

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.
Petitioner,

v.

TAASERA LICENSING LLC,
Patent Owner.

Case No. IPR2023-00704
U.S. Patent No. 8,850,517

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,850,517**

TABLE OF CONTENTS

	Page
Petitioner’s Exhibit List	viii
I. Introduction	1
II. Requirements for <i>Inter Partes</i> Review	2
A. Certification	2
B. Identification of Challenges	3
III. The ’517 Patent	3
A. Effective Filing Date	3
B. Level of Ordinary Skill in the Art	3
C. Overview of the ’517 Patent	4
D. Relevant Prosecution History	7
IV. Claim Construction	10
V. Detailed Discussion of the Grounds for Unpatentability	10
A. Overview of the Prior Art	11
1. Alperovitch (Ex. 1004)	11
2. Yeh (Ex. 1005)	16
3. Chien (Ex. 1006)	17
B. Ground 1: Claims 1-24 Are Rendered Obvious by Alperovitch in View of the Knowledge of a POSITA	18
1. Claim 1	18
a. Preamble	18
b. Limitation 1[a]	19
c. Limitation 1[b]	23
d. Limitation 1[c]	25
e. Limitation 1[d]	27
f. Limitation 1[e]	30
g. Limitation 1[f]	30
2. Claim 2	32
3. Claim 3	33

4. Claim 4	34
5. Claim 5	35
6. Claim 6	35
a. Limitation 6[a]	35
b. Limitation 6[b]	36
c. Limitation 6[c]	37
7. Claim 7	37
a. Limitation 7[a]	37
b. Limitation 7[b]	38
c. Limitation 7[c]	38
8. Claim 8	39
a. Limitation 8[a]	39
b. Limitation 8[b]	39
c. Limitation 8[c]	39
9. Claim 9	40
a. Limitation 9[a]	40
b. Limitation 9[b]	41
c. Limitation 9[c]	41
d. Limitation 9[d]	42
e. Limitation 9[e]	43
f. Limitation 9[f]	43
10. Claim 10	44
11. Claim 11	45
12. Claim 12	46
a. Limitation 12[a]	46
b. Limitation 12[b]	47
13. Claim 13	50
a. Preamble	50
b. Limitation 13[a]	50
c. Limitation 13[b]	51

d. Limitation 13[c]	51
e. Limitation 13[d]	52
f. Limitation 13[e]	53
g. Limitation 13[f].....	53
h. Limitation 13[g]	53
14. Claim 14	53
15. Claim 15	54
16. Claim 16	54
17. Claim 17	54
18. Claim 18	55
a. Limitation 18[a]	55
b. Limitation 18[b]	55
c. Limitation 18[c]	55
19. Claim 19	55
a. Limitation 19[a]	55
b. Limitation 19[b]	56
c. Limitation 19[c]	56
20. Claim 20	56
a. Limitation 20[a]	56
b. Limitation 20[b]	56
c. Limitation 20[c]	57
21. Claim 21	57
a. Limitation 21[a]	57
b. Limitation 21[b]	57
c. Limitation 21[c]	57
d. Limitation 21[d]	58
e. Limitation 21[e]	58
f. Limitation 21[f].....	58
22. Claim 22	58
23. Claim 23	59

24. Claim 24	59
a. Limitation 24[a]	59
b. Limitation 24[b]	59
C. Grounds 2-4: Claims 1-24 Are Rendered Obvious by Alperovitch in View of Yeh (Ground 2), Alperovitch in View of Chien (Ground 3), and Alperovitch in View of Yeh and Chien (Ground 4)	60
1. Claim 1	60
a. Limitation 1[a]	60
b. Limitation 1[e]	65
2. Claim 13	65
a. Limitation 13[a]	65
b. Limitation 13[f]	65
D. No Secondary Considerations Exist	66
VI. The Parallel District Court Proceeding Does Not Warrant a Discretionary Denial	66
VII. Mandatory Notices	67
A. Real Parties-in-Interest	67
B. Related Proceedings	67
C. Lead and Backup Counsel	67
D. Electronic Service	68
VIII. Fees	68
IX. Conclusion	68

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Palo Alto Networks, Inc. v. Taasera Licensing LLC</i> , No. 1-22-cv-02306 (S.D.N.Y.)	67
<i>Palo Alto Networks, Inc. v. Taasera Licensing LLC</i> , No. 2-22-cv-00314 (E.D. Tex.)	67
<i>In re: Taasera Licensing LLC Patent Litig.</i> , No. 2-22-md-03042 (E.D. Tex.)	67
<i>Taasera Licensing LLC v. Palo Alto Networks, Inc.</i> , No. 2-22-cv-00062 (E.D. Tex.)	67
<i>Taasera Licensing LLC v. Trend Micro Inc.</i> , No. 2-21-cv-00441 (E.D. Tex.)	67
<i>Trend Micro Inc v. Taasera Licensing LLC</i> , No. 2-22-cv-00303 (E.D. Tex.)	67
<i>Trend Micro Inc. v. Taasera Licensing LLC</i> , No. 3-22-cv-00477 (N.D. Tex.)	67
<i>Trend Micro, Inc. v. Taasera Licensing LLC</i> , No. 3-22-cv-00518 (N.D. Tex.)	67
<i>Taasera Licensing LLC v. Musarubra US, LLC</i> , No. 2-22-cv-00427 (E.D. Tex.)	67
<i>Taasera Licensing LLC v. CrowdStrike, Inc.</i> , No. 6-22-cv-01094 (W.D. Tex.)	67
<i>Taasera Licensing LLC v. CrowdStrike, Inc.</i> , No. 2-22-cv-00468 (E.D. Tex.)	67
Statutes	
35 U.S.C. § 314(a)	66

Other Authorities

37 C.F.R. § 42.15	2
37 C.F.R. § 42.22	3
37 C.F.R. § 42.104	2
37 C.F.R. § 42.104(a).....	2
37 C.F.R. § 42.104(b)	3
37 C.F.R. § 42.105	2
37 C.F.R. § 42.106	2

PETITIONER’S EXHIBIT LIST

Ex. No.	Brief Description
1001	U.S. Patent No. 8,850,517
1002	U.S. Patent No. 8,850,517 File History
1003	Declaration of Kevin Jeffay, Ph.D.
1004	U.S. Patent App. Pub. No. 2013/0254880 to Alperovitch et al. (“Alperovitch”)
1005	U.S. Patent No. 9,117,075 to Yeh (“Yeh”)
1006	U.S. Patent No. 9,117,078 to Chien et al. (“Chien”)

I. Introduction

Petitioner Palo Alto Networks, Inc. (“Petitioner”) requests *inter partes* review (“IPR”) of claims 1-24 (“Challenged Claims”) of U.S. Patent No. 8,850,517 (the “’517 patent”). All claims of the ’517 patent relate to “assessing the runtime risk of an application or device in a computer system using cognitive behavior recognition.” Ex. 1001, 1:7-10. Specifically, the claimed invention purports to identify “an action sequence and assess[] a runtime risk and subsequent behavior score based on the identified action sequence.” *Id.*, 2:19-22.

To assess runtime risk of an application or device in a computer system, every claim of the ’517 patent involves using an assessment policy that includes at least one rule that identifies an action sequence to identify a runtime risk for an application program. The identified runtime risk indicates a risk or threat of an identified action sequence of the application, and a behavior score for the application program that executes on the device is identified based on the identified runtime risk. As shown below and in the declaration of Dr. Kevin Jeffay (Ex. 1003), all claims of the ’517 patent would have been obvious to a person of ordinary skill in the art (“POSITA”) in view of U.S. Patent App. Pub. No. 2013/0254880 to Alperovitch et al. (“Alperovitch”), which was not before the Examiner during prosecution of the ’517 patent. Alternatively, all claims of the ’517 patent would have been rendered

Petition for IPR re U.S. Patent No. 8,850,517

obvious by Alperovitch in view of U.S. Patent No. 9,117,075 to Yeh (“Yeh”) and/or U.S. Patent No. 9,117,078 to Chien et al. (“Chien”).

As explained in this Petition, the claims of the ’517 patent would not have been allowed if the primary reference Alperovitch had been substantively evaluated by the Examiner during prosecution of the ’517 patent. Alperovitch discloses a materially identical method and system for assessing the probability that a mobile application is malicious software based on attributes involving the mobile application and calculating a reputation score for the mobile application. Therefore, the Challenged Claims should be found unpatentable given the strength of the prior art as shown herein.

II. Requirements for *Inter Partes* Review

This Petition complies with all statutory requirements, as well as 37 C.F.R. §§ 42.104, 42.105, and 42.15, and should be accorded a filing date pursuant to 37 C.F.R. § 42.106. The required fee is being paid electronically through PTAB E2E.

A. Certification

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the ’517 patent is available for IPR, and Petitioner is not barred or estopped from requesting an IPR challenging the claims on the grounds identified herein.

B. Identification of Challenges

Under 37 C.F.R. §§ 42.104(b) and 42.22, Petitioner requests that the Board institute this IPR on all claims of the '517 patent and cancel those claims as unpatentable on the following grounds:

Ground	Claims	Basis	Reference
1	1-24	103	Alperovitch (Ex. 1004)
2	1-24	103	Alperovitch in view of Yeh (Ex. 1005)
3	1-24	103	Alperovitch in view of Chien (Ex. 1006)
4	1-24	103	Alperovitch in view of Yeh and Chien

III. The '517 Patent

A. Effective Filing Date

The '517 patent issued from Application No. 13/741,878 (the "'878 Application"), filed January 15, 2013. For the purposes of this Petition, Petitioner assumes that the Challenged Claims are entitled to a priority date no earlier than January 15, 2013.

B. Level of Ordinary Skill in the Art

As of January 15, 2013, a person of ordinary skill in the art ("POSITA") in the '517 patent's technical field would have had a bachelor's degree in computer science or computer engineering, or an equivalent field and at least two to three years of experience in computer and network security. Ex. 1003, ¶22. Someone with less or different technical education but more relevant practical experience, or more

relevant education but less practical experience, could also be considered a POSITA. *Id.* This level of skill in the art is reflected by the reference cited in this Petition, the state of the art, and the experience of Dr. Kevin Jeffay, as described in his declaration.

C. Overview of the '517 Patent

The '517 patent is titled “Runtime Risk Detection Based on User, Application, and System Action Sequence Correlation.” Ex. 1001, cover. It relates to “assessing runtime risk for an application or device.” *Id.*, abstract. The '517 patent purports to address “[e]merging cyber threats, commonly referred to as advanced persistent threats (APT)” that “remain undetected using traditional security programs and approaches. As a result, many harmful threats and infections can attack a system that includes these security programs unbeknownst to the user and system operator, which could have devastating results. For example, it can place companies at risk for the theft of proprietary information, such as confidential information, trade secrets, etc., and individuals at risk for identify theft.” *Id.*, 1:26-35. The alleged invention of the '517 patent supposedly addresses these threats by “assessing the runtime risk of an application or device in a computer system using cognitive behavior recognition.” *Id.*, 1:8-10.

Figure 1 below shows a high-level architecture of the '517 patent's system for assessing the runtime risk for an application or device in accordance with exemplary embodiments.

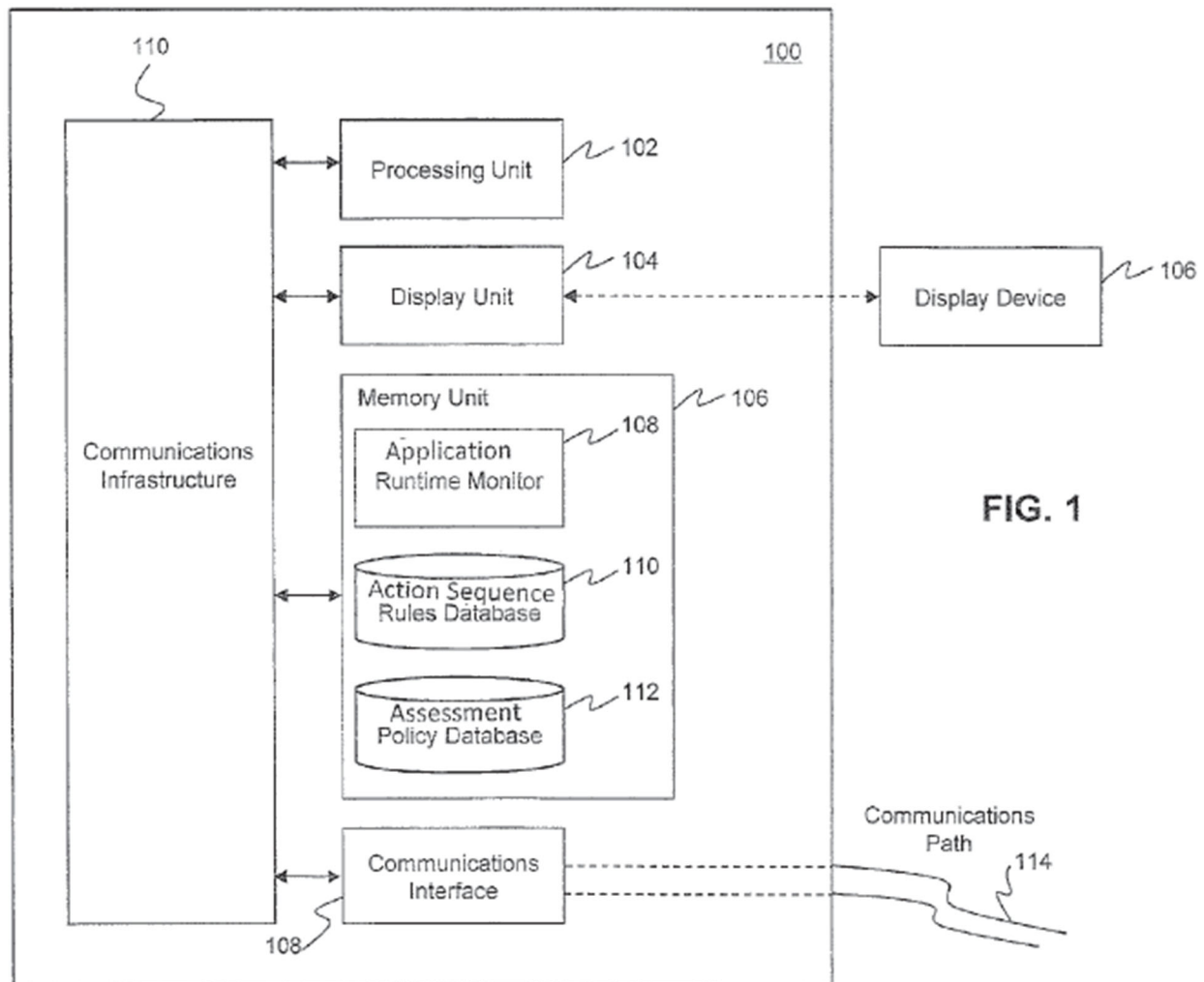


FIG. 1

Id., Fig. 1. “[C]omputing system 100 [is] configured to assess the runtime risk of an application or device and identify a behavior score based on the assessed runtime risk.” *Id.*, 2:40-43.

In assessing the runtime risk of an application or device, computing system 100 includes in memory unit 106 “a runtime monitor 108, a rules database 110, and

a policy database 112.” *Id.*, 3:38-39. The runtime monitor 108 uses at least one assessment policy stored in policy database 112 that comprises one or more rules to identify the runtime risk for an application program. *Id.*, 6:14-17. Furthermore, “[t]he rules database 110 may be configured to store a plurality of rules, wherein each rule identifies an action sequence. An action sequence ... may include a sequence of at least two performed actions, wherein the performed actions may be one of a user action, an application action, and a system action.” *Id.*, 4:12-17.

The ’517 patent has two independent claims. Claim 1 recites:

1. A method for assessing runtime risk for an application program that executes on a device, comprising:
storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence;
storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules;
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; and
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, wherein the action sequence is a sequence of at least two performed actions,
and

each performed action is at least one of: a user action, an application action, and a system action.

Independent claim 13 restates the same steps in the context of a “system.”

The dependent claims add the concept of identifying a behavior score for the application program based on different identified specific examples (claims 2-4, 14-16) or combinations (claims 5-9, 17-21) of performed actions or based on different correlations between performed actions (claims 10-12, 22-24).

D. Relevant Prosecution History

The Examiner issued a non-final office action rejecting pending claims 1-5, 10-17, 22-24 of the '517 patent as, *inter alia*, anticipated by U.S. Patent App. Pub. No. 2013/0096980 to Basavapatna et al. (“Basavapatna”) and rejecting pending claims 6-9, 18-21 as, *inter alia*, rendered obvious by Basavapatna. Ex. 1002, 61, 65.

In response, Applicant amended some of the claims, including the independent claims, to overcome § 112 rejections. *Id.*, 96-97. Applicant further argued that Basavapatna did not anticipate the pending claims because the claims of the present application are directed to assessing the runtime risk of an application program that executes on a device, whereas Basavapatna is directed to testing potential countermeasures against known vulnerabilities of systems. *Id.*, 97. Applicant argued 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 or predict specific types of threats, but instead assesses risk associated with known vulnerabilities.” *Id.*

The Examiner subsequently issued a final office action maintaining, *inter alia*, the rejections of pending claims 1-5, 10-17, 22-24 of the ’517 patent as anticipated by Basavapatna and pending claims 6-9, 18-21 as rendered obvious by Basavapatna. *Id.*, 113, 116.

In response, Applicant amended independent claims 1 and 13 to recite “identifying [~~identify~~], 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 ~~identifies and predicts a specific type of threat~~” and to add “a runtime monitor.” *Id.*, 130, 133.

In an interview with the Examiner, Applicant explained how Basavapatna fails to teach or suggest claims 1 and 13’s “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.” *Id.*, 139. Applicant explained 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.

Furthermore, Applicant explained that Basavapatna does not teach or suggest claims 1 and 13's similar features of "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, wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action" because Basavapatna fails to disclose "a rules database including a plurality of rules that identifies an *action sequence*." *Id.*, 141 (emphasis in original). Applicant contended that the rules in Basavapatna merely define a countermeasure, which are designed to protect against known vulnerabilities. *Id.* Indeed, Applicant argued that not only does Basavapatna not teach or suggest action sequences, "Basavapatna does not teach or suggest any *sequence of performed actions*." *Id.* (emphasis in original). Accordingly, Applicant contended that while the claimed invention assesses risk of action sequences performed by the user, applications, or the system, and thus, can act as a runtime monitor for detecting real-time threats, Basavapatna only assesses risk for systems based on known vulnerabilities. *Id.*, 141-142.

Following Applicant's Request for Continued Examination (*id.*, 158), the Examiner issued a Notice of Allowance (*id.*, 164), which was followed by an additional Applicant's Request for Continued Examination (*id.*, 185) and a Supplemental Notice of Allowability issued by the Examiner (*id.*, 212).

As discussed below, the above limitations that Applicant argued are not taught or suggested in Basavapatna are taught by Alperovitch, Yeh, and Chien. Alperovitch, Yeh, and Chen, the prior art cited in this Petition, were not cited, nor are they cumulative of anything cited, during prosecution.

IV. Claim Construction

The Board construes claims under the same standard used in civil actions in federal district court. Petitioner submits that for the purposes of this Petition, the Board does not need to explicitly construe any claim term, and there are no known claim construction disputes that affect the outcome of this Petition.¹

V. Detailed Discussion of the Grounds for Unpatentability

The Challenged Claims are unpatentable based on one primary ground and three alternative grounds. Ground 1 establishes that claims 1-24 are rendered obvious over Alperovitch in view of the knowledge of a POSITA. Grounds 2, 3, and 4 establish that claims 1-24 are rendered obvious over Alperovitch in view of Yeh, Alperovitch in view of Chien, and Alperovitch in view of Yeh and Chien, respectively.

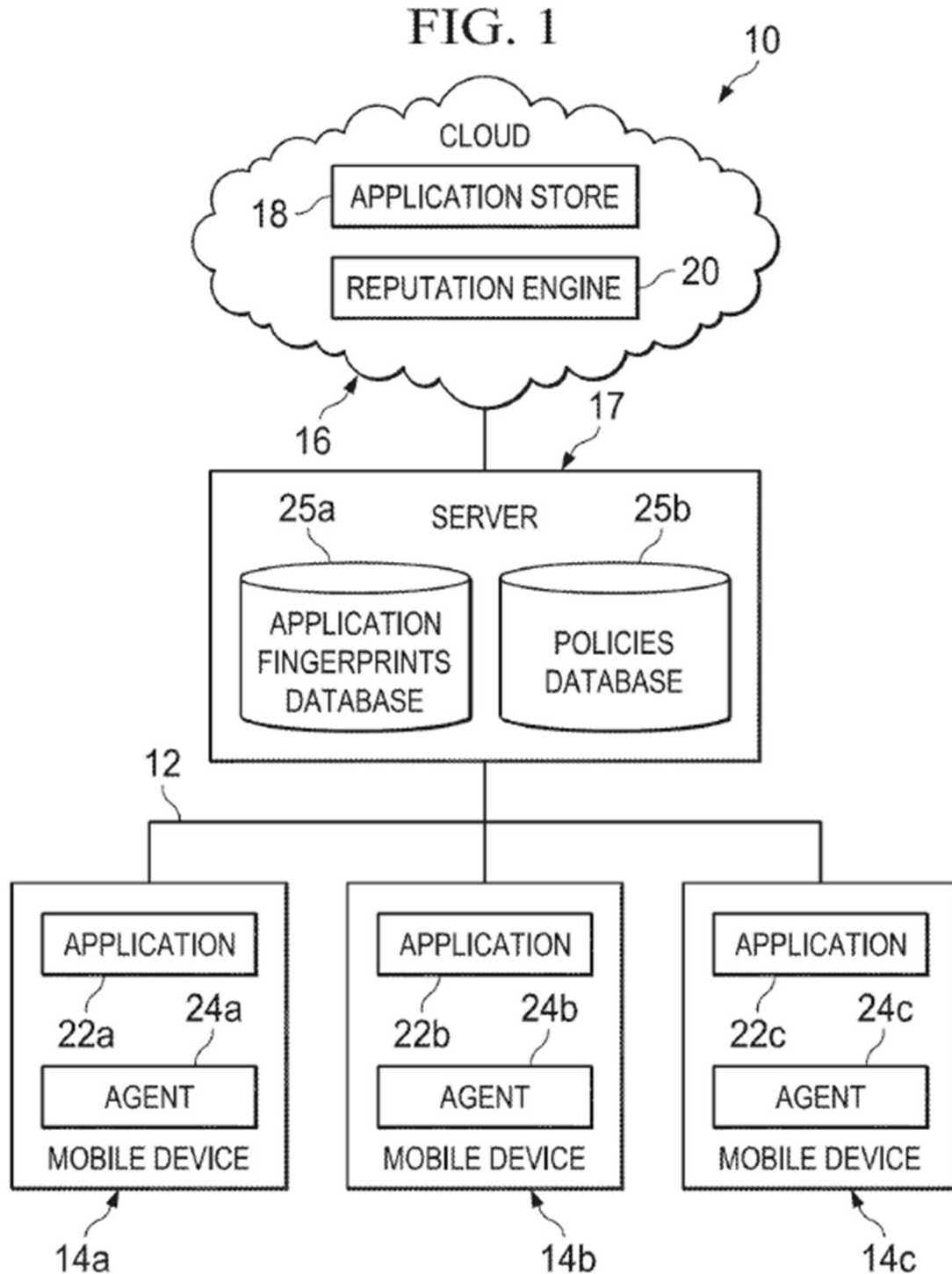
¹ This claim construction analysis is not a concession as to the scope of any claim term in litigation or a waiver of any argument in any proceeding that claim terms are indefinite, invalid, or unpatentable.

A. Overview of the Prior Art

1. Alperovitch (Ex. 1004)

Alperovitch was filed on March 21, 2012 and published on September 26, 2013, and is prior art under § 102(e). Ex. 1004, cover. Alperovitch is directed to a system and method for crowdsourcing of mobile application reputations that include “obtaining a collection of attributes of a mobile application, comparing one or more of the attributes with crowdsourced data associated with other mobile applications to determine one or more trustworthiness indicators, and calculating a reputation score based on the one or more trustworthiness indicators.” *Id.*, abstract. Alperovitch’s approach provides “effective control and management of applications on mobile devices within computer and communication network environments” that prevents problems related to “unrestricted access to mobile resources and application programming interfaces by applications of an unknown or untrusted origin [that] could result in damage to the user, the device, and the network.” *Id.*, [0002].

Alperovitch’s Figure 1 below depicts an example implementation of its system for crowdsourcing mobile application reputations.



Id., FIG. 1. “The exemplary environment illustrates a network 12 connecting one or more mobile devices 14a, 14b, and 14c with a cloud 16.” *Id.*, [0011]. Mobile devices 14a-c can include “mobile phones, smart mobile phones (smartphones), e-

book readers, tablets, iPads, personal digital assistants (PDAs), laptops or electronic notebooks, portable navigation systems, multimedia gadgets (e.g., cameras, video and/or audio players, etc.), gaming systems, other handheld electronic devices, and any other device, component, element, or object capable of initiating voice, audio, video, media, or data exchanges within system 10” of Figure 1. *Id.*

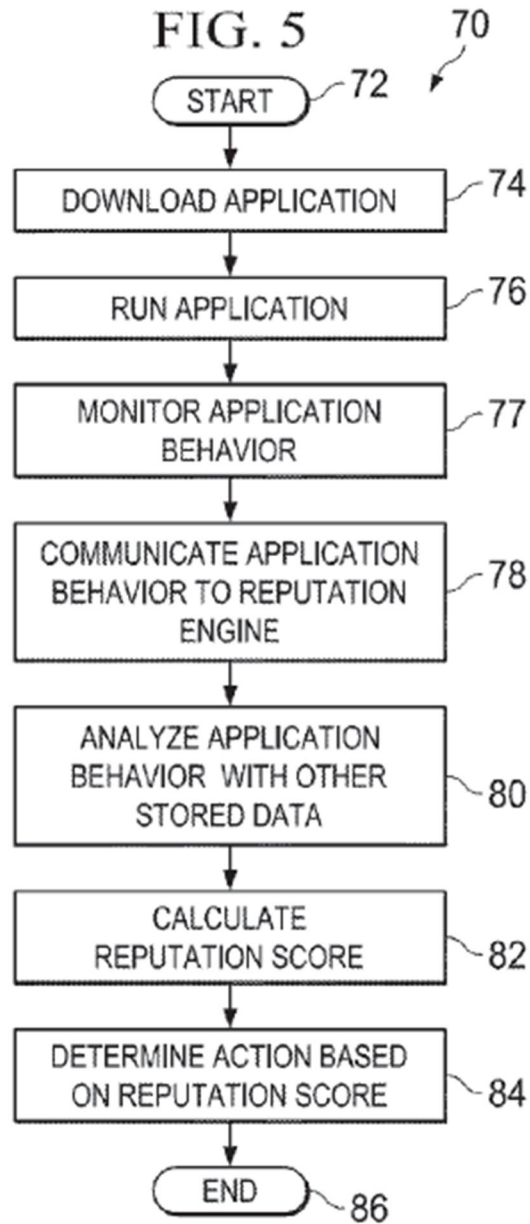
Mobile devices 14a-c are permitted to access mobile applications from one or more application stores 18 located in cloud 16. *Id.*, [0012]. Cloud 16 may also “comprise a reputation engine 20 for collecting and assessing mobile application reputations, also called herein as ‘reputation scores,’” where “[a] reputation score is a value (e.g., numeric, textual, pictorial, etc.) that denotes a relative level of trustworthiness of the mobile application on a spectrum (e.g., continuous or discrete) from benign (e.g., reputable) to malicious (e.g., non-reputable). Reputation score may indicate a probability that a mobile application is a malicious software. For example, mobile applications that have a high probability of being malicious may have a low reputation score.” *Id.*, [0013].

Alperovitch discloses that a reputation score can be calculated by a reputation engine based on many factors. *Id.*, [0021]-[0025]. In certain embodiments, the reputation engine “can calculate reputation scores for mobile applications from real-time activities and requests for resources of the mobile applications. Embodiments of the present disclosure can also enhance a reputation score for mobile applications

from real-time activities and requests for resources of the mobile applications.” *Id.*, [0053]. For instance, “[i]n an example embodiment, each installed application on a mobile device (e.g., 14a-c) may be queried in cloud 16 by reputation engine 20, which can return respective mobile application reputations calculated based on proliferation of the application, its capabilities and longevity, and potentially augmented by manual research analysis.” *Id.*, [0019]. Furthermore, “[i]n yet other example embodiments, the reputation score may be calculated based on capabilities of the mobile application. For example, an application may be assigned a lower reputation score if it asks for a large number of potentially abusable behavior permissions.” *Id.*, [0025].

Agents may be provisioned on each mobile device 14a, 14b, and 14c along with one or more mobile applications. *Id.*, [0014]. “Agents 24a-c may monitor behavior and activities of any one or more mobile applications (e.g., 22a-c) on respective mobile devices 14a-c. Agents 24a-c may also access policies stored on respective mobile devices 14a-c to determine if mobile applications 22a-c violate any policy.” *Id.* For example, “a mobile application that automatically, and without authorization, turns on a camera and a microphone (or other recording device) of a mobile device may be deemed to be malicious.” Ex. 1004, [0013].

Figure 5 below is a flow-chart illustrating example operational steps of Alperovitch’s system and method.



Id., FIG. 5.

As part of determining a mobile application's reputation, "application behavior (e.g., requests for resources and application actions) may be monitored" by the agent on the mobile device, and the "application behavior may be communicated to reputation engine 20." *Id.*, [0054]. Alperovitch discloses that "[a]pplication

behavior may include application requests (e.g., requests for mobile device resources, such as access to files and pictures stored on the mobile device, access to cameras and microphones, etc.) and application actions (e.g., actions initiated by the application, such as turning on the mobile device microphone and camera, initiating a network connection with a rogue IP address, starting a virtual game of cards, etc.).”

Id. After analyzing application behavior, “[r]eputation engine 20 may calculate a reputation score for application 22 in step 82. Calculation may be performed by any suitable means. ... [T]he calculated reputation score may be an updated (e.g., enhanced) reputation score.” *Id.*, [0055].

Moreover, a reputation score “may be classified into a plurality of categories,” e.g., by colors, based on the value of the reputation score. *Id.*, [0057]. “In an example embodiment, low reputation scores may be classified as low risk, and assigned a color green. Reputation scores reflecting an unverified status may be assigned a color yellow. Intermediate reputation scores may be classified as medium risk and assigned a color orange. High reputation scores may be classified as high risk and assigned a color red.” *Id.*

2. Yeh (Ex. 1005)

Yeh was filed on November 22, 2010 and issued on August 25, 2015, and is prior art under § 102(e). Ex. 1005, cover. Yeh is directed to malware detection by “cross-referencing host data on a trusted enterprise host computer to compare to a

suspect computer.” *Id.*, 1:6-9. Yeh discloses a computer network that “includes a central management computer linking at least one trusted host computer with at least one user computer. ... Antivirus software on the user computer screens for suspect activity or features and, if found, the suspect activity or features are compared to rules database.” *Id.*, abstract. Yeh further discloses that if suspect activity, features, or behaviors are “unresolved, the behaviors are compared against any of a number of white lists and known good behavior on the trusted [host] computer to determine if the activity matches that of the trusted computer. If there is no match, then a malware alert may be generated.” *Id.*, 2:7-11.

3. Chien (Ex. 1006)

Chien was filed on September 17, 2008 and issued on August 25, 2015, and is prior art under § 102(e). Ex. 1006, cover. Chien is directed to “[c]reating a policy to be used by a malware prevention system [that] uses multiple events triggered by malware.” *Id.*, abstract. Chien discloses that when a sample of malicious computer code or malware is executed in a computer system that is connected to a malware prevention system, “[e]vent data relating to multiple events caused by the malicious code executing on the computer system are captured and stored. The event data is configured using a specific property, such as process, that facilitates malware behavior analysis. A behavior list is created utilizing the multiple events and associated event data. The behavior list is then used, together with data in a malware

behavior database, to derive a policy for use in a malware prevention system.” *Id.*, 2:47-59.

B. Ground 1: Claims 1-24 Are Rendered Obvious by Alperovitch in View of the Knowledge of a POSITA

1. Claim 1

a. Preamble

The preamble of claim 1 recites “[a] *method for assessing runtime risk for an application program that executes on a device, comprising.*” To the extent the Board considers the preamble a limitation, Alperovitch discloses, teaches, or suggests this limitation. Alperovitch discloses that “[a] system and method in one embodiment includes modules for obtaining a collection of attributes of a mobile application, comparing one or more of the attributes with crowdsourced data associated with other mobile applications to determine one or more trustworthiness indicators, and calculating a reputation score based on the one or more trustworthiness indicators.” Ex. 1004, abstract. A POSITA would have understood that Alperovitch’s disclosed method executes on a device, as illustrated in, e.g., Figure 1 of Alperovitch. *Id.*, Fig. 1; *see also id.*, [0060] (“System 10 may be implemented in hardware or software, and may be used to assess mobile applications either remotely or locally.”); Ex. 1003, ¶60.

Alperovitch further explains that “[a] reputation score is a value (e.g., numeric, textual, pictorial, etc.) that denotes a relative level of trustworthiness of the

mobile application on a spectrum (e.g., continuous or discrete) from benign (e.g., reputable) to malicious (e.g., non-reputable). Reputation score may indicate a probability that a mobile application is a malicious software.” Ex. 1004, [0013]. Reputation scores for applications can be calculated “from real-time activities of and requests for resources of the ... applications,” and a POSITA would have understood that Alperovitch’s reputation scores are an assessment of runtime risk of application programs. *Id.*, [0053], [0057]; Ex. 1003, ¶61. Indeed, Alperovitch discloses that a reputation score “may be classified into a plurality of categories” based on the value of the reputation score. Ex. 1004, [0057]. “[L]ow reputation scores may be classified as low risk, and assigned a color green. Reputation scores reflecting an unverified status may be assigned a color yellow. Intermediate reputation scores may be classified as medium risk and assigned a color orange. High reputation scores may be classified as high risk and assigned a color red.” *Id.* Accordingly, Alperovitch discloses, teaches, or suggests this limitation. Ex. 1003, ¶¶61-62.

b. Limitation 1[a]

Claim 1 continues by reciting “*storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence.*” Alperovitch discloses, teaches, or suggests this limitation. Alperovitch teaches an application manifest database 32 as a rules database for storing a plurality of rules. “[A]pplication behavior may be aggregated into application manifest database 32 and/or real-time

data capture module 40. Data mining module 34 may then extract substantially all relevant information pertaining to application 22 from application manifest database 32 and real-time data capture module 40.” Ex. 1004, [0055]. A POSITA would have understood that application behaviors (which operate equivalent to rules in the ’517 patent, as explained below) are stored in the application manifest database when they are aggregated into the application manifest database. Ex. 1003, ¶63.

Alperovitch further discloses that “application behavior (e.g., requests for resources and application actions) may be monitored.” Ex. 1004, [0054]. A POSITA would have understood that the application behaviors that are monitored form the basis of rules in Alperovitch because the reputation engine analyzes data against the monitored application behaviors to determine a reputation score. Ex. 1003, ¶64; *see also, e.g.*, Ex. 1005, 5:47-49 (“A rules database 119 includes activities, behaviors, or other patterns of normal behavior that may occur within a user computer or over the network by the computer.”). “[R]eputation engine 20 may analyze the application behavior with other stored data (e.g., previously stored data crowdsourced from a plurality of sources) in application manifest database 32. ... In an example embodiment, data mining module 34 may extract comparable information from application manifest database 32 and/or real-time data capture module 40 for analyzing with application behavior. For example, data mining

module 34 may seek information to determine if similar actions have been requested in the past.” Ex. 1004, [0055]; Ex. 1003, ¶64. Furthermore, the ’517 patent only requires that a “rule identifies an action sequence” (Ex. 1001, Abstract, 1:48, 1:63-64, 4:12-14, 6:23-24, 8:61-63), which an application behavior does as well, as explained below. Thus, a POSITA would have understood that Alperovitch’s application behaviors that have been identified for monitoring and are thus monitored for are equivalent to rules in the ’517 patent. Ex. 1003, ¶64.

Moreover, Alperovitch provides a specific example scenario of a rule that identifies an action sequence to monitor for: “In one example scenario, a mobile application that automatically, and without authorization, turns on a camera and a microphone (or other recording device) of a mobile device may be deemed to be malicious.” Ex. 1004, [0013]. The exemplary rule here is whether a camera and a microphone (or other recording device) of a mobile device is automatically, without authorization, turned on, with the identified action sequence being the sequence of the two performed actions of turning on a camera and a microphone (or other recording device) of a mobile device. Ex. 1003, ¶65; *see also, e.g.*, Ex. 1005, 6:42-45 (“[Rules] Database 130 includes rules that ... describe behaviors of the user computer that are allowed and those behaviors that are not allowed.”).

In addition, as Alperovitch discloses, “[a]pplication behavior may include application requests (e.g., requests for mobile device resources, such as access to

files and pictures stored on the mobile device, access to cameras and microphones, etc.) and application actions (e.g., actions initiated by the application, such as turning on the mobile device microphone and camera, initiating a network connection with a rogue IP address, starting a virtual game of cards, etc.).” Ex. 1004, [0054]. Alperovitch further discloses that a reputation score is calculated based on one or more trustworthiness indicators (*id.*, abstract, [0010]), and “[t]rustworthiness indicators may include ... predefined combination of capabilities of the application (e.g., capabilities of the application being analyzed and other similar applications)” (*id.*, [0021]).

A POSITA would have understood that application behaviors are action sequences because the ’517 patent discloses that “the action sequence is a sequence of at least two performed actions.” Ex. 1001, Abstract, 1:56-57; *see also id.*, 4:12-17, 7:30-32; Ex. 1003, ¶67. A POSITA would have understood an application behavior in Alperovitch includes a sequence of two performed actions for at least two reasons. First, “[a]pplication behavior may include application requests ... and application actions,” which explicitly envisions more than a single application request or a single application action. Ex. 1004, [0054]; Ex. 1003, ¶67. Second, Alperovitch discloses that calculating the reputation score is based on trustworthiness indicators that are a predefined combination of capabilities of the application, which would also include a sequence of at least two performed

actions. Ex. 1004, [0021]; *see also id.*, [0014] (“Agents 24a-c may monitor ***behavior and activities*** of any one or more mobile applications (e.g., 22a-c) on respective mobile devices 14a-c.”) (emphasis added); Ex. 1003, ¶67. Indeed, Alperovitch discloses examples of actions sequences of at least two performed actions such as a sequence of requests for “access to files and pictures stored on the mobile device, access to cameras and microphones, etc.” or “turning on the mobile device microphone and camera.” Ex. 1004, [0054]; *see also id.*, [0013] (“[A] mobile application that automatically, and without authorization, turns on a camera and a microphone (or other recording device) of a mobile device may be deemed to be malicious. ... [A] mobile application that merely accesses the mobile device’s processor and memory to facilitate a game of cards may be deemed to be benign.”); Ex. 1003, ¶67. Accordingly, Alperovitch discloses, teaches, or suggests this limitation. Ex. 1003, ¶¶67.

c. Limitation 1[b]

Claim 1 continues by reciting “*storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules.*” Alperovitch discloses, teaches, or suggests this limitation. Alperovitch discloses that “[a]gents 24a-c may monitor behavior and activities of any one or more mobile applications (e.g., 22a-c) on respective mobile devices 14a-c. Agents 24a-c may also access policies stored on respective mobile devices

14a-c to determine if mobile applications 22a-c violate any policy.” Ex. 1004, [0014]. A POSITA would have understood that the policies stored on the mobile devices constitute a policy database. Ex. 1003, ¶69. Indeed, Alperovitch discloses a policy database on a server that holds other policies in Alperovitch’s system. “According to the embodiment illustrated in FIG. 1, server 17 may be provisioned with ... policies database 25b. ... FIG. 1 showing mobile devices 14a-c communicating with cloud 16 through server 17 is merely representative.” Ex. 1004, [0018]; *see also id.*, [0065] (“The information being tracked, sent, received, or stored in system 10 could be provided in any database, register, table, cache, queue, control list, or storage structure, based on particular needs and implementations.”); Ex. 1003, ¶69.

To the extent that Alperovitch is found not to disclose “storing, in a policy database,” use of such a database to store policies in Alperovitch would have been an obvious design choice for a POSITA practicing Alperovitch’s teachings. Use of a database in this context would have been one of a limited number of options for policy storage and would have been well within the level of skill of a POSITA such that a POSITA would have had a reasonable expectation of success of storing policies in a policy database. Ex. 1004, [0065] (“The information being tracked, sent, received, or stored in system 10 could be provided in any database”); Ex. 1003, ¶70.

Furthermore, as discussed above, the policy database in Alperovitch stores policies to determine if mobile applications 22a-c violate any policy (including a rule identifying an action sequence). “In one example scenario, a mobile application that automatically, and without authorization, turns on a camera and a microphone (or other recording device) of a mobile device may be deemed to be malicious.” Ex. 1004, [0013]. A POSITA would have understood this as an example of an assessment policy to determine if a mobile application is malicious, and it includes the rule of whether a camera and a microphone (or other recording device) of a mobile device are automatically, without authorization, turned on, with the identified action sequence of the sequence of the two performed actions of turning on a camera and a microphone (or other recording device) of a mobile device. Ex. 1003, ¶71; *see also e.g.*, Ex. 1004, [0013] (“[A] mobile application that merely accesses the mobile device’s processor and memory to facilitate a game of cards may be deemed to be benign.”), [0046] (“In an example scenario, mobile device 14 may be provisioned with a policy that applications on a network accessing pictures on mobile device 14 are not allowed to run.”).

d. Limitation 1[c]

Claim 1 continues by reciting “*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.” Alperovitch discloses, teaches, or suggests this limitation. In Alperovitch, the runtime risk (i.e., reputation score for the application) is identified (i.e., updated accordingly) using at least one assessment policy (i.e., policies including a rule (identifying an action sequence) stored on mobile devices to determine if mobile applications violate any policy). As an example, Alperovitch teaches that “an application on a particular mobile device may initiate a spying action. Real-time data capture module 40 may recognize the spying action and consequently, reputation engine 20 may calculate an updated reputation score for the application,” where spying may occur when “a mobile application on a mobile phone could be remotely controlled, and configured to turn on the phone’s camera and microphone, permitting spying.” Ex. 1004, [0044], [0030]; Ex. 1003, ¶73.

Moreover, Alperovitch discloses “the identified runtime risk indicates a risk or threat of the identified action sequence of the application.” As discussed above, “a mobile application that automatically, and without authorization, turns on a camera and a microphone (or other recording device) of a mobile device [i.e., spying] may be deemed to be malicious,” and the reputation score is updated accordingly. Ex. 1004, [0013], [0044]; Ex. 1003, ¶74. A “[r]eputation score may indicate a probability that a mobile application is a malicious software. For example, mobile applications that have a high probability of being malicious may

have a low reputation score. In one example scenario, a mobile application that automatically, and without authorization, turns on a camera and a microphone (or other recording device) of a mobile device may be deemed to be malicious.” Ex. 1004, [0013]. Thus, the identified runtime risk (i.e., a mobile application may be deemed to be malicious, and thus, have a low reputation score) indicates a risk or threat of the identified action sequence of the application (i.e., because a mobile application automatically, and without authorization, turns on a camera and a microphone (or other recording device)), which is against the provisioned policy. Ex. 1003, ¶74.

e. Limitation 1[d]

Claim 1 continues by reciting “*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.*” Alperovitch discloses, teaches, or suggests this limitation. In Alperovitch, the reputation engine, which has or is executed by a processor and thus is a processing device, *inter alia*, calculates reputation scores, and together with an agent on the mobile device work as a runtime monitor including a processing device. “[P]rocessor 36 and memory 38 may be provisioned on reputation engine 20 to facilitate calculation of mobile application reputations.” Ex. 1004, [0045]; *see id.*, [0051] (“Reputation engine 20

may calculate a reputation score for application 22 in step 62. Calculation may be performed by any suitable means.”); Ex. 1003, ¶76.

In addition, “[m]obile device 14 may be provisioned with agent 24 that tracks applications 22 and applicable policies 25. In an example embodiment, agent 24 may include event detection capabilities, communication interfaces, policy manager, etc. In another example embodiment, agent 24 may include software capable of communicating with reputation engine 20 and carrying out instructions from policy managers, event detection components, etc. Agent 24 may be configured to receive queries or information from reputation engine 20.” Ex. 1004, [0040]; *see also id.*, [0014] (“Agents 24a-c may monitor behavior and activities of any one or more mobile applications (e.g., 22a-c) on respective mobile devices 14a-c.”). Moreover, “agent 24 on mobile device 14 may monitor the application behavior and communicate it to real-time data capture module 40 in reputation engine 20.” *Id.*, [0054]. A POSITA would have understood that an agent on the mobile device that is tracking and monitoring behavior and activities of applications on the mobile device is providing runtime monitoring because it is keeping up-to-date with runtime changes on the mobile device. Ex. 1003, ¶77.

Alperovitch further teaches that the reputation score is based on aspects of the application’s behavior. Ex. 1004, [0054] (“[A]gent 24 on mobile device 14 may monitor the application behavior and communicate it to real-time data capture

module 40 in reputation engine 20”); [0054] (“[A]pplication behavior (e.g., requests for resources and application actions) may be monitored”); Ex. 1003, ¶78. The reputation score calculated by the reputation engine “may be classified into a plurality of categories. In an example embodiment, low reputation scores may be classified as low risk, and assigned a color green. Reputation scores reflecting an unverified status may be assigned a color yellow. Intermediate reputation scores may be classified as medium risk and assigned a color orange. High reputation scores may be classified as high risk and assigned a color red. ... The colors are provided for illustrative purposes only. Any other classification labels, means, schemes and methods may be used without changing the scope of the present disclosure.” Ex. 1004, [0057]. A POSITA would have understood that Alperovitch teaches that the runtime monitor including a processing device (i.e., reputation engine and agent) identifies a behavior score for the application program that executes on the device (e.g., a risk category denoted by color) based on the identified runtime risk (i.e., reputation score of the mobile application). Ex. 1003, ¶78. The ’517 patent discloses that “[t]he behavior score may be a number or other value (e.g., a rating)” (Ex. 1001, 6:35-36), and a POSITA would have understood that Alperovitch’s risk category denoted by color is equivalent to “a rating.” Ex. 1003, ¶78.

f. Limitation 1[e]

Claim 1 continues by reciting “*the action sequence is a sequence of at least two performed actions.*” Alperovitch discloses, teaches, or suggests this limitation for the reasons explained above for Limitation 1[a]. *See supra* §V.B.1.b; Ex. 1003, ¶¶80-82.

g. Limitation 1[f]

Claim 1 continues by reciting “*each performed action is at least one of: a user action, an application action, and a system action.*” Alperovitch discloses, teaches, or suggests this limitation. As discussed above for Limitation 1[e], Alperovitch teaches that performed actions include “application requests (e.g., requests for mobile device resources, such as access to files and pictures stored on the mobile device, access to cameras and microphones, etc.) and application actions (e.g., actions initiated by the application, such as turning on the mobile device microphone and camera, initiating a network connection with a rogue IP address, starting a virtual game of cards, etc.).” Ex. 1004, [0054]. A POSITA would have understood that Alperovitch’s application requests and application actions, e.g., requests for mobile device resources, such as access to files and pictures stored on the mobile device, access to cameras and microphones, etc., and other actions initiated by the application, are application actions as disclosed in the ’517 patent. *See* Ex. 1001, 9:18-21 (“The application action 304 may be any

activity performed by the application initiated programmatically by a task in execution of the computing system 100.”); Ex. 1003, ¶¶83-84. Furthermore, a POSITA would have understood that application actions described in Alperovitch include system actions performed by the computing system, e.g., as a result of application actions (“as a consequence of, an application or user action that changes the state of the computing system” (Ex. 1001, 7:17-19)), such as the mobile device’s processor turning on the mobile device microphone and camera, initiating a network connection with a rogue IP address, starting a virtual game of cards, etc. Ex. 1003, ¶¶83-84.

In addition, Alperovitch also teaches a performed action that is a user action. Alperovitch discloses actions similar to the ’517 patent’s “program launch” (Ex. 1001, 6:58), such as “the fact that a user chose to download and install an application could be a tacit assertion by the user that the application is trustworthy and desirable” (Ex. 1004, [0023]), and “a user may provide permission to reputation engine 20 to access mobile device 14” (*id.*, [0041]). *See also id.*, [0036] (“Not shown in system 10 of FIG. 1 is hardware that may be suitably coupled to reputation engine 20 in the form of consoles, user interfaces.”). A user choosing to download and install an application and a user providing permission to the reputation engine to access the mobile device are examples of user actions. Ex. 1003, ¶¶83, 85.

2. Claim 2

Claim 2 depends on claim 1 and further recites: “*wherein the user action is any form of explicit input from a user of a computing system.*” Alperovitch discloses, teaches, or suggests this limitation. As explained above for Limitation 1[f], Alperovitch discloses, teaches, or suggests user actions. Alperovitch discloses “the fact that a user chose to download and install an application could be a tacit assertion by the user that the application is trustworthy and desirable” (Ex. 1004, [0023]), and “a user may provide permission to reputation engine 20 to access mobile device 14” (*id.*, [0041]). *See also id.*, [0036] (“Not shown in system 10 of FIG. 1 is hardware that may be suitably coupled to reputation engine 20 in the form of consoles, user interfaces.”). A POSITA would have understood that a user choosing to download and install an application and a user providing permission to the reputation engine to access the mobile device are examples of user actions that are forms of explicit input, e.g., through a user interface, from a user of a computing system because a user has to provide an input to initiate the downloading and installation of an application, and a user has to provide an input to grant permission to the reputation engine to access the mobile device. Ex. 1003, ¶106.

To the extent Alperovitch is found not to explicitly disclose this limitation, it would have been obvious in view of Alperovitch. Alperovitch discloses that agent

24 tracks applications and has event detection capabilities. Ex. 1004, [0040]. A POSITA would have understood that in the context of Alperovitch's focus on mobile applications, this would include detecting explicit inputs from a user. It would have been an obvious design variation of Alperovitch's teachings to include explicit user inputs as part of the performed actions monitored in mobile applications, as it was well-known that user inputs can control an application's behavior, which is the core focus of Alperovitch's monitoring and the basis for Alperovitch's computation of a reputation score. Ex. 1003, ¶107.

3. Claim 3

Claim 3 depends on claim 1 and further recites: "*wherein the application action is any activity performed by the application initiated programmatically by a task in execution of a computing system.*" Alperovitch discloses, teaches, or suggests this limitation. For example, Alperovitch teaches that an application can perform an application action, which includes "actions initiated by the application, such as turning on the mobile device microphone and camera, initiating a network connection with a rogue IP address, starting a virtual game of cards, etc." Ex. 1004, [0054]. A POSITA would have understood that the activity of, e.g., turning on of the mobile device microphone and camera performed by the application is initiated programmatically by a task in execution of a computing system in response to the application's "request[] for mobile device resources, such as ...

access to cameras and microphones.” Ex. 1004, [0054]; Ex. 1003, ¶110. In other words, the application’s request for access to cameras and microphones causes a task in execution of the computing system to initiate programmatically the turning on of the mobile device microphone and camera. Ex. 1003, ¶110.

4. Claim 4

Claim 4 depends on claim 1 and further recites: “*wherein the system action is any operation performed by a computing system on behalf of, or as a consequence of, a user action or application action that changes the state of the computing system.*” Alperovitch discloses, teaches, or suggests this limitation. Alperovitch discloses an application action that includes “requests for mobile device resources, such as ... access to cameras and microphones.” Ex. 1004, [0054]. A POSITA would have understood that as a consequence of such application action, which changes the state of the computing system because a request to change the state of a computing resource is being made (i.e., the mobile device microphone and camera is off at the moment), the system action of turning on the mobile device microphone and camera (or at least allowing access to these devices by the application) is performed by the computing system (i.e., the mobile device’s processor). Ex. 1003, ¶113.

5. Claim 5

Claim 5 depends on claim 1 and further recites: “*wherein a first action of the at least two performed actions is performed at a first time, and the second action of the at least two performed actions is performed at a second time.*” Alperovitch discloses, teaches, or suggests this limitation. Alperovitch teaches two performed actions, e.g., “requests for mobile device resources, such as ... access to cameras and microphones” and “actions initiated by the application, such as turning on the mobile device microphone and camera.” Ex. 1004, [0054]. A POSITA would have understood that requesting access to cameras and microphones is a first action performed at a first time, and then turning on the mobile device microphone and camera would be the second action performed at a second time because the mobile device microphone and camera would not need to be turned on until after there has been a request to access the cameras and microphones, and there would be no need to request access to the cameras and microphones if the cameras and microphones are already turned on. Ex. 1003, ¶¶115-116.

6. Claim 6

a. Limitation 6[a]

Claim 6 depends on claim 5 and further recites, among other things: “*wherein the first action is a user action.*” Alperovitch discloses, teaches, or suggests this limitation. As discussed above for claim 2, Alperovitch teaches an example of a user action where “a user may provide permission to reputation

engine 20 to access mobile device 14.” Ex. 1004, [0041]. A POSITA would have understood that a user providing permission to the reputation engine to access the mobile device is a first action that is a user action because a user has to provide an input to grant permission to the reputation engine to access the mobile device. Ex. 1003, ¶119.

b. Limitation 6[b]

Claim 6 continues by reciting “*the second action is a system action.*”

Alperovitch discloses, teaches, or suggests this limitation. As discussed above for Limitation 1[f], Alperovitch discloses “application actions (e.g., actions initiated by the application, such as turning on the mobile device microphone and camera, initiating a network connection with a rogue IP address, starting a virtual game of cards, etc.)” (Ex. 1004, [0054]), which a POSITA would have understood include system actions performed by the computing system, e.g., as a result of application actions (“as a consequence of, an application or user action that changes the state of the computing system” (Ex. 1001, 7:17-19)), such as the mobile device’s processor turning on the mobile device microphone and camera, initiating a network connection with a rogue IP address, starting a virtual game of cards, etc. Ex. 1003, ¶121. The mobile device’s processor turning on the mobile device microphone and camera is a second action that is a system action. *Id.*

c. Limitation 6[c]

Claim 6 continues by reciting “*the second time occurs after the first time.*” Alperovitch discloses, teaches, or suggests this limitation. A POSITA would have understood that to be part of the reputation engine’s calculated reputation score, the second action performed at the second time (i.e., the mobile device’s processor turning on the mobile device microphone and camera) would have to occur after the first action performed at the first time (i.e., after the user has provided permission to the reputation engine to access the mobile device). Ex. 1003, ¶123. A POSITA would have understood that the reputation engine needs to be provided permission to access the mobile device in order to calculate a reputation score, and if the user has not provided permission to the reputation engine to access the mobile device first, any actions by the mobile device cannot be part of the reputation score calculation. *Id.*

7. Claim 7

a. Limitation 7[a]

Claim 7 depends on claim 5 and further recites, among other things: “*wherein the first action is a user action.*” Alperovitch discloses, teaches, or suggests Limitation 7[a] for the same reasons discussed above for Limitation 6[a]. *See supra* § V.B.6.a; Ex. 1003, ¶¶127-128.

b. Limitation 7[b]

Claim 7 continues by reciting “*the second action is an application action.*” As discussed above for Limitation 1[f], Alperovitch discloses “application requests (e.g., requests for mobile device resources, such as access to files and pictures stored on the mobile device, access to cameras and microphones, etc.)” (Ex. 1004, [0054]), which a POSITA would have understood is an application action, such as an application’s request for access to the mobile device’s cameras and microphones. Ex. 1003, ¶129. The application’s request for access to the mobile device’s cameras and microphones is a second action. *Id.*

c. Limitation 7[c]

Claim 7 continues by reciting “*the second time occurs after the first time.*” A POSITA would have understood that to be part of the reputation engine’s calculated reputation score, the second action performed at the second time (i.e., the application’s request for access to the mobile device’s cameras and microphones) would have to occur after the first action performed at the first time (i.e., after the user has provided permission to the reputation engine to access the mobile device). Ex. 1003, ¶131. A POSITA would have understood that the reputation engine needs to be provided permission to access the mobile device in order to calculate a reputation score, and if the user has not provided permission to

the reputation engine to access the mobile device first, any actions by the mobile device cannot be part of the reputation score calculation. *Id.*

8. Claim 8

a. Limitation 8[a]

Claim 8 depends on claim 5 and further recites, among other things:

“wherein the first action is an application action.” Alperovitch discloses, teaches, or suggests this limitation. As discussed above for Limitation 1[f], Alperovitch discloses “application requests (e.g., requests for mobile device resources, such as access to files and pictures stored on the mobile device, access to cameras and microphones, etc.)” (Ex. 1004, [0054]), which a POSITA would have understood is an application action, such as an application’s request for access to the mobile device’s cameras and microphones. Ex. 1003, ¶135. The application’s request for access to the mobile device’s cameras and microphones is a first action. *Id.*

b. Limitation 8[b]

Claim 8 continues by reciting *“the second action is a system action.”* Alperovitch discloses, teaches, or suggests Limitation 8[b] for the same reasons discussed above for Limitation 6[b]. *See supra* § V.B.6.b; Ex. 1003, ¶¶137-138.

c. Limitation 8[c]

Claim 8 continues by reciting *“the second time occurs after the first time.”* Alperovitch discloses, teaches, or suggests this limitation. A POSITA would have understood that the second action performed at the second time (i.e., the mobile

device's processor turning on the mobile device microphone and camera) would have occurred after the first action performed at the first time (i.e., after the application's request for access to the mobile device's cameras and microphones) because the mobile device microphone and camera would not need to be turned on until after there has been a request to access the cameras and microphones, and there would be no need to request access to the cameras and microphones if the cameras and microphones are already turned on. Ex. 1003, ¶139.

9. Claim 9

a. Limitation 9[a]

Claim 9 depends on claim 1 and further recites, among other things:

“wherein the action sequence includes three performed actions.” Alperovitch discloses, teaches, or suggests this limitation. Alperovitch teaches an example of a performed action where “a user may provide permission to reputation engine 20 to access mobile device 14.” Ex. 1004, [0041]. Alperovitch further teaches examples of performed actions that include “application requests (e.g., requests for mobile device resources, such as access to files and pictures stored on the mobile device, access to cameras and microphones, etc.) and application actions (e.g., actions initiated by the application, such as turning on the mobile device microphone and camera, initiating a network connection with a rogue IP address, starting a virtual game of cards, etc.).” Ex. 1004, [0054]. Thus, Alperovitch discloses, teaches, or

suggests the action sequence includes three performed actions, such as providing permission to the reputation engine to access the mobile device, an application's request for access to the mobile device's cameras and microphones, and the mobile device's processor turning on the mobile device microphone and camera. Ex. 1003, ¶143.

b. Limitation 9[b]

Claim 9 continues by reciting “*a first action of the three performed actions is a user action.*” Alperovitch discloses, teaches, or suggests this limitation. As discussed above, Alperovitch teaches an example of a user action where “a user may provide permission to reputation engine 20 to access mobile device 14.” Ex. 1004, [0041]. A POSITA would have understood that a user providing permission to the reputation engine to access the mobile device is a first action of the three performed actions that is a user action because a user has to provide an input to grant permission to the reputation engine to access the mobile device. Ex. 1003, ¶145.

c. Limitation 9[c]

Claim 9 continues by reciting “*a second action of the three performed actions is an application action.*” Alperovitch discloses, teaches, or suggests this limitation. As discussed above, Alperovitch discloses “application requests (e.g., requests for mobile device resources, such as access to files and pictures stored on

the mobile device, access to cameras and microphones, etc.)” (Ex. 1004, [0054]), which a POSITA would have understood is an application action, such as an application’s request for access to the mobile device’s cameras and microphones. Ex. 1003, ¶147. The application’s request for access to the mobile device’s cameras and microphones is a second action of the three performed actions that is an application action. *Id.*

d. Limitation 9[d]

Claim 9 continues by reciting “*a third action of the three performed actions is a system action.*” Alperovitch discloses, teaches, or suggests this limitation. As discussed above, Alperovitch discloses “application actions (e.g., actions initiated by the application, such as turning on the mobile device microphone and camera, initiating a network connection with a rogue IP address, starting a virtual game of cards, etc.)” (Ex. 1004, [0054]), which a POSITA would have understood include a system action performed by the computing system, e.g., as a result of application actions (“as a consequence of, an application or user action that changes the state of the computing system” (Ex. 1001, 7:17-19)), such as the mobile device’s processor turning on the mobile device microphone and camera. Ex. 1003, ¶149. The mobile device’s processor turning on the mobile device microphone and camera is a third action of the three performed actions that is a system action. *Id.*

e. Limitation 9[e]

Claim 9 continues by reciting “*the second action is performed temporally after the first action.*” Alperovitch discloses, teaches, or suggests this limitation. A POSITA would have understood that to be part of the reputation engine’s calculated reputation score, the second action would have to be performed temporally after the first action, i.e., the application’s request for access to the mobile device’s cameras and microphones would have to occur after the user has provided permission to the reputation engine to access the mobile device. Ex. 1003, ¶151. A POSITA would have understood that the reputation engine needs to be provided permission to access the mobile device in order to calculate a reputation score, and if the user has not provided permission to the reputation engine to access the mobile device first, any actions by the mobile device cannot be part of the reputation score calculation. *Id.*

f. Limitation 9[f]

Claim 9 continues by reciting “*the third action is performed temporally after the second action.*” Alperovitch discloses, teaches, or suggests this limitation. A POSITA would have understood that the third action (i.e., the mobile device’s processor turning on the mobile device microphone and camera) would have to be performed temporally after the second action (i.e., after the application’s request for access to the mobile device’s cameras and microphones) because the mobile

device microphone and camera would not need to be turned on until after there has been a request to access the cameras and microphones, and there would be no need to request access to the cameras and microphones if the cameras and microphones are already on. Ex. 1003, ¶153.

10. Claim 10

Claim 10 depends on claim 1 and further recites: “*wherein the runtime risk is identified based on matching rules and probabilistic weights and scores of performed actions on the device.*” Alperovitch discloses, teaches, or suggests this limitation. Alperovitch discloses that “[a]n overall reputation score may be determined based upon the calculated probabilities and provided to agent 24a on mobile device 14a.” Ex. 1004, [0035]. The calculated probabilities include “aggregated behaviors of the application that may also be evaluated to determine a reputation score of the mobile application. As more information about an application is reported or otherwise made available to reputation engine 20, a statistical confidence level of the reputation score may be higher.” *Id.*, [0034]. Thus, Alperovitch teaches that the runtime risk (i.e., reputation score) is identified based on matching rules and probabilistic weights and scores of performed actions on the device (i.e., determined based on aggregating monitored application behaviors to increase the confidence level of the reputation score). Ex. 1003, ¶157. A POSITA would have understood that increasing the statistical confidence level

by aggregating monitored application behaviors is equivalent to matching probabilistic weights and scores of the application behaviors because it is taking into account the probability of the application behaviors occurring to increase the statistical confidence level of the reputation score. *Id.*

11. Claim 11

Claim 11 depends on claim 1 and further recites: “*wherein the runtime risk is identified based on time proximity of the at least two performed actions of the action sequence and natural affinity inferred between the at least two performed actions.*” Alperovitch discloses, teaches, or suggests this limitation. Alperovitch discloses that “the reputation score may be calculated based on capabilities of the mobile application” that include “identify[ing] unusual combinations of permissions, or unexpected permissions (e.g., a purported game application sending unauthorized SMS messages).” Ex. 1004, [0025]. A POSITA would have understood that when, e.g., a purported game application is running, and the purported game application sends an unauthorized SMS message, the application is performing an action sequence where the time proximity of the at least two performed actions of running the game application and then sending an unauthorized SMS message as well as the natural affinity inferred between the at least two performed actions are unexpected. Ex. 1003, ¶160. Thus, Alperovitch teaches that the runtime risk (i.e., reputation score) is identified (i.e., calculated)

based on the unexpected time proximity of running the game application and then sending an unauthorized SMS message because an SMS message is not expected to be sent while running the game application and based on the unnatural affinity inferred between running the game application and then sending an unauthorized SMS message for the same reason. *Id.*

12. Claim 12

a. Limitation 12[a]

Claim 12 depends on claim 1 and further recites: “*further comprising: assessing, by the processing device, that the at least two performed actions of the action sequence describe a forensic chain of events based on a plurality of factors.*” Alperovitch discloses, teaches, or suggests this limitation. Alperovitch discloses that “the reputation score may be calculated based on capabilities of the mobile application” (Ex. 1004, [0025]), including a “predefined combination of capabilities of the application (e.g., capabilities of the application being analyzed and other similar applications)” (*id.*, [0021]). Moreover, unauthorized or unusual combinations of performed actions by the application is reflected in the calculated reputation score. For example, “a mobile application that automatically, and without authorization, turns on a camera and a microphone (or other recording device) of a mobile device may be deemed to be malicious” (*id.*, [0013]), and “unusual combinations of permissions, or unexpected permissions (e.g., a

purported game application sending unauthorized SMS messages)” of an application may cause the application to receive a lower reputation score (*id.*, [0025]). Ex. 1003, ¶163. A POSITA would have understood that in calculating the reputation score, the reputation engine and agent are assessing that the at least two performed actions of the action sequence are describing a forensic chain of events based on a plurality of factors because the above examples are a forensic chain of events (i.e., the above performed actions of the action sequence are investigated together as a chain of events, such as turning on a camera and a microphone (or other recording device) of a mobile device or running a purported game application and sending unauthorized SMS messages) based on a plurality of factors, as explained below for Limitation 12[b]. *Id.*

b. Limitation 12[b]

Claim 12 continues by reciting “*wherein the plurality of factors includes at least one of: ordered sequences, unordered sequences, proximity analysis, outliers, probabilistic weights and scores, and probable action inferences based on an application's competency.*” Alperovitch discloses, teaches, or suggests this limitation. Alperovitch teaches that the assessing of the at least two performed actions of the action sequence describe a forensic chain of events that is based on at least one of ordered sequences, unordered sequences, proximity analysis, outliers, probabilistic weights and scores, and probable action inferences based on

an application's competency. For example, Alperovitch discloses that "the reputation score may be calculated based on capabilities of the mobile application" (Ex. 1004, [0025]), including a "predefined combination of capabilities of the application (e.g., capabilities of the application being analyzed and other similar applications)" (*id.*, [0021]). A POSITA would have understood that predefined combinations of capabilities of the application is a forensic chain of events that is based on ordered sequences, as the capabilities of an application performed in a predefined combination is an ordered sequence. Ex. 1003, ¶165.

Further, Alperovitch discloses that "[i]n one example scenario, a mobile application that automatically, and without authorization, turns on a camera and a microphone (or other recording device) of a mobile device may be deemed to be malicious." Ex. 1004, [0013]. A POSITA would have understood that an application turning on a camera and a microphone (or other recording device) of a mobile device without authorization is a forensic chain of events that is based on unordered sequences because turning on separate recording devices without authorization is not following a proper order of sequences. Ex. 1003, ¶166.

Moreover, Alperovitch discloses that "[i]n yet other example embodiments, the reputation score may be calculated based on capabilities of the mobile application. For example, an application may be assigned a lower reputation score if it asks for a large number of potentially abusable behavior permissions." Ex.

1004, [0025]. Such an action sequence consisting of unusual combinations of permissions, or unexpected permissions may be, e.g., running a purported game application and sending unauthorized SMS messages. *Id.* A POSITA would have understood that running a purported game application and sending unauthorized SMS messages is a forensic chain of events that is based on unordered sequences, proximity analysis, outliers, and probable action inferences based on an application's competency. Ex. 1003, ¶167. Running a purported game application and sending unauthorized SMS messages is a forensic chain of events that is based on unordered sequences because running a purported game application and sending SMS messages without authorization is not following a proper order of sequences. *Id.* Running a purported game application and sending unauthorized SMS messages is a forensic chain of events that is based on proximity analysis and probable action inferences based on an application's competency for the same reasons discussed above for claim 11. *See supra* § V.B.11; Ex. 1003, ¶167. This example is also based on outliers because it is outlier behavior (unexpected) for a purported gaming application that is running properly to send unauthorized SMS messages. Ex. 1003, ¶167.

Finally, Alperovitch discloses that “[a]n overall reputation score may be determined based upon the calculated probabilities and provided to agent 24a on mobile device 14a.” Ex. 1004, [0035]. The calculated probabilities include

“aggregated behaviors of the application that may also be evaluated to determine a reputation score of the mobile application. As more information about an application is reported or otherwise made available to reputation engine 20, a statistical confidence level of the reputation score may be higher.” *Id.*, [0034]. A POSITA would have understood that increasing the statistical confidence level by aggregating monitored application behaviors is equivalent to assessing that the at least two performed actions of the action sequence describe a forensic chain of events based on probabilistic weights and scores because the reputation engine and agent are assessing the probability of the application behaviors occurring to increase the statistical confidence level of the reputation score. Ex. 1003, ¶168.

13. Claim 13

a. Preamble

The preamble of claim 13 recites “[a] *system for assessing runtime risk for an application program that executes on a device, comprising.*” To the extent the Board considers the preamble a limitation, Alperovitch discloses, teaches, or suggests the preamble of claim 13 for the same reasons discussed above for the preamble of claim 1. *See supra* § V.B.1.a; Ex. 1003, ¶¶87-88.

b. Limitation 13[a]

Claim 13 continues by reciting “*a rules database storing a plurality of rules, wherein each rule identifies an action sequence.*” Alperovitch discloses, teaches,

or suggests Limitation 13[a] for the same reasons discussed above for Limitation 1[a]. *See supra* § V.B.1.b; Ex. 1003, ¶¶89-90.

c. Limitation 13[b]

Claim 13 continues by reciting “*a policy database storing a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules.*” Alperovitch discloses, teaches, or suggests Limitation 13[b] for the same reasons discussed above for Limitation 1[b]. *See supra* § V.B.1.c; Ex. 1003, ¶¶91-92.

d. Limitation 13[c]

Claim 13 continues by reciting “*a runtime monitor including a processing device.*” Alperovitch discloses, teaches, or suggests this limitation. In Alperovitch, the reputation engine, which has or is executed by a processor and thus is a processing device, *inter alia*, calculates reputation scores, and together with an agent on the mobile device work as a runtime monitor including a processing device. “[P]rocessor 36 and memory 38 may be provisioned on reputation engine 20 to facilitate calculation of mobile application reputations.” Ex. 1004, [0045]; *see id.*, [0051] (“Reputation engine 20 may calculate a reputation score for application 22 in step 62. Calculation may be performed by any suitable means.”). Ex. 1003, ¶93.

In addition, “[m]obile device 14 may be provisioned with agent 24 that tracks applications 22 and applicable policies 25. In an example embodiment, agent 24 may include event detection capabilities, communication interfaces, policy manager, etc. In another example embodiment, agent 24 may include software capable of communicating with reputation engine 20 and carrying out instructions from policy managers, event detection components, etc. Agent 24 may be configured to receive queries or information from reputation engine 20.” Ex. 1004, [0040]; *see also id.*, [0014] (“Agents 24a-c may monitor behavior and activities of any one or more mobile applications (e.g., 22a-c) on respective mobile devices 14a-c.”). Moreover, “agent 24 on mobile device 14 may monitor the application behavior and communicate it to real-time data capture module 40 in reputation engine 20.” *Id.*, [0054]. A POSITA would have understood that an agent on the mobile device that is tracking and monitoring behavior and activities of applications on the mobile device is providing runtime monitoring because it is keeping up-to-date with runtime changes on the mobile device. Ex. 1003, ¶94.

e. Limitation 13[d]

Claim 13 continues by reciting “*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.*” Alperovitch discloses, teaches, or suggests

Limitation 13[d] for the same reasons discussed above for Limitation 1[c]. *See supra* § V.B.1.d; Ex. 1003, ¶¶96-97.

f. Limitation 13[e]

Claim 13 continues by reciting “*identifying a behavior score for the application program that executes on the device based on the identified runtime risk.*” Alperovitch discloses, teaches, or suggests Limitation 13[e] for the same reasons discussed above for Limitation 1[d]. *See supra* § V.B.1.e; Ex. 1003, ¶¶78, 98.

g. Limitation 13[f]

Claim 13 continues by reciting “*the action sequence is a sequence of at least two performed actions.*” Alperovitch discloses, teaches, or suggests Limitation 13[f] for the same reasons discussed above for Limitation 1[e]. *See supra* § V.B.1.f; Ex. 1003, ¶¶100-101.

h. Limitation 13[g]

Claim 13 continues by reciting “*each performed action is at least one of: a user action, an application action, and a system action.*” Alperovitch discloses, teaches, or suggests Limitation 13[g] for the same reasons discussed above for Limitation 1[f]. *See supra* § V.B.1.g; Ex. 1003, ¶¶102-103.

14. Claim 14

Claim 14 depends on claim 13 and further recites: “*wherein the user action is any form of explicit input from a user of a computing system.*” Alperovitch

discloses, teaches, or suggests claim 14 for the same reasons discussed above for claim 2. *See supra* § V.B.2; Ex. 1003, ¶¶105-108.

15. Claim 15

Claim 15 depends on claim 13 and further recites: “*wherein the application action is any activity performed by the application initiated programmatically by a task in execution of a computing system.*” Alperovitch discloses, teaches, or suggests claim 15 for the same reasons discussed above for claim 3. *See supra* § V.B.3; Ex. 1003, ¶¶109-111.

16. Claim 16

Claim 16 depends on claim 13 and further recites: “*wherein the system action is any operation performed by a computing system on behalf of, or as a consequence of, a user action or application action that changes the state of the computing system.*” Alperovitch discloses, teaches, or suggests claim 16 for the same reasons discussed above for claim 4. *See supra* § V.B.4; Ex. 1003, ¶¶112-114.

17. Claim 17

Claim 17 depends on claim 13 and further recites: “*wherein a first action of the at least two performed actions is performed at a first time, and the second action of the at least two performed actions is performed at a second time.*” Alperovitch discloses, teaches, or suggests claim 17 for the same reasons discussed above for claim 5. *See supra* § V.B.5; Ex. 1003, ¶¶115-117.

18. Claim 18

a. Limitation 18[a]

Claim 18 depends on claim 17 and further recites: “*wherein the first action is a user action.*” Alperovitch discloses, teaches, or suggests Limitation 18[a] for the same reasons discussed above for Limitation 6[a]. *See supra* § V.B.6.a; Ex. 1003, ¶¶119-120.

b. Limitation 18[b]

Claim 18 continues by reciting “*the second action is a system action.*” Alperovitch discloses, teaches, or suggests Limitation 18[b] for the same reasons discussed above for Limitation 6[b]. *See supra* § V.B.6.b; Ex. 1003, ¶¶121-122.

c. Limitation 18[c]

Claim 18 continues by reciting “*the second time occurs after the first time.*” Alperovitch discloses, teaches, or suggests Limitation 18[c] for the same reasons discussed above for Limitation 6[c]. *See supra* § V.B.6.c; Ex. 1003, ¶¶123-124.

19. Claim 19

a. Limitation 19[a]

Claim 19 depends on claim 17 and further recites: “*wherein the first action is a user action.*” Alperovitch discloses, teaches, or suggests Limitation 19[a] for the same reasons discussed above for Limitation 6[a]. *See supra* § V.B.6.a; Ex. 1003, ¶¶127-128.

b. Limitation 19[b]

Claim 19 continues by reciting “*the second action is an application action.*” Alperovitch discloses, teaches, or suggests Limitation 19[b] for the same reasons discussed above for Limitation 7[b]. *See supra* § V.B.7.b; Ex. 1003, ¶¶129-130.

c. Limitation 19[c]

Claim 19 continues by reciting “*the second time occurs after the first time.*” Alperovitch discloses, teaches, or suggests Limitation 19[c] for the same reasons discussed above for Limitation 7[c]. *See supra* § V.B.7.c; Ex. 1003, ¶¶131-132.

20. Claim 20

a. Limitation 20[a]

Claim 20 depends on claim 17 and further recites: “*wherein the first action is an application action.*” Alperovitch discloses, teaches, or suggests Limitation 20[a] for the same reasons discussed above for Limitation 8[a]. *See supra* § V.B.8.a; Ex. 1003, ¶¶135-136.

b. Limitation 20[b]

Claim 20 continues by reciting “*the second action is a system action.*” Alperovitch discloses, teaches, or suggests Limitation 20[b] for the same reasons discussed above for Limitation 6[b]. *See supra* § V.B.6.b; Ex. 1003, ¶¶137-138.

c. Limitation 20[c]

Claim 20 continues by reciting “*the second time occurs after the first time.*” Alperovitch discloses, teaches, or suggests Limitation 20[c] for the same reasons discussed above for Limitation 8[c]. *See supra* § V.B.8.c; Ex. 1003, ¶¶139-140.

21. Claim 21

a. Limitation 21[a]

Claim 21 depends on claim 13 and further recites: “*wherein the action sequence includes three performed actions.*” Alperovitch discloses, teaches, or suggests Limitation 21[a] for the same reasons discussed above for Limitation 9[a]. *See supra* § V.B.9.a; Ex. 1003, ¶¶143-144.

b. Limitation 21[b]

Claim 21 continues by reciting “*a first action of the three performed actions is a user action.*” Alperovitch discloses, teaches, or suggests Limitation 21[b] for the same reasons discussed above for Limitation 9[b]. *See supra* § V.B.9.b; Ex. 1003, ¶¶145-146.

c. Limitation 21[c]

Claim 21 continues by reciting “*a second action of the three performed actions is an application action.*” Alperovitch discloses, teaches, or suggests Limitation 21[c] for the same reasons discussed above for Limitation 9[c]. *See supra* § V.B.9.c; Ex. 1003, ¶¶147-148.

d. Limitation 21[d]

Claim 21 continues by reciting “*a third action of the three performed actions is a system action.*” Alperovitch discloses, teaches, or suggests Limitation 21[d] for the same reasons discussed above for Limitation 9[d]. *See supra* § V.B.9.d; Ex. 1003, ¶¶149-150.

e. Limitation 21[e]

Claim 21 continues by reciting “*the second action is performed temporally after the first action.*” Alperovitch discloses, teaches, or suggests Limitation 21[e] for the same reasons discussed above for Limitation 9[e]. *See supra* § V.B.9.e; Ex. 1003, ¶¶151-152.

f. Limitation 21[f]

Claim 21 continues by reciting “*the third action is performed temporally after the second action.*” Alperovitch discloses, teaches, or suggests Limitation 21[f] for the same reasons discussed above for Limitation 9[f]. *See supra* § V.B.9.f; Ex. 1003, ¶¶153-154.

22. Claim 22

Claim 22 depends on claim 13 and further recites: “*wherein the runtime risk is identified based on matching rules and probabilistic weights and scores of performed actions on the device.*” Alperovitch discloses, teaches, or suggests claim 22 for the same reasons discussed above for claim 10. *See supra* § V.B.10; Ex. 1003, ¶¶156-158.

23. Claim 23

Claim 23 depends on claim 13 and further recites: “*wherein the runtime risk is identified based on time proximity of the at least two performed actions of the action sequence and natural affinity inferred between the at least two performed actions.*” Alperovitch discloses, teaches, or suggests claim 23 for the same reasons discussed above for claim 11. *See supra* § V.B.11; Ex. 1003, ¶¶159-161.

24. Claim 24

a. Limitation 24[a]

Claim 24 depends on claim 13 and further recites: “*wherein the processing device assesses that the at least two performed actions of the action sequence describe a forensic chain of events based on a plurality of factors.*” Alperovitch discloses, teaches, or suggests Limitation 24[a] for the same reasons discussed above for Limitation 12[a]. *See supra* § V.B.12.a; Ex. 1003, ¶¶163-164.

b. Limitation 24[b]

Claim 24 continues by reciting “*the plurality of factors includes at least one of: ordered sequences, unordered sequences, proximity analysis, outliers, probabilistic weights and scores, and probable action inferences based on an application's competency.*” Alperovitch discloses, teaches, or suggests Limitation 24[b] for the same reasons discussed above for Limitation 12[b]. *See supra* § V.B.12.b; Ex. 1003, ¶¶165-169.

C. Grounds 2-4: Claims 1-24 Are Rendered Obvious by Alperovitch in View of Yeh (Ground 2), Alperovitch in View of Chien (Ground 3), and Alperovitch in View of Yeh and Chien (Ground 4)

Ground 1 asserts that all the limitations of claims 1-24 of the '517 patent are rendered obvious by Alperovitch in view of the knowledge of a POSITA for the reasons discussed above. Alternative Grounds 2-4 assert that if it is found that Ground 1 would not have rendered the limitations discussed below obvious, then Alperovitch in view of Yeh, Alperovitch in view of Chien, and Alperovitch in view of Yeh and Chien, respectively, would have rendered those limitations obvious, as discussed below. Other than the limitations discussed below, all the other limitations of claims 1-24 would have been rendered obvious for the same reasons discussed in Ground 1 above. Ex. 1003, ¶171.

1. Claim 1

a. Limitation 1[a]

Limitation 1[a] recites “*storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence.*” As explained above, Alperovitch discloses, teaches, or suggests this limitation. *See supra* § V.B.1.b; Ex. 1003, ¶172. To the extent Alperovitch is found not to teach this limitation, Alperovitch in view of Yeh would have rendered this limitation obvious (Grounds 2 and 4). Yeh explicitly discloses a rules database for storing a plurality of rules. “Also included within each user computer as part of the monitoring agent (or separately) is a rules database 130. Database 130 includes rules that have been downloaded

from the central computer 20 and describe behaviors of the user computer that are allowed and those behaviors that are not allowed.” Ex. 1005, 6:40-45; *see also id.*, 5:47-51, 6:61-64. A POSITA would have found it obvious to store rules that describe behaviors of the user computer, such as rules describing the application behaviors taught in Alperovitch, in a database, whether in a rules database as taught in Yeh or an application manifest database as taught in Alperovitch. Ex. 1003, ¶172.

A POSITA would have been motivated to combine Yeh’s rules database in Alperovitch because both Alperovitch and Yeh are directed to determining whether activity on a computing device is malicious (*see* Ex. 1004, [0010] (“determin[ing] one or more trustworthiness indicators, and calculating a reputation score based on the one or more trustworthiness indicators” of a mobile application); Ex. 1005, 2:4-7 (“anomaly monitoring software on the user computer detects activities that, while not malware, are suspect. These activities are compared against a rules database on the user computer.”)) by having agents monitor whether certain behaviors on the computing device are suspicious (*see* Ex. 1004, [0014] (“Agents 24a-c may monitor behavior and activities of any one or more mobile applications (e.g., 22a-c) on respective mobile devices 14a-c.”); Ex. 1005, 6:22-24 (“Also included on computer 14 is monitoring agent software 128 that has the ability to monitor processes, registry keys, system alerts, etc.”)); Ex. 1003, ¶173.

Further, Alperovitch discloses an application manifest database that aggregates application behaviors of a mobile device for use in determining the reputation score of an application. Ex. 1004, [0055]. It would have been obvious to a POSITA to include rules stored in a rules database as disclosed in Yeh as part of the application manifest database because the rules in Yeh describe whether behaviors are allowed or not, and Alperovitch's application manifest database already has behaviors that are monitored. *Id.*, [0054]; *see also* Ex. 1005, 6:40-45; Ex. 1003, ¶174. It would have been a known technique to have and keep rules about application behaviors that are monitored in a database because Alperovitch already discloses that it determines whether certain behaviors are allowed or not (Ex. 1004, [0013]), and keeping information such as rules about application behaviors in a database was a known method that would have yielded predictable results, with a reasonable expectation of success. Ex. 1003, ¶174. Indeed, Alperovitch discloses that the use of databases to store information was well-known. Ex. 1004, [0065] (“The information being tracked, sent, received, or stored in system 10 could be provided in any database.”); Ex. 1003, ¶174.

Furthermore, to the extent that Alperovitch's application behaviors are found not to teach, disclose, or suggest “an action sequence,” Alperovitch in view of Chien would have rendered this limitation obvious (Grounds 3 and 4). Chien explicitly discloses behavior lists that identify an action sequence—“*a sequence of*

at least two performed actions.” Chien discloses that “a behavior list is a sequence or stream of events.” Ex. 1006, 3:62-65; *see also id.*, 4:8-13; Ex. 1003, ¶175.

Alperovitch discloses that “application behavior (e.g., requests for resources and application actions) may be monitored.” Ex. 1004, [0054]. It would have been obvious to a POSITA that a sequence of at least two performed actions (e.g., a sequence of requests for resources and application actions in Alperovitch) may be monitored based on Chien’s teaching of using a behavior list, which identifies a sequence or stream of events. Ex. 1003, ¶175.

A POSITA would have been motivated to combine Chien’s teachings of behavior lists with Alperovitch because both Alperovitch and Chien are directed to analyzing whether software can be trusted. Ex. 1004, [0010] (“determin[ing] one or more trustworthiness indicators, and calculating a reputation score based on the one or more trustworthiness indicators” of a mobile application); Ex. 1006, 1:57-59 (a “behavior list is then used, together with data in a malware behavior database, to derive a policy for use in a malware prevention system.”); Ex. 1003, ¶176. They do so by provisioning policies to protect users from undesirable malicious software. Ex. 1004, [0046] (“mobile device 14 may be provisioned with a policy that applications on a network accessing pictures on mobile device 14 are not allowed to run”); Ex. 1006, 4:13-14 (“behavior lists are provided so that they may be used to derive or extract policy” for use in a malware detection system); Ex.

1003, ¶176. Moreover, both Alperovitch and Chien perform this analysis based on collected data. Ex. 1004, [0055] (“reputation engine 20 may analyze the application behavior with other stored data (e.g., previously stored data crowdsourced from a plurality of sources) in application manifest database 32”); Ex. 1006, 2:6-8 (“The computer system also has a memory that may contain a malware behavior database that stores malware samples and results from parsing the samples for analysis.”); Ex. 1003, ¶176.

Further, the combination would be a simple matter. Alperovitch teaches a sequence of performed actions, such as “access to files and pictures stored on the mobile device” or “turning on the mobile device microphone and camera.” Ex. 1004, [0054]; Ex. 1003, ¶177. It would have, thus, been a simple and obvious modification to group the application behaviors taught in Alperovitch into a sequence of at least two performed actions by using Chien’s teaching of behavior lists, which are “a sequence or stream of events.” Ex. 1006, 3:63-65; Ex. 1003, ¶177. As Chien discloses, “[g]enerally, it is difficult to characterize malicious behavior by examining one event.” Ex. 1006, 1:29-30. Thus, examining a sequence of multiple events was a known method for detecting malicious behavior that would have yielded predictable results, with a reasonable expectation of success. Ex. 1003, ¶177. Indeed, Alperovitch already discloses assessing mobile application risks by examining a sequence of multiple events. Ex. 1004, [0013] (“a

mobile application that automatically, and without authorization, turns on a camera and a microphone (or other recording device) of a mobile device may be deemed to be malicious.”). Ex. 1003, ¶177.

b. Limitation 1[e]

Limitation 1[e] recites “*the action sequence is a sequence of at least two performed actions.*” As explained above for Limitation 1[a], to the extent Alperovitch is found not to render this limitation obvious, Alperovitch in view of Chien would have rendered that the action sequence is a sequence of at least two performed actions obvious (Grounds 3 and 4). *See supra* § V.C.1.a; Ex. 1003, ¶178.

2. Claim 13

a. Limitation 13[a]

Limitation 13[a] recites “*a rules database storing a plurality of rules, wherein each rule identifies an action sequence.*” Grounds 2-4 would have rendered Limitation 13[a] obvious for the same reasons discussed above for Limitation 1[a]. *See supra* § V.C.1.a; Ex. 1003, ¶¶179-180.

b. Limitation 13[f]

Limitation 13[f] recites “*the action sequence is a sequence of at least two performed actions.*” Alperovitch in view of Chien would have rendered Limitation 13[f] obvious for the same reasons discussed above for Limitation 1[e] (Grounds 3 and 4). *See supra* § V.C.1.b; Ex. 1003, ¶¶181-182.

D. No Secondary Considerations Exist

Petitioner is unaware of any secondary indicia of non-obviousness, and no such indicia were alleged during prosecution. Petitioner reserves the right to respond to any assertion of secondary indicia of non-obviousness advanced by Patent Owner.

VI. The Parallel District Court Proceeding Does Not Warrant a Discretionary Denial

Under the Director's interim procedure for evaluating requests for discretionary denial under 35 U.S.C. § 314(a), regardless of any factors that otherwise apply, "the PTAB will not discretionarily deny institution of an IPR or PGR in view of parallel district court litigation where a petitioner stipulates not to pursue in a parallel district court proceeding the same grounds as in the petition or any grounds that could have reasonably been raised in the petition." *Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation*, 7 (USPTO Dir. June 21, 2022).

Petitioner stipulates that, should the Board institute review, Petitioner will not pursue in parallel district court proceedings the same grounds as in the Petition or any grounds that could have reasonably been raised in the petition. Thus, the Board should not exercise discretion to deny institution under § 314(a).

VII. Mandatory Notices

A. Real Parties-in-Interest

Petitioner is the real party-in-interest. No other party had access to or control over the present Petition, and no other party funded or participated in preparation of the present Petition.

B. Related Proceedings

No previous IPR or post-granting proceeding has been filed challenging the '517 patent. The '517 patent has been asserted by Patent Owner in the following district court litigations: *Taasera Licensing LLC v. Trend Micro Inc.*, No. 2-21-cv-00441 (E.D. Tex.); *Taasera Licensing LLC v. Palo Alto Networks, Inc.*, No. 2-22-cv-00062 (E.D. Tex.); *Trend Micro Inc. v. Taasera Licensing LLC*, No. 3-22-cv-00477 (N.D. Tex.); *Trend Micro, Inc. v. Taasera Licensing LLC*, No. 3-22-cv-00518 (N.D. Tex.); *Palo Alto Networks, Inc. v. Taasera Licensing LLC*, No. 1-22-cv-02306 (S.D.N.Y.); *In re: Taasera Licensing LLC Patent Litig.*, No. 2-22-md-03042 (E.D. Tex.); *Trend Micro Inc v. Taasera Licensing LLC*, No. 2-22-cv-00303 (E.D. Tex.); *Palo Alto Networks, Inc. v. Taasera Licensing LLC*, No. 2-22-cv-00314 (E.D. Tex.); *Taasera Licensing LLC v. Musarubra US, LLC*, No. 2-22-cv-00427 (E.D. Tex.); *Taasera Licensing LLC v. CrowdStrike, Inc.*, No. 6-22-cv-01094 (W.D. Tex.); *Taasera Licensing LLC v. CrowdStrike, Inc.*, No. 2-22-cv-00468 (E.D. Tex.).

C. Lead and Backup Counsel

Petitioner's lead and backup counsel are:

Lead Counsel for Petitioner	Backup Counsel for Petitioner
Juan C. Yaquian Winston & Strawn LLP 800 Capital Street, Suite 2400 Houston, TX 77002-2925 JYaquian@winston.com T: 713.651.2600 F: 713.651.2700 USPTO Reg. No. 70,755	Michael Rueckheim Winston & Strawn LLP 255 Shoreline Drive, Suite 520 Redwood City, CA 94065 mrueckheim@winston.com T: 650.858.6500 F: 650.858.6550 (<i>pro hac vice</i> to be filed) James C. Lin Winston & Strawn LLP 255 Shoreline Drive, Suite 520 Redwood City, CA 94065 jalin@winston.com T: 650.858.6500 F: 650.858.6550 (<i>pro hac vice</i> to be filed)

D. Electronic Service

Petitioner consents to electronic service at:

Winston-PAN-Taasera@winston.com.

VIII. Fees

All fees may be charged to Deposit Account No. 50-1814.

IX. Conclusion

Petitioner respectfully requests that the Board institute IPR and enter a final written decision finding the Challenged Claims of the '517 patent unpatentable.

Dated: March 10, 2023

Respectfully submitted,

/ Juan C. Yaquian /
Juan C. Yaquian
Lead Counsel
Winston & Strawn LLP
800 Capital Street, Suite 2400
Houston, TX 77002-2925
JYaquian@winston.com
T: 713.651.2600
F: 713.651.2700
USPTO Reg. No. 70,755

Michael Rueckheim
(pro hac vice to be filed)
Winston & Strawn LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
mrueckheim@winston.com
T: 650.858.6500
F: 650.858.6550

James C. Lin
(pro hac vice to be filed)
Winston & Strawn LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
jalin@winston.com
T: 650.858.6500
F: 650.858.6550

Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

This Petition complies with the word count limits set forth in 37 C.F.R. § 42.24(a)(1)(i), because this Petition contains 13,939 words, excluding the parts of the Petition exempted by 37 C.F.R. § 42.24(a)(1), determined using the word count provided by Microsoft Word, which was used to prepare this Petition.

Dated: March 10, 2023

Respectfully submitted,

/ Juan C. Yaquian /
Juan C. Yaquian
Lead Counsel
Winston & Strawn LLP
800 Capital Street, Suite 2400
Houston, TX 77002-2925
JYaquian@winston.com
T: 713.651.2600
F: 713.651.2700
USPTO Reg. No. 70,755

Michael Rueckheim
(pro hac vice to be filed)
Winston & Strawn LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
mrueckheim@winston.com
T: 650.858.6500
F: 650.858.6550

James C. Lin
(pro hac vice to be filed)
Winston & Strawn LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
jalin@winston.com
T: 650.858.6500
F: 650.858.6550

Counsel for Petitioner

CERTIFICATE OF SERVICE

Under 37 C.F.R. §§ 42.6(e) and 42.105(a), this is to certify that on March 10, 2023, I caused to be served a true and correct copy of the foregoing “**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 8,850,517**” and Exhibits 1001-1006 by Federal Express on the Patent Owner at the correspondence address of record for U.S. Patent No. 8,850,517:

BUCHANAN, INGERSOLL & ROONEY PC
1737 KING STREET
SUITE 500
ALEXANDRIA, VA 22314-2727

A courtesy copy of this Petition and supporting material was also served on litigation counsel for Patent Owner via email:

ALFRED ROSS FABRICANT
FABRICANT LLP - NY
230 PARK AVENUE, 3RD FLOOR W.
NEW YORK, NY 10169
Email: ffabricant@fabricantllp.com

/ Juan C. Yaquian /
Juan C. Yaquian
Lead Counsel
Winston & Strawn LLP
800 Capital Street, Suite 2400
Houston, TX 77002-2925
JYaquian@winston.com
T: 713.651.2600
F: 713.651.2700
USPTO Reg. No. 70,755