

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. 8,327,441

Filing Date: February 17, 2012

Issue Date: December 4, 2012

Inventors: Srinivas Kumar and Gurudatt Shashikumar

Title: SYSTEM AND METHOD FOR APPLICATION ATTESTATION

PATENT OWNER'S PRELIMINARY RESPONSE

Case No. IPR2023-00801

TABLE OF CONTENTS

	<u>Page(s)</u>
I. INTRODUCTION	1
II. THE '441 PATENT	3
III. THE ALLEGED PRIOR ART	5
A. Munetoh.....	5
B. Rajan.....	7
IV. CLAIM CONSTRUCTION	9
V. LEVEL OF ORDINARY SKILL IN THE ART	11
VI. PETITIONER HAS NOT DEMONSTRATED A REASONABLE LIKELIHOOD OF SUCCESS FOR THE GROUNDS ADVANCED IN THE PETITION, AND THE PETITION SHOULD BE DENIED	12
A. A PHOSITA Would Not Find a Motivation to Combine Munetoh and Rajan	14
B. Ground 1: Claim 1 is Not Obvious Over Munetoh in Combination with Rajan.....	15
1. Munetoh in Combination with Rajan Does Not Disclose “a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application,” as Required by Claim 1	15
2. Munetoh in Combination with Rajan Does Not Disclose “a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components,” as Required by Claim 1	19

3.	Munetoh in Combination with Rajan Does Not Disclose “generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result,” as Required by Claim 1	22
C.	Ground 2: Claim 1 is Not Obvious Over Rajan in Combination with Munetoh	23
1.	Rajan in Combination with Munetoh Does Not Disclose “a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application,” as Required by Claim 1	23
2.	Rajan in Combination with Munetoh Does Not Disclose “a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components,” as Required by Claim 1	24
3.	Rajan in Combination with Munetoh Does Not Disclose “generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result,” as Required by Claim 1	25
D.	Dependent Claims 2-7 and 9	28
VII.	THE PETITION SHOULD BE DENIED IN THE DISCRETION OF THE DIRECTOR UNDER 35 U.S.C. § 314(A)	28
A.	The Parallel District Court Proceeding and the Petition Involve the Same Parties	30

B.	The District Court Litigation Involves Substantially the Same Claims.....	30
C.	Proximity of the District Court’s Trial Date	31
D.	Significant Investment and Petitioner’s Delay in Filing the Petition.....	32
E.	No Stay of the Parallel District Court Litigation	33
F.	Other Factors Favor Discretionary Denial	34
VIII.	THE BOARD SHOULD REJECT ANY LATE SOTERA STIPULATION	35
IX.	CONCLUSION.....	36

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020)	28, 36
<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)	12
<i>Broadcom Corp. v. Emulex Corp.</i> , 732 F.3d 1325 (Fed. Cir. 2013)	13
<i>Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.</i> , IPR2020-00122, Paper 15 (P.T.A.B. May 15, 2020)	30, 32
<i>Edward LifeSciences Corp. v. Evalve, Inc.</i> , IPR2019-01479, Paper 7 (P.T.A.B. Feb. 26, 2020).....	31
<i>Gen. Plastic Indus. Co. v. Canon Kabushiki Kaisha</i> , IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017).....	30
<i>Graham v. John Deere Co. of Kansas City</i> , 383 U.S. 1 (1966).....	12
<i>Innogenetics, N.V. v. Abbott Lab'ys.</i> , 512 F.3d 1363 (Fed. Cir. 2008)	14
<i>Intell. Ventures II v. FedEx Corp.</i> , No. 2:16-cv-00980-JRG, Dkt. 141 (E.D. Tex. Oct. 24, 2017)	33, 34
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	13
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	12

<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)	33
<i>Los Angeles Biomedical Rsch. Inst. at Harbor-UCLA Med. Ctr. v. Eli Lilly & Co.</i> , 849 F.3d 1049 (Fed. Cir. 2017)	13
<i>Next Caller Inc. v. TrustID, Inc.</i> , IPR2019-00961, -00962, Paper 10, at 8-16 (P.T.A.B. Oct. 16, 2019)	32
<i>NHK Spring Co. v. Intri-Plex Techs., Inc.</i> , IPR2018-00752, Paper 8 (P.T.A.B. Sept. 12, 2018).....	30
<i>NXP USA, Inc. v. Impinj, Inc.</i> , IPR2021-01556, Paper 12, 5-6 (P.T.A.B. Aug. 25, 2022); <i>see also</i> <i>id.</i> , IPR2021-01556, Paper 13, 3-4 (P.T.A.B. Sept. 7, 2022)	36
<i>Pers. Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	13
<i>Samsung Elecs. Am., Inc. v. Uniloc 2017 LLC</i> , IPR2019-01218, Paper 7 (P.T.A.B. Jan. 7, 2020)	31
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12, 13-14 (P.T.A.B. Dec. 1, 2020) (designated Dec. 17, 2020)	35, 36
<i>Stratoflex, Inc. v. Aeroquip Corp.</i> , 713 F.2d 1530 (Fed. Cir. 1983)	12
<i>Supercell Oy v. Gree, Inc.</i> , IPR2020-00513, Paper 11 (P.T.A.B. June 24, 2020)	31
<i>Trend Micro, Inc., v. Taasera Licensing LLC</i> , IPR2023-00801, Paper 3 (P.T.A.B. April 27, 2023)	30
<i>In re Van Os</i> , 844 F.3d 1359 (Fed. Cir. 2017)	14

Statutes

35 U.S.C. § 314(a)	1, 28, 29, 34
35 U.S.C. § 314(b)(1).....	31
35 U.S.C. § 316(a)(11).....	31

Other Authorities

37 C.F.R. § 42.1(b)’s.....	35
Munetoh, et al., “Integrity Management Infrastructure for Trusted Computing” IEICE TRANS. INF. & SYST., Vol. E91-D, No. 5, 1242-1251, (May 2008).....	1
Rajan, et al. “Tisa: Toward Trustworthy Services in a Service-Oriented Architecture,” IEEE Transactions on Services Computing, Vol. 1, No. 4, 201-213, (October-December 2008).....	1

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 6, 2023, Trend Micro, Inc. (“Petitioner”) submitted a petition (Paper 2, “Petition” or “Pet.”) to institute *inter partes* review (“IPR”) of U.S. Patent No. 8,327,441 (Ex. 1001, the “’441 Patent”), challenging claims 1-7 and 9 (the “Challenged Claims”). The Petition asserts that the Challenged Claims are obvious over Munetoh, et al., “Integrity Management Infrastructure for Trusted Computing” IEICE TRANS. INF. & SYST., Vol. E91-D, No. 5, 1242-1251, (May 2008) (“Munetoh”) in combination with Rajan, et al. “Tisa: Toward Trustworthy Services in a Service-Oriented Architecture,” IEEE Transactions on Services Computing, Vol. 1, No. 4, 201-213, (October-December 2008) (“Rajan”). Pet. at 3. However, 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 Munetoh in combination with Rajan; and (2) the Board should exercise its discretion to deny the Petition under 35 U.S.C. § 314(a).

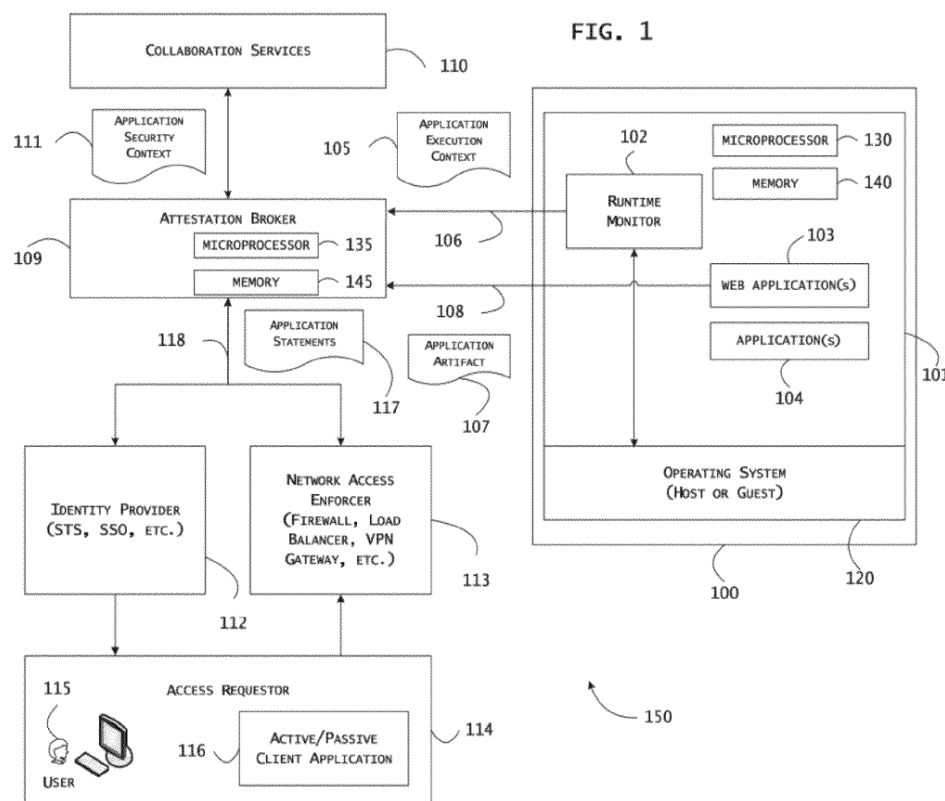
Both of Petitioner’s cited references, Munetoh and Rajan, only disclose, at most, monitoring loaded components *on the platform* rather than components *of the application*. Munetoh and Rajan are silent on executable file binaries and loaded components, let alone executable file binaries and loaded components of the application, and therefore cannot disclose at least the “execution context” or “security context” that is based on those executable file binaries of the application

and loaded components of the application. Rajan also does not disclose a report indicating security risks associated with the application because the system of Rajan is directed towards the monitor and the local architecture broadly. Moreover, a PHOSITA would not find a motivation to combine Munetoh and Rajan at least because the two systems of Munetoh and Rajan contradict each other. Rajan teaches away from measuring applications, while Munetoh at least allows applications running on the platform to be measured. A PHOSITA could not combine them in view of the contradiction.

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 '441 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 '441 PATENT

The '441 Patent “relates to the field of data center virtualization and, more particularly, to a system and method to provide attestation of applications at runtime.” '441 Patent, 1:15-19. Such applications are a part of a broader platform, as indicated in Fig. 1, represented below.



Id., Fig. 1.

The '441 Patent specification and other claims describe executable file binaries that are the subject of an execution analysis, such as by a malware analysis system, and that executable file binaries are related to running processes of an

application on an instrumented target platform, but are not processes of the platform itself:

The attestation broker 402 may also request on [sic] or more collaboration services 403 to perform a static, dynamic and/or virtual execution analysis of the executable file binary, for example, by a malware analysis system.

Id., 14:45-48.

a runtime monitor for;

discovering, identifying and *inspecting running application processes on the instrumented target platform*,¹

wherein the discovering includes *analysis of executable file binaries of the target, running applications*;

a collaboration service configured to:

...

analyze *executable file binaries for the target application running on the instrumented target platform*.

Id., Claim 21.

The '441 Patent also explicitly distinguishes the platform, as a whole, versus the specific loaded components of the application running on the platform:

In certain exemplary embodiments, the generation of attribute value assertions for the application *execution context 105 by the runtime monitor 102 on the instrumented platform 100* may include, for example, the collection of file hash digests and/or file attributes (e.g.,

¹ Emphasis added unless otherwise noted.

file size, publisher details, creation and/or modification timestamps, digital signings, and product versions) for *loaded (e.g., all loaded and/or in process) components of the running target application* 103 or 104.

Id., 8:5-13.

III. THE ALLEGED PRIOR ART

A. Munetoh

Munetoh is directed towards integrity measurement of a target platform. Munetoh “introduce[s] the notion of the Platform Validation Authority, a trusted third party, which verifies the composition of the integrity measurement of the target platform in the Integrity Reports.” Ex. 1005, 1. Munetoh also uses Platform Trust Services (PTS) in the target platform, which “collects and measures the runtime integrity of the target platform in a secure way.” *Id.* The general architecture of PTS is shown below:

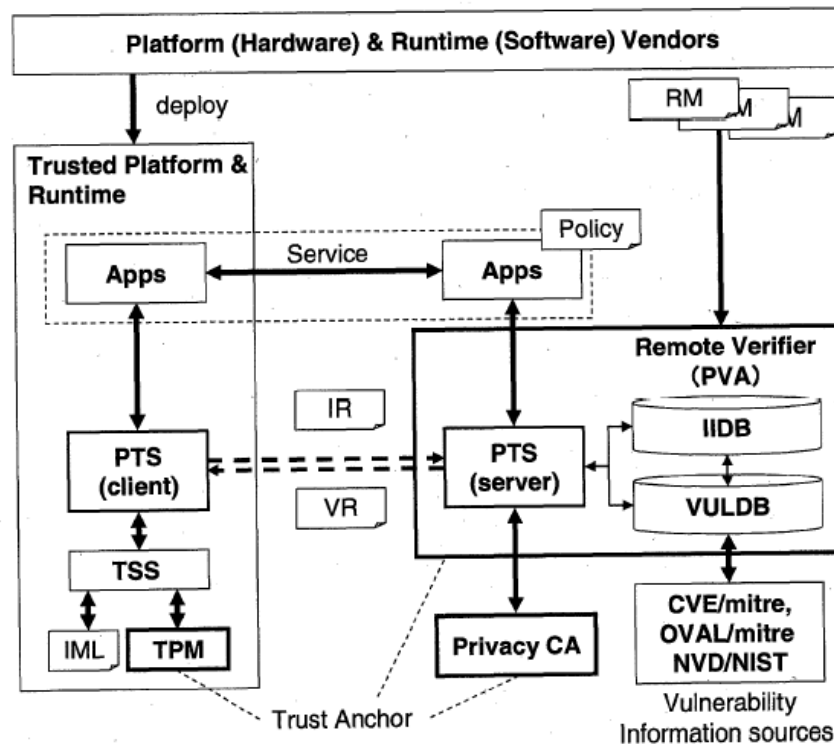


Fig. 1 PTS Client/Server architecture.

Id., Fig. 1.

Munetoh describes that the platform may “send additional information in an attestation, such as the integrity measurement log, which includes a list of components loaded *on the platform* and measured by the TPM, and how these components are composed.” *Id.*, 3.

Munetoh’s Integrity Measurement Log (IML) “includes a list of components loaded on the platform and measured by the TPM and how they are composed.” *Id.* Munetoh discloses a finite state machine (FSM) that analyzes the IML and IR based

on a behavioral model that represents platform states and ‘the integrity of the component that is loaded and executed.’” *Id.*, 5-6.

B. Rajan

Rajan is directed toward “[v]erifying whether a service implementation is conforming to its service-level agreements,” which “is important to inspire confidence in services in a service-oriented architecture.” Ex. 1006 at 1.

More particularly, Rajan is directed towards verifying the integrity of a remotely-hosted requirements monitor, and specifically “look[ing] at static checksum as a method of ensuring the integrity of the monitor”:

In this work, we proposed a technique, its implementation, and experimental validation, which serve to verify the integrity of a remotely-hosted requirements monitor. The implementation of the proposed technique was evaluated using the standard Web services available with the Apache Axis Distribution. The evaluation demonstrated the feasibility of implementing our technique. It also demonstrated that our technique was effective in monitoring the nonfunctional requirements of the Web services. Our current experimental results have looked at static checksum as a method of ensuring the integrity of the monitor.

Id. at 12

Rajan discloses a trace-based monitor, where traces are used for the purpose of compliance with certain policies or “requirements [that] are specified as logical formulas:”

In a trace-based monitor, requirements are specified as logical formulas over program traces. An example of such a trace-based requirement for the payment processing service could be, “in no trace of the service implementation, the argument credit card number directly or indirectly flows to a persistence-related method, e.g., File.write (...).”

Id., 5-6.

For the purpose of this experiment, we defined the requirement as “the execution trace of the program involving the variables and methods dealing with client data labeled as sensitive, should not include APIs dealing with persistence or serialization.”

Id. at 6.

Rajan discloses that its system provides a report that includes an *immutable integrity measurement of the local architecture*:

The trust analyzer component, which derives its root of trust from the TPM on the provider’s side, serves to verify the integrity of the requirements monitor. It ***provides a report that includes an immutable integrity measurement of the local architecture*** along with a time stamp to indicate the freshness of the measurement. The requirements monitor in turn determines whether the trace of service execution satisfied the desired nonfunctional requirements. TPM is also used to attest to the identity of the service provider.

Id. The “immutable” or unchangeable nature of the integrity measurement of Rajan’s local architecture is irrespective of any application running on that

architecture, which is why Rajan states that “we are not directly measuring applications which may change frequently.”

[W]e are not directly measuring the applications which may change frequently, but all that we monitor is the specific requirements of the applications that are not supposed to change.

Id. at 10. The “specific requirements,” noted above, which are monitored by the system of Rajan, refer to policies that need to be checked:

Our prototype can also be easily extended to support a full-fledged specification language, such as the one we are currently developing [34], which allows policies specified in linear temporal logic [35] to be checked.

Id. at 6.

IV. CLAIM CONSTRUCTION

For the purposes of this Preliminary Response only, Patent Owner believes that claim construction is not required to resolve any issues. Petitioner also notes that it believes that claim construction is not otherwise warranted. Pet. at 10-11; However, there are several terms that both Petitioner and Patent Owner have proposed constructions for in the District Court Litigation:

<u>Claim Term</u>	<u>Patent Owner's Proposed Construction</u>	<u>Petitioner's Proposed Construction</u>
“attestation” ’441 Patent Claims 1, 2, 3, 5, and 7	“verification”	“verifying/verifies the identity of an application”
“runtime” ’441 Patent Claims 1, 2, and 5	“the time the application is running”	“the time the application is running”
“at runtime” ’441 Patent Claim 1	preamble limiting at least as to “at runtime”; meaning “at the time the application is running”	preamble limiting at least as to “at runtime”; meaning “at the time the application is running”
“receiving ... a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application” ’441 Patent Claims 1 and 4	Plain and ordinary meaning subject to the construction of “runtime”	Receiving at the time the application is running an execution context that includes the executable file binaries of the application (as distinct from binary hashes) and loaded components of the application
“a security context providing security information about the application” ’441 Patent Claims 1, 4, and 5	Plain and ordinary meaning	“security information about the application provided by a collaboration service”

<u>Claim Term</u>	<u>Patent Owner's Proposed Construction</u>	<u>Petitioner's Proposed Construction</u>
“an application artifact” '441 Patent Claim 2	Plain and ordinary meaning	“data identifying one or more attribute value assertions that describe the application runtime execution context”
“introspective security context” '441 Patent Claims 4 and 5	Plain and ordinary meaning	a security context based on evaluation of historic state information and measurements [of the remote computing platform] sampled over a period of time; Otherwise, Indefinite.

Ex. 2003 at 39-55, 62-69. Petitioner’s conflicting claim construction positions between this proceeding and the District Court Litigation, in addition to the plethora of other outstanding issues that affect validity, weigh 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 to two years of education or experience in the field of computer security topics. More education can supplement practical experience and vice versa.” Pet. at 10 (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. A PHOSITA Would Not Find a Motivation to Combine Munetoh and Rajan

A PHOSITA would not find a motivation to combine Munetoh and Rajan at least because the system of Rajan teaches away from measuring applications (“we are not directly measuring the applications”) (Ex. 1006, 10), while the PTS system of Munetoh (although it is silent on executable file binaries and loaded components of applications), at least “allows applications running on the platform to be measured” (Ex. 1005, 5). The two references directly contradict each other and a PHOSITA would not combine them, particularly where the claim limitations require “runtime execution context indicating *attributes of the application* at runtime” and a “security context providing *security information about the application.*”

B. Ground 1: Claim 1 is Not Obvious Over Munetoh in Combination with Rajan

1. Munetoh in Combination with Rajan Does Not Disclose “a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application,” as Required by Claim 1

Claim 1 of the '441 Patent recites “a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application.” Munetoh in combination with Rajan does not render this claim limitation obvious, as Petitioner incorrectly asserts. Pet. at 22-24.

Petitioner argues that Munetoh’s integrity reports disclose the claimed runtime execution context indicating attributes of the application at runtime. Pet. at 22. However, the claim language is clear that “attributes comprise one or more executable file binaries of the application and loaded components of the application.” Petitioner and Munetoh are silent on executable file binaries *of the application* and loaded components *of the application*. Petitioner merely states that “Munetoh describes a trusted bootstrap process that ‘comprises an iterative process of ‘measurement’, loading, and execution of software components’ (corresponding to ‘executable file binaries of the application and loaded components of the application’”). Pet. at 23. Petitioner does not meet its burden to show how Munetoh’s

iterative *process*, which comprises actions, corresponds to two tangible aspects of the application: executable file binaries and loaded components.

Petitioner completely ignores the claimed “executable file binaries of the application.” Munetoh only mentions “binaries” or “binary” in the context of “Related Work” that has been performed. Ex. 1005, 2. For example, Munetoh describes that “Terra [6] provides isolated trusted platforms on top of a virtual machine monitor, and allows attestation by a binary image of each virtual machine, such as virtual disk images, virtual BIOS, and VM descriptions. The binary attestation approach of Terra is suitable for closed-architecture platforms. . . . The verification of binary attestation has been recognized as a difficult research problem for years.” *Id.* The mention of binary or binaries in Munetoh is completely inapposite to the claim language.

The ’441 Patent describes executable file binaries that are the subject of an execution analysis, such as by a malware analysis system, and that executable file binaries are related to running processes of an application on an instrumented target platform, but are not processes of the platform itself:

The attestation broker 402 may also request on [sic] or more collaboration services 403 to perform a static, dynamic and/or virtual execution analysis of the executable file binary, for example, by a malware analysis system.

’441 Patent, 14:45-48.

a runtime monitor for;

discovering, identifying and *inspecting running application processes on the instrumented target platform*,

wherein the discovering includes *analysis of executable file binaries of the target, running applications*;

a collaboration service configured to:

...

analyze *executable file binaries for the target application running on the instrumented target platform*.

Id., Claim 21. Nowhere does Munetoh mention executable file binaries, let alone executable file binaries *of the application* for the purpose of analysis, as described in subsequent claim limitations.

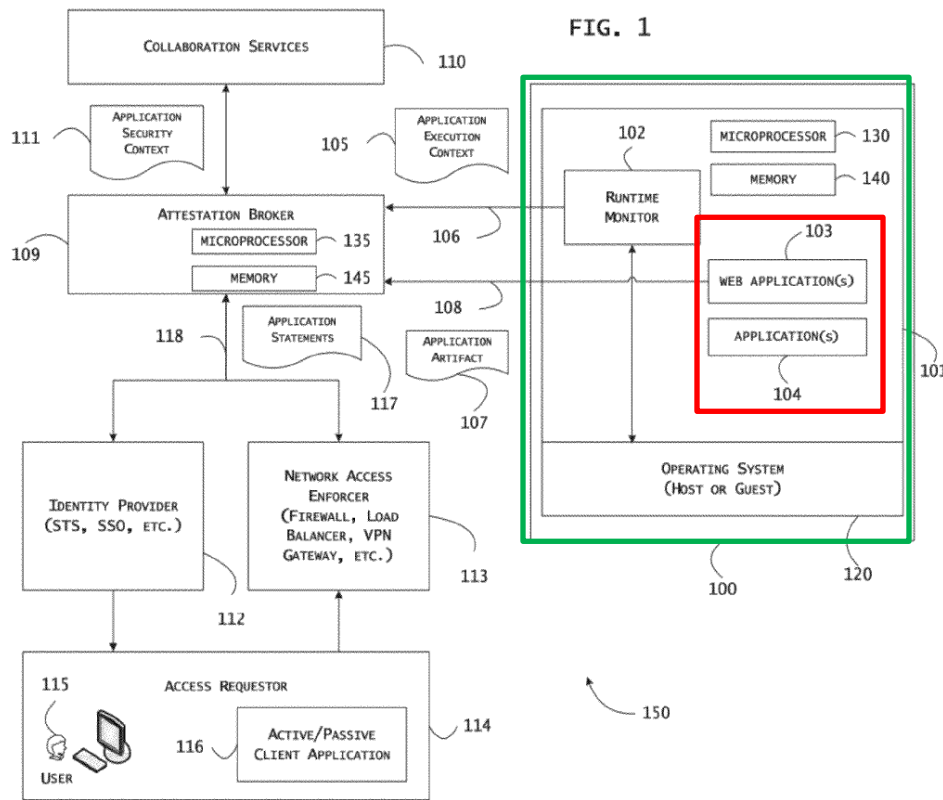
Munetoh only discloses monitoring loaded components *on the platform* rather than components *of the application*. Petitioner also admits this: “Munetoh describes that the platform may ‘send additional information in an attestation, such as the integrity measurement log, which includes a list of *components loaded on the platform* and measured by the TPM, and how these components are composed.’” Pet. at 24 (citing Ex. 1005, p.3).

The ’441 Patent explicitly distinguishes the platform, as a whole, versus the specific loaded components of the application:

In certain exemplary embodiments, the generation of attribute value assertions for the application *execution context 105 by the runtime monitor 102 on the*

instrumented platform 100 may include, for example, the collection of file hash digests and/or file attributes (e.g., file size, publisher details, creation and/or modification timestamps, digital signings, and product versions) for *loaded (e.g., all loaded and/or in process) components of the running target application 103 or 104.*

'441 Patent, 8:5-13.



Id., Fig. 1 (annotated) (indicating the applications in red and the overall platform in green). Petitioner glosses over this apparent distinction between loaded components *on the platform* versus loaded components *of the application*.

For these reasons, Munetoh in combination with Rajan does not render obvious this claim limitation.

2. Munetoh in Combination with Rajan Does Not Disclose “a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components,” as Required by Claim 1

Claim 1 of the '441 Patent recites “a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components.” Munetoh in combination with Rajan does not render this claim limitation obvious, as Petitioner asserts. Pet. at 24-27.

Since Petitioner fails to show how Munetoh in combination with Rajan discloses, teaches, or suggests the claimed “one or more executable file binaries and the loaded components,” it cannot now disclose, teach, or suggest “an execution analysis of the one or more executable file binaries and the loaded components.” *See supra* Section VI.B.1.

As with the previous claim limitation, Munetoh only discloses monitoring loaded components *on the platform* rather than components *of the application*. Petitioner argues that the claimed “execution analysis of the one or more executable file binaries and the loaded components” is disclosed by Munetoh’s “Integrity Measurement Log (IML) [which] ‘includes a list of *components loaded on the platform* and measured by the TPM and how they are composed.’ Munetoh discloses a finite state machine (FSM) that analyzes the IML and IR based on a behavioral

model that represents *platform states* and ‘the integrity of the component that is loaded and executed.’” Pet. at 25 (citations omitted). Again, Petitioner and the cited portions of Munetoh fail to mention analyzing executable file binaries or loaded components, let alone executable file binaries or loaded components *of the application*.

Rajan does not cure the deficiencies of Munetoh. Petitioner incorrectly argues that Rajan’s “requirements monitor [which] traces the operations of running programs and traces variables, methods, and arguments of the programs” discloses the claimed “execution analysis.” *Id.* at 26-27. However, Rajan’s disclosure of the trace-based monitor is clear that traces are used for the purpose of compliance with certain policies or “requirements [that] are specified as logical formulas:”

In a trace-based monitor, requirements are specified as logical formulas over program traces. An example of such a trace-based requirement for the payment processing service could be, “in no trace of the service implementation, the argument credit card number directly or indirectly flows to a persistence-related method, e.g., File.write (...).”

Ex. 1006, 5-6.

For the purpose of this experiment, we defined the requirement as “the execution trace of the program involving the variables and methods dealing with client data labeled as sensitive, should not include APIs dealing with persistence or serialization.”

Id. at 6. Notably, Rajan is devoid of any mention of executable file binaries and loaded components of the application.

A PHOSITA would also not expect to find an analysis to analyze executable file binaries or loaded components of application because the system of Rajan is not directed to applications. Rajan explicitly describes that it does not measure applications:

[W]e are not directly measuring the applications which may change frequently, but all that we monitor is the specific requirements of the applications that are not supposed to change.

Id. at 10. The monitored “specific requirements” described above refer to policies that need to be checked:

Our prototype can also be easily extended to support a full-fledged specification language, such as the one we are currently developing [34], which allows policies specified in linear temporal logic [35] to be checked.

Id. at 6.

Therefore, Munetoh in combination with Rajan does not render obvious this claim limitation.

3. Munetoh in Combination with Rajan Does Not Disclose “generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result,” as Required by Claim 1

Claim 1 of the '441 Patent recites “generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result.” Munetoh in combination with Rajan does not render this claim limitation obvious, as Petitioner incorrectly asserts. Pet. at 27-31.

Since Petitioner fails to show how Munetoh in combination with Rajan discloses, teaches, or suggests the claimed “execution context” and “security context,” it cannot now disclose, teach, or suggest “generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result.” *See supra* Sections VI.B.1 and VI.B.2.

Therefore, Munetoh in combination with Rajan does not render obvious this claim limitation.

C. Ground 2: Claim 1 is Not Obvious Over Rajan in Combination with Munetoh

1. Rajan in Combination with Munetoh Does Not Disclose “a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application,” as Required by Claim 1

Claim 1 of the '441 Patent recites “a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application.” Rajan in combination with Munetoh does not render this claim limitation obvious, as Petitioner incorrectly asserts. Pet. at 48-49.

Petitioner’s argument amounts to one sentence stating that “Rajan discloses that the traces are a ‘static checksum of the software stack’ (corresponding to ‘the attributes comprise one or more executable file binaries of the application’) and logs of running services (corresponding to ‘the attributes comprise one or more ...loaded components of the application’).” *If.* at 49. But Rajan’s static checksum of the software stack is inapposite. Nowhere does Rajan refer to “software stack” as the application. Rajan only describes that “[o]ur current experimental results have looked at static checksum as a method of ensuring the integrity of the monitor.” As noted above, the system of Rajan does not measure applications. Ex. 1006, 10 (“[W]e are not directly measuring the applications”). Therefore a PHOSITA would not

assume that such software stacks have any relation to the claimed “one or more executable file binaries of the application and loaded components of the application.”

For these reasons, Rajan in combination with Munetoh does not render obvious this claim limitation.

2. Rajan in Combination with Munetoh Does Not Disclose “a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components,” as Required by Claim 1

Claim 1 of the '441 Patent recites “a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components.” Rajan in combination with Munetoh does not render this claim limitation obvious, as Petitioner asserts. Pet. at 49-51.

Since Petitioner fails to show how Rajan in combination with Munetoh discloses, teaches, or suggests the claimed “one or more executable file binaries of the application and loaded components of the application,” it cannot now disclose, teach, or suggest “an execution analysis of the one or more executable file binaries and the loaded components.” *See supra* Section VI.C.1.

Petitioner relies on the same arguments as its Ground 1 combination of Munetoh and Rajan. Specifically, Petitioner relies upon Rajan’s “requirements

monitor [which] traces the operations of running programs and traces variables, methods, and arguments of the programs” (Pet. at 49) and Munetoh’s “Integrity Measurement Log (IML) [which] ‘includes a list of components loaded on the platform and measured by the TPM and how they are composed’” (Pet. at 50). As noted above in Section VI.B.2, neither of these cited aspects of Munetoh and Rajan, or any other disclosure in Munetoh and Rajan, disclose analyzing one or more executable file binaries and the loaded components.

Further, as described in Section VI.A, there is no motivation to combine Munetoh and Rajan when they directly contradict each other on measuring applications.

Therefore, Rajan in combination with Munetoh does not render obvious this claim limitation.

3. Rajan in Combination with Munetoh Does Not Disclose “generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result,” as Required by Claim 1

Claim 1 of the ’441 Patent recites “generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result.” Rajan in combination with Munetoh does not render this claim limitation obvious, as Petitioner incorrectly asserts. Pet. at 51-53.

Since Petitioner fails to show how Rajan in combination with Munetoh discloses, teaches, or suggests the claimed “execution context” and “security context,” it cannot now disclose, teach, or suggest “generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result.” *See supra* Sections VI.C.1 and VI.C.2.

Petitioner argues that Rajan discloses this claim limitation through an “attestation response.” Pet. at 52. Petitioner does not make any effort to disclose a “report,” let alone the claimed “report indicating security risks *associated with the application.*” As noted before, Rajan does not directly measure applications. Ex. 1006, 10.

The only report disclosed in Rajan does not indicate security risks associated with the application based on the received runtime execution context and the received security context, but is a report that includes an *immutable integrity measurement of the local architecture*:

The trust analyzer component, which derives its root of trust from the TPM on the provider’s side, serves to verify the integrity of the requirements monitor. It *provides a report that includes an immutable integrity measurement of the local architecture* along with a time stamp to indicate the freshness of the measurement. The requirements monitor in turn determines whether the trace of service execution satisfied the desired nonfunctional

requirements. TPM is also used to attest to the identity of the service provider.

Id. at 6. The “immutable” or unchangeable nature of the integrity measurement of Rajan’s local architecture is irrespective of any application running on that architecture, which is why Rajan states it does not directly measure applications “which may change frequently.”

[W]e are not directly measuring the applications which may change frequently, but all that we monitor is the specific requirements of the applications that are not supposed to change.

Id. at 10. Again, Rajan is directed towards verifying the integrity of a remotely-hosted requirements monitor, and specifically “look[ing] at static checksum as a method of ensuring the integrity of the monitor.”

In this work, we proposed a technique, its implementation, and experimental validation, which serve to ***verify the integrity of a remotely-hosted requirements monitor***. The implementation of the proposed technique was evaluated using the standard Web services available with the Apache Axis Distribution. The evaluation demonstrated the feasibility of implementing our technique. It also demonstrated that our technique was effective in monitoring the nonfunctional requirements of the Web services. ***Our current experimental results have looked at static checksum as a method of ensuring the integrity of the monitor.***

Id. at 12. Because the system of Rajan is directed towards the monitor and the local architecture broadly, a PHOSITA would not expect to find a report indicating security risks associated with the application to be disclosed in Rajan.

Therefore, Rajan in combination with Munetoh does not render obvious this claim limitation.

D. Dependent Claims 2-7 and 9

Claims 2-7 and 9 are dependent on Claim 1. Therefore, Claims 2-7 and 9 are not rendered obvious by any combination of Munetoh and Rajan for at least the same reasons as Claim 1.

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. *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. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8, at 20 (P.T.A.B. Sept. 12, 2018) (quoting *Gen. Plastic Indus. Co. 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 ’441 Patent). *Trend Micro, Inc., v. Taasera Licensing LLC*, IPR2023-00801, Paper 3 at 2-3 (P.T.A.B. April 27, 2023); Pet. at 64. 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

All of the asserted claims of the ’441 Patent in the District Court Litigation are at issue in this Petition. “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, Pat. Litig.*, 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.*,

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.

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.*, IPR2020-00122, 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 were 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 references that Petitioner raised

³ As noted above, the statutory deadline for institution is December 14, 2023. *See supra* n. 1. Per Ex. 2001, the claim construction hearing is October 11, 2023, and the deadline to complete fact discovery is November 6, 2023.

in the District Court Litigation for both anticipation or any of the combinations of obviousness, and do not include Petitioner's challenges under § 112 or § 101. *See generally* Ex. 2002, at 13-17, 33-34, 40-43, 64-65, 100-110, 253-256, and 339-340. *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 61-63.

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 on 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 ’441 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 Inc.*, 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

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
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 7,016 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
Email: pat-docketing@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