risk.” Wright in combination with Daswani does not render this claim limitation obvious, as Petitioner asserts. Pet. at 31-36.

Since Petitioner fails to show how Wright discloses, teaches, or suggests “identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application,” it cannot now disclose, teach, or suggest “a behavior score for the application program that executes on the device based on the identified runtime risk.” *See supra* Section VI.A.3.

Petitioner incorrectly argues that “ranking of captured user and code behaviors is equivalent to the ‘behavior score’” but fails to describe how Wright’s rankings are based on “the identified runtime risk,” which Petitioner alleged is Wright’s “identification of a known family of malware.” Pet. at 31, 33-34. Nowhere does Petitioner argue that Wright’s “rankings” are *based on* Wright’s “identification of a known family of malware.” Petitioner admits that behaviors comprising a

phenotype are ranked *prior to* identifying “a known family of malware” (*i.e.*, determining a level of confidence that a known family of malware is being executed). Pet. at 33-34 (citing Ex. 1005, [0069], [0169]). Wright confirms that such behavior rankings are predetermined because the phenotypes comprising the ranked behaviors are predetermined, and the predetermined rankings are based on scaled analysis from a “threat research facility” or “threat management facility:”

Behavior-code *phenotypes may capture a combination or a series of user and code behaviors that may be ranked* to create increasing levels of confidence that the runtime object being monitored is executing a behavior pattern comparable to a known family of malware. The *predetermined collections of behaviors, or phenotypes*, may be created based on suspicious or risky user behavior (e.g. downloading a file from a website, running an executable, opening a signed file with an unverifiable digital signature, or other potentially suspicious or risky behavior) and *scaled analysis of families of malware in runtime, such as in a threat research facility 132 of a threat management facility 100*.

Ex. 1005, [0089] (emphasis added). Since Wright’s predetermined rankings are only based on scaled analyses from threat research facilities or threat management facilities, the rankings cannot be *based on* “identification of a known family of malware,” as Petitioner incorrectly asserts. The inverse is true because Wright’s identification of a known family of malware (*i.e.*, confidence level that a known family of malware is executed) is based on Wright’s rankings of stored behaviors in a phenotype.

Wright in view of Daswani also does not render this claim limitation obvious because Petitioner does not provide a coherent motivation to combine Wright with Daswani. As noted above, Petitioner argued that the claimed “identified runtime risk” is disclosed by Wright’s “identification of a known family of malware.” Pet. at 31. Petitioner relies on Daswani’s “calculated probability of maliciousness to be a ‘behavior score.’” Pet. at 36. The claim limitation requires “identifying...a behavior score based on the identified runtime risk” but Petitioner does not explain how a PHOSITA would identify Daswani’s “calculated probability of maliciousness” *based on* Wright’s “identification of a known family of malware.” Petitioner’s cited portions of Daswani are clear that probabilities of maliciousness are derived from an analysis module, and not from the claimed “identified runtime risk”:

Similarly, analysis module 204 determines 504 observed soft signal behaviors and determines a probability of maliciousness for each of the soft signals.

Ex. 1006, 8:14-16.

Similarly, Daswani describes that individual hard and soft signals have pre-existing probabilities of maliciousness *prior to* classifying an application as malicious, which precludes them from being “based on the identified runtime risk.”

In one embodiment, as previously discussed, individual hard signals have a probability of maliciousness high enough to classify the application as malicious. On the other hand, the probability of maliciousness for each of the observed soft signals is combined to calculate 506 a

combined probability of maliciousness. If hard signal is observed, or if the combined probability of maliciousness exceeds a maliciousness threshold, the application is classified 508 as malicious. If no hard signal is observed, and if the combined probability of maliciousness fails to exceed the maliciousness threshold, the application is classified as non-malicious.

Id., 8:13-27. Based on the pre-existence of Daswani's probabilities of maliciousness to identifying a family of malware, the combination of Wright and Daswani could not yield a scenario where Daswani's probabilities of maliciousness are ***based on*** Wright's "identification of a known family of malware" (*i.e.*, Petitioner's alleged runtime risk).

Therefore, Petitioner fails to show that Wright in combination with Daswani renders this limitation obvious.

B. Claims 2-24 are Not Obvious Over Wright in Combination With Daswani

Claims 2-12 depend from Claim 1. Therefore, Claims 2-12 are not obvious over Wright in combination with Daswani, for at least the same reasons as Claim 1.

Claims 13-24 are the system claim analogues to the method claims of Claims 1-12. Therefore, Claims 13-24 are not obvious over Wright in combination with Daswani, for at least the same reasons as Claims 1-12, respectively.

VII. THE PETITION SHOULD BE DENIED IN THE DISCRETION OF THE DIRECTOR UNDER 35 U.S.C. § 314(A)

Based on Petitioner's reasons regarding § 314(a), the Board should exercise its discretion to deny this Petition.

The circumstances of the parallel District Court Litigation necessitate denial of the Petition under the Board's precedent, as every factor considered in relation to efficiency, fairness, and the merits supports denial. *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11, at 6 (P.T.A.B. Mar. 20, 2020) (precedential) (considering (a) "whether the petitioner and the defendant in the parallel proceeding are the same party"; (b) "overlap between issues raised in the petition and in the parallel proceeding" (c) "proximity of the court's trial date to the Board's projected statutory deadline for a final written decision"; (d) "investment in the parallel proceeding by the court and the parties"; (e) "whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted"; and (f) "other circumstances that impact the Board's exercise of discretion, including the merits.")).

As set forth below, these factors collectively demonstrate that efficiency and integrity of the AIA are best served by denying review. First, the Petitioner is the Defendant in the parallel proceeding. *See infra* Section VII.A. Second, the asserted claims in the District Court Litigation are all at issue in the Petition, and Petitioner has raised substantially similar, if not identical, arguments for invalidity in the

District Court Litigation. *See infra* Section II.B. Third, trial in the District Court Litigation is set for April 15, 2024, eight months earlier than the projected statutory deadline for a final written decision of this Petition in December 16, 2024. *See infra* Section VII.C. Fourth, the parties (and Patent Owner in particular) have invested significant resources on developing legal and factual issues of validity and infringement in the District Court Litigation and will have invested substantially more resources before any decision on this Petition. *See infra* Section VII.D. Fifth, the Court has neither granted nor denied a stay pending this Petition. *See infra* Section VII.E. Finally, no other factors favor institution. *See infra* Section VII.F.

Accordingly, the Board should exercise its discretion under § 314(a) and deny the Petition because institution of this proceeding would not be consistent with the objective of the AIA to “provide an effective and efficient alternative to District Court litigation.” *NHK Spring Co. v. Intrix-Plex Techs., Inc.*, IPR2018-00752, Paper 8, at 20 (P.T.A.B. Sept. 12, 2018) (quoting *Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19, at 16–17 (P.T.A.B. Sept. 6, 2017) (precedential)).

**A. The Parallel District Court Proceeding and the Petition
Involve the Same Parties**

As noted in Patent Owner’s Mandatory Notice, there exists a parallel District Court Litigation between the same parties regarding the same subject patent (the

'517 Patent). *Trend Micro, Inc., v. Taasera Licensing LLC*, IPR2023-00798, Paper 3 at 2-3 (P.T.A.B. April 26, 2023); Pet. at 69. Petitioner is a party to the District Court Litigation captioned as *In re: Taasera Licensing LLC, Patent Litigation*, No. 2:22-md-03042-JRG (E.D. Tex. Aug. 3, 2022) (the "District Court Litigation"). Accordingly, this factor weighs in favor of discretionary denial.

B. The District Court Litigation Involves Substantially the Same Claims

The asserted claims in the District Court Litigation are all at issue in the Petition, since this Petition involves all of the '517 Patent's claims. "In at least these ways, the parallel proceedings would duplicate effort. This is an inefficient use of Board, party, and judicial resources and raises the possibility of conflicting decisions." *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15 at 10 (P.T.A.B. May 15, 2020). Accordingly, this fact weighs in favor of discretionary denial.

C. Proximity of The District Court's Trial Date

The proximity of the District Court Litigation's trial date to the Board's projected statutory deadline for a final written decision strongly weighs in favor of discretionary denial.

The parties' trial is scheduled for April 15, 2024. Exhibit 2001 (Eighth Amended Docket Control Order, Dkt. 278, *In re: Taasera Licensing LLC, Patent*

Litigation, No. 2:22-md-03042-JRG (E.D. Tex. September 7, 2023)). Pursuant to 35 U.S.C. §§ 314(b)(1) and 316(a)(11), the projected statutory deadline for a final written decision of this Petition is December 16, 2024.² As the District Court’s trial will be almost *eight months before* the projected statutory deadline, this factor weighs strongly in favor of denying institution. *See Supercell Oy v. Gree, Inc.*, IPR2020-00513, Paper 11 at 10-12 (P.T.A.B. June 24, 2020) (denying institution where the jury trial was scheduled to conclude approximately ten months before the statutory deadline); *Edward LifeSciences Corp. v. Evalve, Inc.*, IPR2019-01479, Paper 7, at 6-13 (P.T.A.B. Feb. 26, 2020) (denying institution where jury trial would conclude more than nine months before a final decision would be due); *Samsung Elecs. Am., Inc. v. Uniloc 2017 LLC*, IPR2019-01218, Paper 7, at 7-10 (P.T.A.B. Jan. 7, 2020) (denying institution where jury selection was scheduled for approximately six months before trial in the Board proceeding would conclude); *Next Caller Inc. v. TrustID, Inc.*, IPR2019-00961, -00962, Paper 10, at 8-16 (P.T.A.B. Oct. 16, 2019) (denying institution where trial was scheduled to conclude “several months,” before a final decision would be due); *Cisco Sys., Inc.*, IPR2020-

² The statutory deadline for institution is December 14, 2023, “three months after receiving a preliminary response to the petition under section 313.” *See* 35 U.S.C. § 314(b)(1). If instituted, the statutory deadline for final written decision is December 16, 2024, “not later than 1 year after the date on which the Director notices the institution of a review,” because December 14, 2024 falls on a Saturday.

00122, Paper 15 at 8 (“Because the trial date is substantially earlier than the projected statutory deadline for the Board’s final decision, this factor weighs in favor of discretionary denial.”).

Petitioner does not contest that the proximity of the trial favors denial of institution. Thus, this factor also weighs in favor of discretionary denial.

D. Significant Investment and Petitioner’s Delay in Filing the Petition

The parties’ investment in the parallel proceeding weighs in favor of discretionary denial.

In the District Court Litigation, the Court has already entered nine Docket Control Orders (Dkts. 8, 15, 46, 84, 209, 225, 239, 257, 278), Discovery Order (Dkt. 137), Protective Order (Dkt. 162), and E-Discovery Order (Dkt. 195). Discovery is also well under way. The parties have already exchanged claim construction briefing, infringement contentions pursuant to P.R. 3-1, and invalidity contentions pursuant to P.R. 3-3, fact discovery closes in less than three months on November 6, 2023, and a trial date is set for April 15, 2024, which is less than seven months away. Ex. 2001.

Thus, the parties’ and Court’s substantial investment in this proceeding weighs in favor of denial of institution under this factor.

E. No Stay of the Parallel District Court Litigation

There is no stay of the parallel District Court Litigation. Even if the Petition was instituted and Petitioner filed a motion to stay the District Court Litigation, prejudice, tactical disadvantage to Taasera, the late stage of the litigation, and the lack of potential simplification would weigh strongly against such a motion. *See Lennon Image Techs., LLC v. Macy's Retail Holdings, Inc.*, 2:13-CV-00235-JRG, 2014 WL 4652117, at *1 (E.D. Tex. Sept. 18, 2014). The statutory deadline for institution is not until after the district court's claim construction hearing and the deadline to complete fact discovery,³ placing any motion for a stay close to trial. Ex. 2001; *see Intell. Ventures II v. FedEx Corp.*, No. 2:16-cv-00980-JRG, Dkt. 141 at 5 (E.D. Tex. Oct. 24, 2017) ("The Court agrees that the Parties have already invested substantial effort and resources during discovery and in preparing claim construction briefing. . . . These circumstances weigh against staying this case").

Moreover, a stay would not decrease the burden on the Court and the parties since any instituted IPR would not cover any of the eleven references that Petitioner raised in the District Court Litigation for both anticipation and at least 12 combinations of obviousness that each include 12 references, and not include Petitioner's challenges under § 112 or § 101. Ex. 2002, at 82, 144-165, 371-374,

³ As noted above, the statutory deadline for institution is December 14, 2023. *See supra* n. 5. Per Ex. 2001, the claim construction hearing is October 11, 2023, and the deadline to complete fact discovery is November 6, 2023.

421-430. *Intell. Ventures II*, No. 2:16-cv-00980-JRG, Dkt. 141 at 3-4 (“[T]he instituted IPRs only cover a narrow slice of the invalidity arguments Defendants have raised in this case. For example, Defendants have argued that the ’715 Patent is invalid under § 102 with respect to at least eight references . . . under § 103 with respect to at least twenty-six combinations . . . under § 112 [], and under § 101.”).

Accordingly, it would be unlikely for the Court to hold that a stay would streamline the litigation and this factor supports denial of institution.

F. Other Factors Favor Discretionary Denial

Petitioner does not present a strong case on the merits, further supporting denial of institution. *See supra* Section VI. Petitioner also does not identify any other factors which weigh against discretionary denial. Pet. at 66-68.

Thus, when viewing the factors together, the Petition should be denied in the Director’s discretion under 35 U.S.C. § 314(a).

VIII. THE BOARD SHOULD REJECT ANY LATE SOTERA STIPULATION

Petitioner has not made a *Sotera*-style stipulation that “if IPR is instituted, [Petitioner] will not pursue in the District Court Litigation any ground raised or that could have been reasonably raised in an IPR” in its Petition, which weighs further in favor of discretionarily denying institution. *See Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12, 13-14 (P.T.A.B. Dec. 1, 2020) (designated Dec. 17, 2020).

The Board should not accept any late *Sotera* stipulation after this Patent Owner Preliminary Response. Petitioner has known about the related District Court Litigation since Patent Owner filed a complaint asserting infringement of the ’517 patent against Trend Micro Incorporated (November 30, 2021) approximately 16 months before this Petition (April 5, 2023), and has had several docket control orders for the District Court Litigation, which originally anticipated a trial date for October 30, 2023. Docket Control Order, Dkt. 17, *Taasera Licensing LLC v. Trend Micro Incorporated*, No. 2:21-cv-00441-JRG (E.D. Tex. August 3, 2022). Any withholding of the *Sotera* stipulation in its Petition is gamesmanship and prejudicial to Patent Owner in this proceeding, and is inconsistent with 37 C.F.R. § 42.1(b)’s mandate to “secure the just, speedy, and inexpensive resolution of every proceeding.”

Both the Board and Director are abundantly clear that Petitioner cannot wait until after the Board renders its Institution Decision to address the issue of *Fintiv*, the Board’s discretionary authority, and to submit a *Sotera* stipulation. *NXP USA, Inc. v Impinj, Inc.*, IPR2021-01556, Paper 12, 5-6 (P.T.A.B. Aug. 25, 2022); *see also id.*, IPR2021-01556, Paper 13, 3-4 (P.T.A.B. Sept. 7, 2022) (the Director finding “that the Board correctly determined that a stipulation, offered by a petitioner for the first time after a decision denying institution, is not a proper basis for granting rehearing of the decision on institution;” “[p]ermitting a petitioner to wait and see if the Board denies institution under *Fintiv*, and then offer such a stipulation for the first time on rehearing, frustrates these goals [of avoiding conflicting decisions] and would open the door to gamesmanship;” “***the only appropriate time for a petitioner to offer a stipulation related to the Fintiv factor 4 analysis is prior to the Board’s decision of whether to institute review.***”).

IX. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests that the Board deny institution of the Petition in its entirety.

Respectfully submitted,

Dated: September 14, 2023

/ Peter Lambrianakos /
Peter Lambrianakos (Reg. No. 58,279)
Lead Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax. 212-257-5517
Email: plambrianakos@fabricantllp.com

Vincent J. Rubino, III (Reg. No. 68,594)
Alfred R. Fabricant (subject to motion to
appear *pro hac vice*)
Joseph M. Mercadante (Reg. No. 64,077)
Backup Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax.: 212-257-5517
Email: vrubino@fabricantllp.com
Email: ffabricant@fabricantllp.com
Email: jmercadante@fabricantllp.com

CERTIFICATE OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned PATENT OWNER'S PRELIMINARY RESPONSE specified in 37 C.F.R. § 42.24 has 7743 words in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24. This word count was prepared using Microsoft Word for Office 365.

Respectfully Submitted,

September 14, 2023

By: / Peter Lambrianakos /
Peter Lambrianakos (Reg. No. 58,279)
Lead Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax. 212-257-5517

CERTIFICATE OF SERVICE

A copy of PATENT OWNER'S PRELIMINARY RESPONSE and EXHIBITS 2001 through 2003 have been served on Petitioner's counsel of record as follows:

Robert M. Hansen
Email: rhansen@marburylaw.com
Matthew J. Anderson
Email: manderson@marburylaw.com
Scott B. Amankwatia
Email: samankwatia@marburylaw.com
THE MARBURY LAW GROUP, PLLC
11800 Sunrise Valley Drive, 15th Floor
Reston, VA 20191

Attorneys for Trend Micro Inc.

September 14, 2023

By: / Peter Lambrianakos /
Peter Lambrianakos (Reg. No. 58,279)
Lead Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax. 212-257-5517