UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD. and
SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner

v.

DAEDALUS PRIME LLC,
Patent Owner.

Case No. IPR2023-00660
U.S. Patent No. 8,359,629

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 8,359,629

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

LIST OF EXHIBITS[1]

Ex-1001	U.S. Patent No. 8,359,629 to Kohlenberg ("the '629 Patent")
Ex-1002	Declaration of Dr. Benjamin Bederson
Ex-1003	Curriculum Vitae of Dr. Benjamin Bederson
Ex-1004	Prosecution History of the '629 Patent (Application No. 12/567,386)
Ex-1005	U.S. Patent Publication No. 2010/0076777 to Paretti ("Paretti")
Ex-1006	U.S. Patent No. 6,750,883 to Parupudi ("Parupudi")
Ex-1007	U.S. Patent No. 6,594,483 to Nykanen ("Nykanen")
Ex-1008	INTENTIONALLY LEFT BLANK
Ex-1009	INTENTIONALLY LEFT BLANK
Ex-1010	INTENTIONALLY LEFT BLANK
Ex-1011	INTENTIONALLY LEFT BLANK
Ex-1012	INTENTIONALLY LEFT BLANK
Ex-1013	INTENTIONALLY LEFT BLANK
Ex-1014	INTENTIONALLY LEFT BLANK
Ex-1015	INTENTIONALLY LEFT BLANK
Ex-1016	INTENTIONALLY LEFT BLANK
Ex-1017	INTENTIONALLY LEFT BLANK
Ex-1018	INTENTIONALLY LEFT BLANK
Ex-1019	INTENTIONALLY LEFT BLANK
Ex-1020	Claim Comparison Table for the '629 Patent

[1] Four-digit pin citations that begin with 0 are to the branded numbers added by Samsung in the bottom right corner of the exhibits. All other pin citations are to original page, column, paragraph, or line numbers.

Ex-1021	U.S. District Courts – Combined Civil and Criminal Federal Court Management Statistics (June 30, 2022), available at: https://www.uscourts.gov/statistics-reports/federal-court-management-statistics-june-2022
Ex-1022	Benjamin B. Bederson. 1995. Audio augmented reality: a prototype automated tour guide. In Conference Companion on Human Factors in Computing Systems (CHI '95), I. Katz, R. Mack, and L. Marks (Eds.). ACM, New York, NY, USA, 210-211. DOI: http://dx.doi.org/10.1145/223355.223526.
Ex-1023	Bederson, B.B., Clamage, A., Plaisant, C. (2008) Enhancing In-Car Navigation Systems with Personal Experience, in Transportation Research Record (TRR), The National Academies, 2064 (2008) 33-42.
Ex-1024	Benjamin B. Bederson and James D. Hollan, Pad++: A Zooming Graphical Interface for Exploring Alternate Interface Physics, USIT '94 Proceedings of the 7th Annual ACM Symposium on User Interface Software and Technology 17 (1994), DOI: http://dx.doi.org/10.1145/192426.192435.
Ex-1025	U.S. Patent No. 8,261,211
Ex-1026	Ben Shneiderman and Catherine Plaisant, Designing the User Interface, 4th Edition (2004).

I. INTRODUCTION

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Petitioner") request *inter partes* review ("IPR") of Claims 1, 3-5, 7-16, and 18-25 of U.S. Patent No. 8,359,629 ("the '629 Patent") (Ex-1001), currently assigned to Daedalus Prime LLC ("PO").

II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

Real Parties-in-Interest: Petitioner identifies the following real parties-in-interest: Samsung Electronics Co., Ltd., Samsung Electronics America, Inc., Samsung Semiconductor, Inc., and Samsung Austin Semiconductor, LLC.

Related Matters: Patent Owner has asserted the '629 Patent against Samsung Electronics Co., Ltd., Samsung Electronics America, Inc., Samsung Semiconductor, Inc., and Samsung Austin Semiconductor, LLC in *Daedalus Prime LLC v. Samsung Electronics Co., Ltd*., No. 2:22-cv-00354 (E.D. Tex. Sept. 12, 2022).

Lead and Back-Up Counsel:

- Lead Counsel:

John Kappos (Reg. No. 37,861)
O'Melveny & Myers LLP
2501 North Harwood Street, Suite 1700
Dallas, TX 75201
Telephone: (972) 360-1900
E-Mail: jkappos@omm.com

- First Backup Counsel:

Benjamin M. Haber (Reg. No. 67,129)

O'Melveny & Myers LLP
400 South Hope Street, 18th Floor
Los Angeles, CA 90071
Telephone: (213) 430-6000
E-Mail: bhaber@omm.com

- Additional Backup Counsel:

Xin-Yi Zhou (Reg. No. 63,366)
O'Melveny & Myers LLP
400 South Hope Street, 18th Floor
Los Angeles, CA 90071
Telephone: (213) 430-6000
Fax: (213) 430-6407
E-Mail: vzhou@omm.com

Jeff Baxter (Reg. No. 45,560)
O'Melveny & Myers LLP
2501 North Harwood Street, Suite 1700
Dallas, TX 75201
Telephone: (972) 360-1900
Fax: (972) 360-1901
E-Mail: jbaxter@omm.com

William M. Fink (Reg. No. 72,332)
O'Melveny & Myers LLP
1625 Eye Street, NW
Washington, DC 20006
Telephone: (202) 383-5300
E-Mail: tfink@omm.com

Service Information: Petitioner consents to electronic service by email to the following addresses:

- jkappos@omm.com
- bhaber@omm.com
- vzhou@omm.com
- jbaxter@omm.com

- tfink@omm.com
- OMMSAMSUNGDAEDALUSEDTX@omm.com

III. FEE AUTHORIZATION

Pursuant to 37 C.F.R. §42.15(a) and §42.103(a), the PTO is authorized to charge any and all fees to Deposit Account No. 50-0639.

IV. GROUNDS FOR STANDING

Petitioner certifies that the '629 Patent is available for review, this Petition is timely filed, and Petitioner is not barred or estopped from requesting review.

V. PRECISE RELIEF REQUESTED

Petitioner requests review and cancellation of Claims 1, 3-5, 7-16, and 18-25 as unpatentable based on the following grounds, supported by a declaration from Dr. Benjamin Bederson. Ex-1002 ¶¶67-342; Ex-1003.

Ground	Summary
1	Claims 1, 3-5, 7, 9-16, 18-19, 21-25 are obvious over Paretti (Ex-1005).
2	Claims 1, 3-5, 7-8, 13-16, 18, 20-25 are obvious over Parupudi (Ex-1006) in view of Nykanen (Ex-1007).

VI. THE CHALLENGED PATENT

The '629 Patent purports to describe a device and method for controlling the "use of context information of a user" by a requesting application or entity by

"establishing a context policy enforcement engine on a mobile computing device." Ex-1001, Abstract. The '629 Patent's mobile computing device receives a request for user context information (e.g., the user's location) and, in response, the context policy enforcement engine retrieves context policy data defining a set of rules for responding to context requests. *Id*., 8:62-9:10. The mobile computing device then determines a level of specificity of a context characteristic ("e.g., what city is the user located in, what building is the user located in, what are the GPS coordinates of the user, etc.") for a context parameter (e.g., the user's location) associated with the requested context information "based on or according to the context policy rules stored in the context policy rule database" and based on an identity of a requesting application or entity; retrieves the corresponding context data; and responds to the requesting application or entity with the retrieved context data. *Id*., 4:56-67, 5:38-54, 9:11-52, Figure 5 (depicting a flow chart of the claimed method for controlling the use of context information of a user executed by the mobile computing device of the invention).

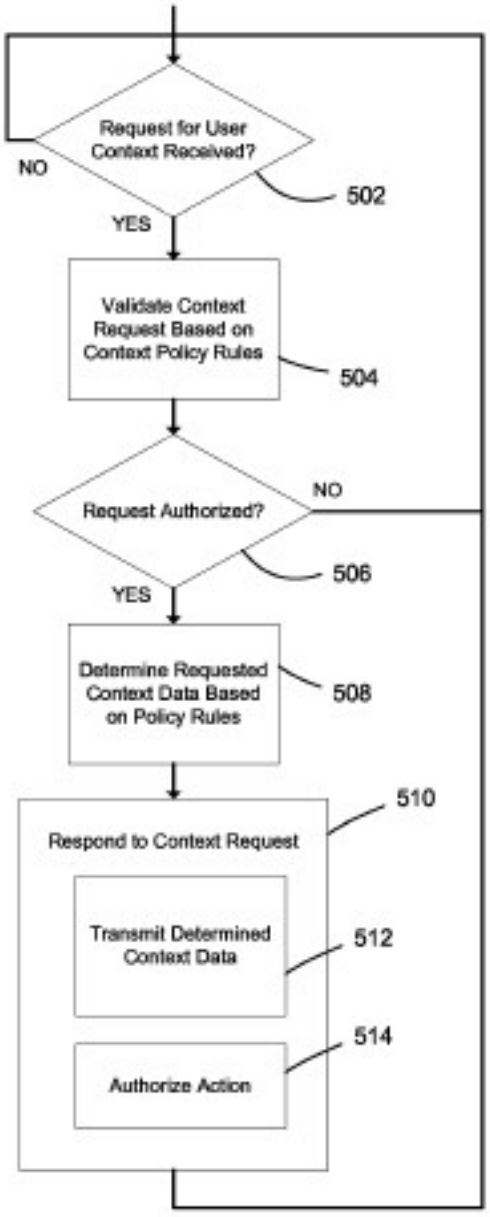

FIG. 5

VII. PATENT PROSECUTION HISTORY

The '629 Patent, filed as Application No. 12/567,386 on September 25, 2009, was allowed after two office actions. On November 10, 2011, the Examiner rejected then-pending Claims 1-25 as anticipated by Lee (WO 2006/106303). Ex-1004, 206-215. In its February 10, 2012 response, Applicant amended independent Claims 1,

20, and 25 to add the following limitations: receiving "from a requesting entity"; "determining a level of specificity of a context characteristic for a context parameter associated with the requested context information as a function of the context policy data and an identity of the requesting entity"; "retrieving context data identified by the determined level of specificity of the context characteristic for the context parameter associated with the requested content information; and" "responding to the request for context information with the retrieved context data." *Id.*, 241-255. On June 13, 2012, the Examiner rejected then-pending Claims 1 and 3-25 as obvious over Parupudi (U.S. Patent No. 7,072,956) ("the '956 Patent") in view of Henry (U.S. Patent Pub. No. 2008/0194233) and Claim 2 as obvious in further view of Smith (U.S. Patent Pub. No. 2009/0319806). Ex-1004, 259-272. In its July 23, 2012 response, Applicant argued that the '956 Patent "fails to disclose retrieving *context* policy for responding to policy requests, instead appearing to disclose retrieving *enterprise* policy based on context." *Id.*, 297-298 (emphases in original). The Examiner allowed the claims on December 18, 2013. *Id.*, 465-468.

This Petition presents new arguments that were not considered during prosecution. The particular prior art relied on in this Petition was not before the PTO during prosecution of the '629 Patent. The '956 Patent (to Parupudi) cited by the Examiner during prosecution and EP 1217857 (to Parupudi) (Ex-1004, 81-131), which was listed on an IDS by Applicant but not substantively addressed by the

Examiner during prosecution, are *unrelated* to Ex-1006 discussed herein, having different titles, inventors, families, and priority dates. Moreover, the disclosures of the '956 Patent upon which Applicant relied to distinguish the claimed subject matter in its July 23, 2012 response, i.e., the '956 Patent's "enterprise policy" disclosures (Ex-1004, 297-298), are not present in Ex-1006. As discussed in Section XII, Ex-1006 in view of Nykanen (Ex-1007) renders obvious Claims 1, 3-5, 7-8, 13-16, 18, and 20-25 of the '629 Patent. To the extent there is any overlap in the subject matter disclosed by the Parupudi references cited during prosecution and the grounds presented below based on Ex-1006, the Examiner overlooked those disclosures. Thus, the Board should decline to exercise it discretion to deny institution under §325(d). *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 8 (PTAB Feb. 13, 2020) (precedential). Ex-1002 ¶¶45-49.

VIII. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art at the relevant time ("POSITA") would have had a bachelor's degree in computer science, electrical engineering, computer engineering, or a related field, and 3-4 years of experience in the research, design, development, or testing of human-computer interaction, mobile location services, and/or mobile privacy technologies, or the equivalent, with additional education substituting for experience and vice versa. Ex-1002 ¶¶30-32.

IX. PRIORITY DATE

For purposes of this proceeding only, Petitioner assumes that the '629 Patent is entitled to its earliest alleged priority date, September 25, 2009, and thus applies pre-AIA 35 U.S.C. §102.

X. CLAIM CONSTRUCTION

Petitioner interprets the claims of the '629 Patent according to the *Phillips* claim construction standard. 37 C.F.R. §42.100(b). To resolve the particular grounds presented in this Petition, Petitioner does not believe that any term requires explicit construction.[2] Ex-1002 ¶¶22-23.

XI. BRIEF DESCRIPTION OF THE APPLIED PRIOR ART REFERENCES

A. Paretti (Ex-1005)

Paretti is §102(e) prior art as of its U.S. filing date, September 23, 2008.

Paretti discloses "a method for recommending a location tracking privacy policy to a user." Ex-1005 ¶11. Paretti discloses "mobile devices" that include a visibility manager that is designed "to automatically control the manner in which location information associated with [a] user is provided to [an] application" commensurate with an "identified location tracking privacy policy." *Id*. ¶14.

[2] Petitioner reserves all rights to raise claim construction and other arguments in district court. Additionally, Petitioner will request leave to submit the district court's claim construction as soon as it becomes available.

Paretti's visibility manager 208 enforces any existing privacy policy warranted by specific conditions "by applying the location reporting methodology to the user location information." *Id*. ¶75. Visibility manager 208 is designed to "receive location information about a user from location tracking system interface 212," "access privacy policies specified by the user that are stored in privacy policies database 206," and "enforce the polic[ies]" by "[p]roviding the user location information at a specified level of granularity." *Id*. ¶¶75, 86, Figure 4 (depicting a flow diagram of a method for allowing a user to control the manner in which the user's location information is provided to an application).

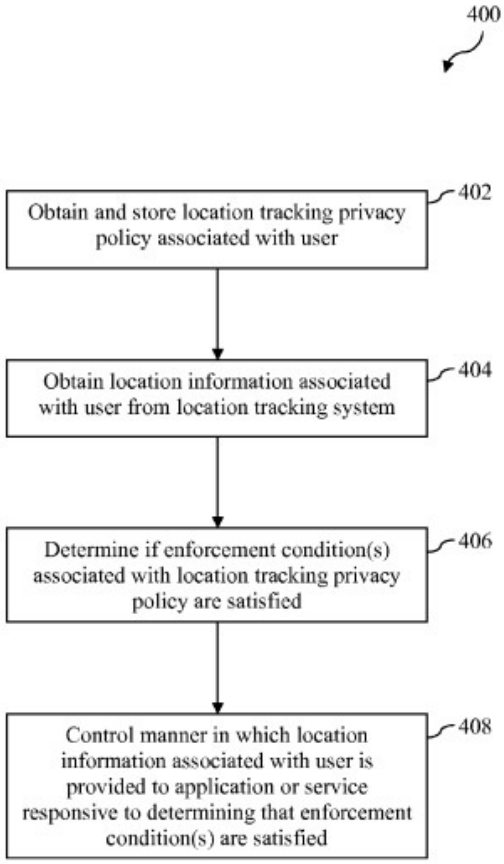

FIG. 4

Paretti discloses that "[p]roviding the user location information at a specified level of granularity" means that the user's location can be communicated "with varying levels of precision." *Id.* ¶86. For instance, the user's actual location "may be specified very precisely by providing a set of latitude and longitude coordinates" identifying the user's location or by providing the user's "full address…including street address, city, state and zip code"; or the location may be specified "less

precisely by providing a range of latitude and longitude coordinates" indicating the user's location or "by only providing the city name, state name or zip code." *Id*.

B. Parupudi (Ex-1006)

Parupudi is §102(b) prior art as of its issuance date, June 15, 2004.

Parupudi discloses "identity-based context aware computing systems and methods." Ex-1006, Title. Parupudi discloses that "a privacy policy can be applied to" requested context information (e.g., location) relating to a user's device "before it is returned to [requesting] applications." *Id*., 23:65-67, 24:5-7. To that end, Parupudi discloses a privacy manager comprising "a software module that is incorporated in the mobile computing device." *Id*., 24:10-19. Parupudi's privacy manager 704 "addresses privacy concerns that are associated with the information that is collected by the computing device." *Id*., 24:20-22. For example, Parupudi states that it is very "likely that a user may not want their specific location information provided to untrusted applications" and instead "just desire…to inform such applications that the user is in the State of Washington." *Id*., 24:26-30. Indeed, the below table describes "different privacy levels" and "associated approximate scale[s]" that can be assigned by users to individual applications that call a location service module, such as "a privacy level of 0," which "means that no location information is returned" and "[a] privacy level of 90," which "means that very detailed location information is returned." *Id*., 24:56-60.

Privacy Level	Approximate Scale	Level of Revelation
0	—	No location information is returned
10	100,000 Km	Planet/Continent
20	1,000 Km	Country
30	100 Km	State
40	10–100 Km	City & County or Region
50	10 Km	Postal Code & Phone Area Code
60	1 Km	Full Postal Code (Zip + 4) & Area Code and Exchange
70	100 m	Phone Number & Building/Floor
80	10 m	Room #
90	1 m	Exact Coordinates

Parupudi's Figure 10 depicts a flow diagram describing "the steps in a privacy protection method" that may be employed by privacy manager 704. *Id*., 24:31-34, Figure 10.

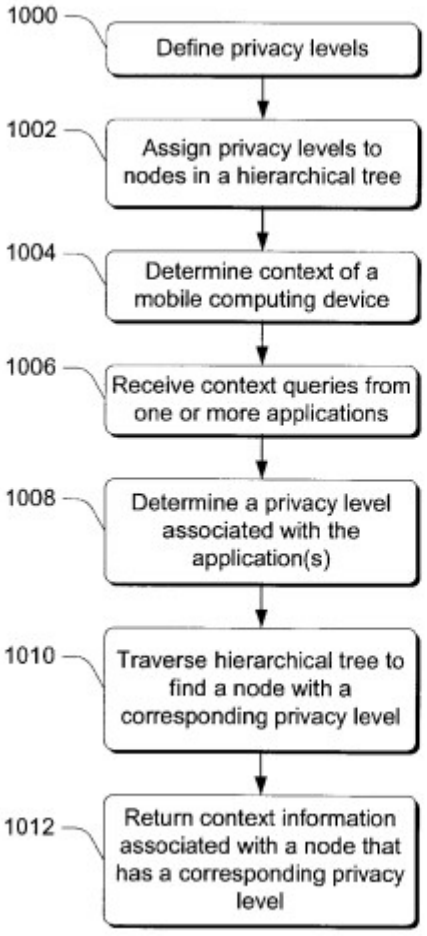

Fig. 10

At Steps 1000 and 1002, privacy levels are defined and assigned "to nodes in a hierarchical tree." *Id*. At Step 1006, context queries are received "from one or more applications." *Id*. At Step 1008, "the privacy level associated with the application or applications" is determined. *Id*., 25:11-19. Privacy manager 704 "then traverses…one or more hierarchical tree structures" at Step 1010 "to find a node with a corresponding privacy level so that it can select the information that is associated with that node." *Id*. When "the corresponding node is found," at Step 1012, "the context information (e.g., location information) associated with the node"

is returned to the requesting application, such as by having "the location service module…inform the application that the user's location is the State of Washington." *Id*., 25:22-27, Figure 10.

C. Nykanen (Ex-1007)

Nykanen is §102(b) prior art as of its issuance date, July 15, 2003.

Nykanen discloses a method "for location based web services" through which "a user can specify his privacy preferences to one database" with assurance that they will "be adhered to by all location providing sources," thus ensuring that the user will have "direct control over which applications and web services have access to data concerning the location of his mobile." Ex-1007, Title, Abstract.

With respect to the "terminal" of Figure 1, Nykanen discloses that "positioning service 1-9 interfaces with positioning hardware and driver 1-11" to send information concerning the terminal's location. *Id*., 3:48-50. Application 1-1 "requests information" regarding the terminal's location "via location application program interface (API) 1-3," which "forwards data" regarding "the location information request to privacy control module 1-5." *Id*., 3:50-56. Forwarded data may include, e.g., the identity of the requesting application and "the specifics of the location information request," such as the desired latitude, longitude, and altitude data and "the level of accuracy" that is required. *Id*., 3:56-63, Figure 1.

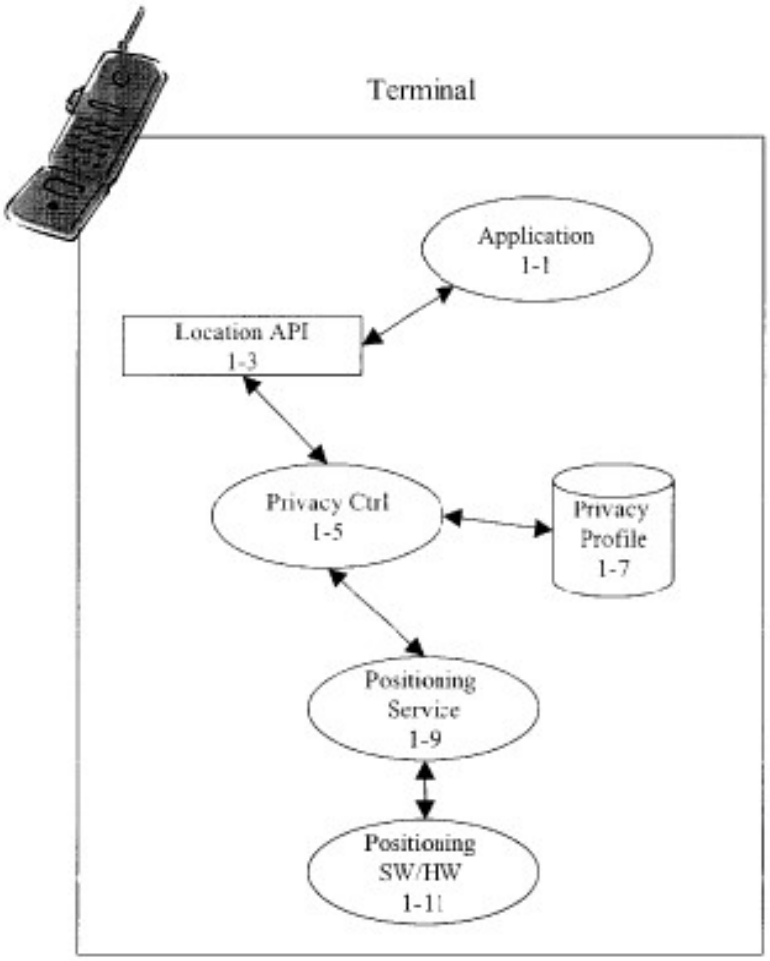

FIG. 1

Privacy control module 1-5 then "interfaces with privacy profile database 1-7" to determine "whether to allow or disallow application 1-1's information request." *Id*., 4:5-8. "To comply with one or more of the rules" that are stored in privacy profile database 1-7, privacy control 1-5 may, for example, command positioning service 1-9 to limit "the accuracy of the location information provided to application 1-1" to a certain level, by having it direct positioning

software/hardware 1-11 "to provide it with a specified level of position accuracy, or…alter the location information received from positioning SW/HW 1-11 before passing it on" in order to regulate the location accuracy level. *Id*., 4:11-19, Claim 1.

Nykanen also discloses a "rules variable" field that contains a listing of the requesting applications and "specifies for each the highest level of location accuracy that may be requested." *Id*., 5:6-9. Thus, for example, Nykanen's "AllowTheseRequestersDisallowOthers" rule "allows access only to requesters that are noted in the 'Rule Variables' field…and that request a level of accuracy no higher than that specified for them." *Id*., 5:1-6.

XII. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS

The '629 Patent contains three independent claims—Claims 1, 21, and 25—that are substantially similar in scope but directed to different classes. *See* Ex-1020. Substantially similar claim elements are discussed together in the below element-by-element analysis. *Id*. Any meaningful differences between the elements are individually identified and discussed.

A. Ground 1: Claims 1, 3-5, 7, 9-16, 18-19, and 21-25 are obvious over Paretti.

1. Independent Claims 1, 21, and 25

a. Element 1[pre]: A method comprising:

Paretti discloses a "method…for enabling a user to control the manner in which location information associated with the user is provided to a context-aware application or service." Ex-1005 ¶82, Figure 4; *see also id*., Abstract ("method…that automatically provides users with recommendations regarding location tracking privacy policies that may be…enact[ed] in certain contexts as well as a means for enacting such policies"), ¶10; Ex-1002 ¶¶67-72.

b. Element 1[a]/21[a]: establishing a context policy enforcement engine on a mobile computing device;

Element 25[pre]: A mobile computing device comprising:
Element 25[a]: a context policy enforcement engine;

Paretti discloses establishing a context policy enforcement engine on a mobile computing device.

Paretti discloses "mobile user devices (e.g., mobile telephones, personal digital assistants, laptop and handheld computers…)" that include a "location tracking privacy engine," which is "configured to control the manner in which…location information is provided to context-aware applications/services."

Ex-1005 ¶¶38-40, 52, 158-163, Figure 12. Paretti's location tracking privacy engine is "a context policy enforcement engine." Ex-1002 ¶¶73-85.

Paretti's location tracking privacy engine comprises "user interface," "W4 data database," "privacy policies database," "visibility manager," and "location tracking system interface." Ex-1005 ¶47, Figure 2. The user interface allows a user to interact with the location tracking privacy engine to define "privacy policies" that govern how location information is provided to context-aware applications. *Id*. ¶¶44, 49; *see also id*. ¶¶36-43, 51-52. The privacy policies database stores said privacy policies, which may include both a "location reporting methodology" and "one or more conditions under which the location reporting methodology is to be enforced." *Id*. ¶¶70-73. The visibility manager is designed to "receive location information about a user from location tracking system interface," "access privacy policies…stored in privacy policies database," and enforce the policies "by applying the location reporting methodology to the user location information." *Id*. ¶75; *see also id*. ¶¶82-92. Accordingly, Paretti discloses establishing a context policy enforcement engine. Ex-1002 ¶¶73-85.

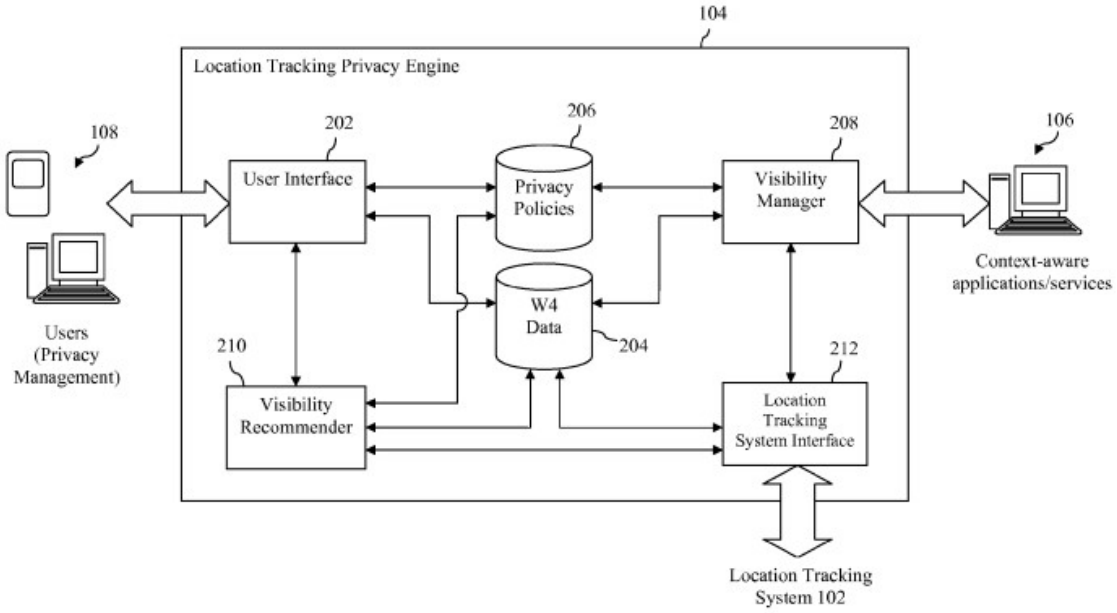

FIG. 2

Paretti discloses that its "context policy enforcement engine" may reside on the "mobile computing device." Figure 12's "Client-Side Implementation" discloses implementing the "location tracking privacy engine" (i.e., the claimed "context policy enforcement engine") in the user device itself. Ex-1005 ¶¶158-163 ("FIG. 12 is a block diagram of a location tracking privacy engine 1200 that may be implemented in a user device to perform similar functions to location tracking privacy engine 104 described above in reference to FIG. 2."), Figure 12 (showing "location tracking privacy engine 1200" comprising "user interface 1202," "W4 data database," "privacy policies database 1206," "visibility manager 1208," and "location tracking system interface 1212"). Accordingly, Paretti discloses a mobile

computing device comprising the context policy enforcement engine. Ex-1002 ¶¶73-85.

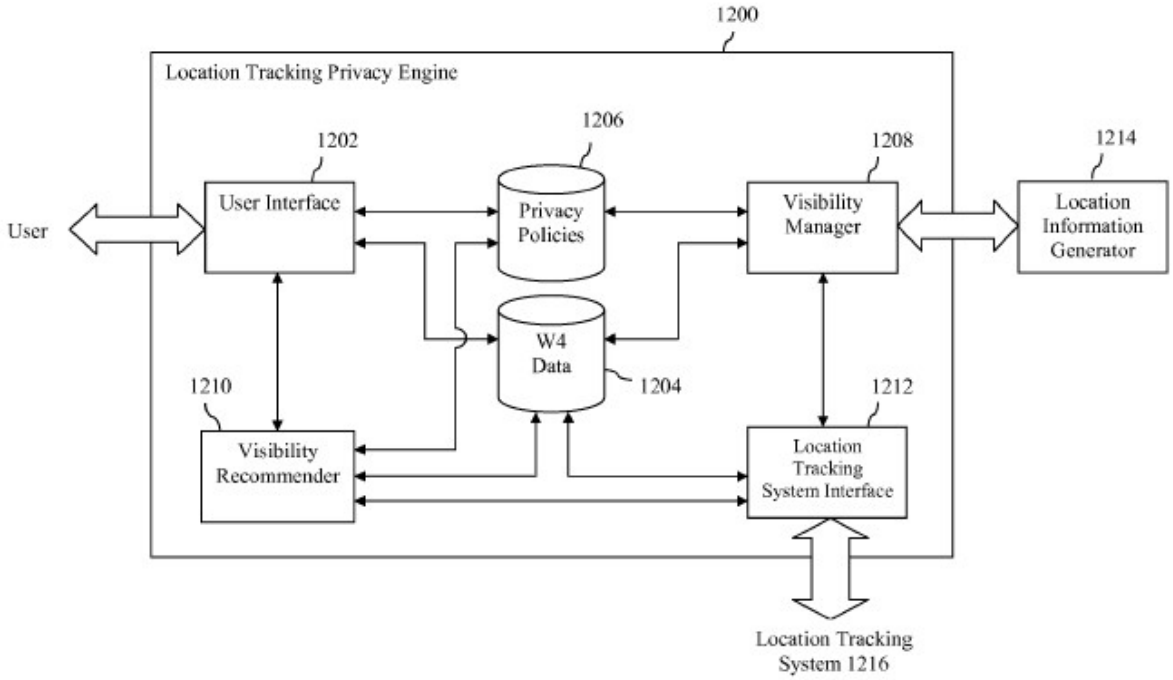

FIG. 12

c. Element 21[pre]: A non-transitory, machine readable medium comprising a plurality of instructions, that in response to being executed, result in a computing device:

Element 25[b]: a processor; and
Element 25[c]: a memory device having stored therein a plurality of instructions, which when executed by the processor, cause the context policy enforcement engine to:

Paretti discloses a non-transitory, machine readable medium comprising (or a memory device having stored therein) a plurality of instructions, that in response to being executed (by a processor), result in a computing device.

Paretti discloses that "[e]ach of the elements of the various systems depicted in FIGS. 1, 2, 5, 7, 9 and 12 and each of the steps of flowcharts depicted in FIGS. 4, 6, 8, 10 and 11 may each be implemented by one or more processor-based computer systems," such as "computer system 1300 [] depicted in FIG. 13." Ex-1005 ¶164. Paretti discloses that computer system 1300 "includes a processing unit 1304 that includes one or more processors," "a main memory 1306, preferably random access memory (RAM), and may also include a secondary memory 1320." *Id*. ¶¶165-166. Paretti further discloses that "[c]omputer programs…are stored in main memory 1306 and/or secondary memory 1320," and, "when executed, enable the computer system 1300 to implement features of the present invention as discussed herein." *Id*.

¶¶164-171; *see also id*. ¶169 (defining "computer program medium" and "computer readable medium"); Ex-1002 ¶¶86-91.

d. Element 1[b]: receiving, from a requesting entity, a request for context information related to a user of the mobile computing device,
Element 1[c]/21[b]/25[c][i]: retriev[e/ing] context policy data [] with the context policy enforcement engine [], the context policy data defining a set of rules for responding to context requests;

Paretti discloses receiving, from a requesting entity, a request for context information related to a user of the mobile computing device. Paretti's Figure 6, at Step 602, states that a first request is received by the system from an "application/service" (i.e., from the claimed "requesting entity") "to access location information associated with the user." Ex-1005 ¶¶122, 82-92, Figure 6; *see also id*. ¶¶36-44, 47-52, 70-75; Ex-1002 ¶¶92-102.

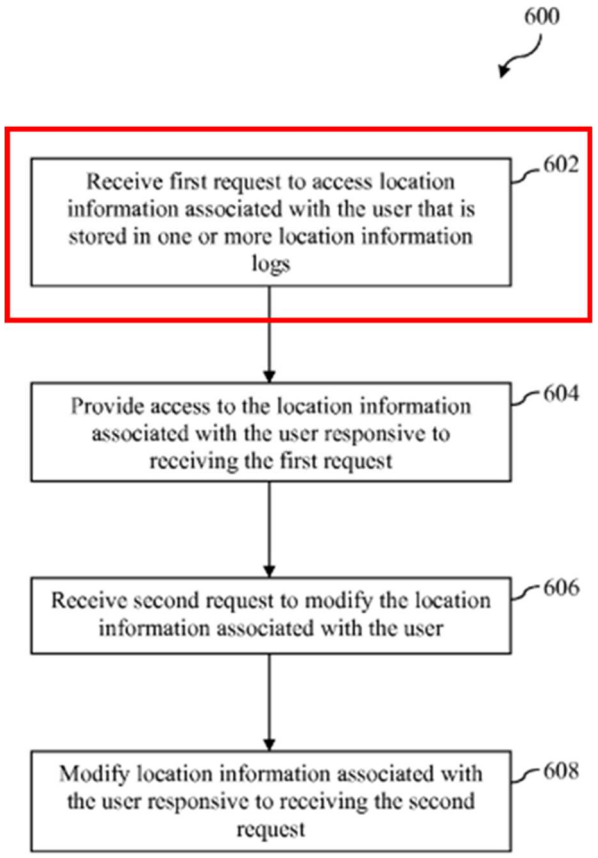

FIG. 6

Paretti also discloses the context policy enforcement engine retrieving context policy data which defines a set of rules for responding to context requests. Paretti's visibility manager is designed to "access privacy policies specified by the user that are stored in privacy policies database." Ex-1005 ¶¶75, 86; *see also id*. ¶¶36-44, 48-52, 70-75, 82-92, Figure 4; Ex-1002 ¶¶92-102. These privacy policies may include both a "location reporting methodology" (e.g., "providing the location information,

not providing the location information, modifying the content or granularity of the location information, selectively providing the location information to certain applications/services or users thereof, and/or selectively modifying the content or granularity of the location information based on a recipient application/service or user thereof") and "one or more conditions under which the location reporting methodology is to be enforced." Ex-1005 ¶¶70-73; Ex-1002 ¶¶92-102.

e. Element 1[d]/21[c]/25[c][ii]: determin[e/ing] a level of specificity of a context characteristic for a context parameter associated with the requested context information as a function of the context policy data and an identity of [the/a] requesting entity [that requested the context information];

Paretti discloses that its visibility manager determines a level of specificity as a function of the context policy data and an identity of the requesting entity. Paretti discloses "access[ing] privacy policies" (i.e., the claimed "context policy data") that comprise "one or more conditions under which the location reporting methodology is to be enforced" as well as the "location reporting methodology" that "defines how location information…is to be provided to context-aware applications," including "***selectively providing*** the user location information ***to certain applications***" (i.e., the claimed "identity of a requesting entity that requested the context information") and "***selectively modifying the content or granularity*** of the user location information ***based on a recipient application***" (i.e., the claimed "determining a level

of specificity," including as a function of the claimed "identity of a requesting entity that requested the context information"). Ex-1005 ¶¶75, 84 (emphasis added); *see also id*. ¶¶82-92; Ex-1002 ¶¶103-115. Indeed, after accessing the privacy policies, Paretti's visibility manager "access[es] W4 data database…to determine whether the condition(s) associated with each of the privacy policies…exist," and "[i]f the condition(s) associated with a particular privacy policy exist," "enforce[s] that policy by applying the location reporting methodology to the user location information before providing the user location information to context-aware applications." Ex-1005 ¶75, Figure 4; *see also id*. ¶¶36-44, 70-73.

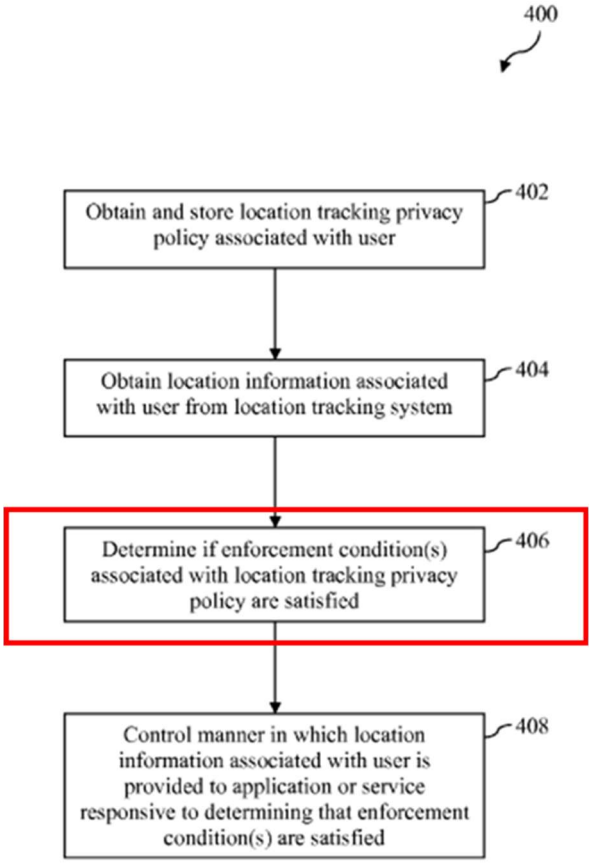

FIG. 4

The enforcement condition(s) associated with a location tracking privacy policy (i.e., the claimed "context policy data") "serve to specify a context within which the location reporting methodology is to be applied," "may be based on any social, topical, temporal or spatial data or conditions associated with the user," and "may be reflected by data stored in W4 data database." Ex-1005 ¶88; *see also id*. ¶¶82-92. Accordingly, Paretti discloses determining a level of specificity of a context characteristic for a context parameter associated with the requested context

information as a function of the context policy data and an identity of the requesting entity. Ex-1002 ¶¶103-115.

Indeed, Paretti specifically discloses determining a level of specificity of a context characteristic for a context parameter associated with the requested context information. Paretti explains that "[p]roviding the user ***location information***" (i.e., the claimed "context parameter") "at a specified level of granularity refers to the fact that the location of a user may be reported with varying levels of precision" (e.g., providing the user's location information "very precisely by providing ***a set of latitude and longitude coordinates***…or less precisely by providing ***a range of latitude and longitude coordinates*** within which the user is located" and/or "very precisely by providing ***a full address*** at which the user is located, ***including street address, city, state and zip code***, or less precisely by ***only providing the city name, state name or zip code***") (i.e., the claimed "context characteristic").[3] Ex-1005 ¶86 (emphasis added); *see also id*. ¶¶82-92; Ex-1002 ¶¶103-115.

[3] The '629 Patent discloses: "the context of the user may be defined by a plurality of context parameters (e.g., location, activity, environmental aspects, etc.), each having an associated characteristic (e.g., granularity, confidence, currency, etc.). For each parameter-characteristic combination, context data of varying levels of specificity may be stored or otherwise determined such that requests for context data may be responded to with context data having a selected level of specificity as desired by the user. For example, in one embodiment, the context data structure 300 may include context data 302 that defines three levels of specificity for the granularity characteristic of the location context parameter. As shown, the location granularity

f. Element 1[e]/21[d]/25[c][iii]: retriev[e]/[ing] context data identified by the determined level of specificity of the context characteristic for the context parameter associated with the requested context information; and

Paretti discloses retrieving context data identified by the determined level of specificity of the context characteristic for the context parameter associated with the requested context information.

After determining whether the "condition(s) associated with a particular privacy policy exist," Paretti's visibility manager "will enforce that policy by applying the location reporting methodology to the…location information before providing the…location information to context-aware applications." Ex-1005 ¶¶75, 81, 91, Figure 4; *see also id*. ¶¶36-44, 48-52, 70-73, 82-92, Figure 4; Ex-1002 ¶¶116-126. This includes, for example, selectively providing the location information to certain applications and selectively altering the granularity of the location information based on the requesting application (i.e., the claimed "retriev[e]/[ing]

includes a high granularity level indicating that the user is at a particular GPS coordinate location, a middle granularity level indicating that the user is inside a particular building at work, and a low granularity level indicating that the user is simply at work." Ex-1001, 5:38-54; *see also id*., 4:56-67 ("[E]ach context parameter may have one or more characteristics associated therewith that define the level of specificity of the context parameter. Such characteristics may include, for example, the granularity of the context parameter data (e.g., what city is the user located in, what building is the user located in, what are the GPS coordinates of the user, etc.).").

context data identified by the determined level of specificity"). Ex-1005 ¶84; *see also id*. ¶¶82-92; Ex-1002 ¶¶116-126.

Paretti discloses that "[p]roviding the user location information at a specified level of granularity" means that the user's location can be communicated "with varying levels of precision." Ex-1005 ¶86. For example, the user's location "may be specified" to the requesting application "very precisely" "by providing a set of latitude and longitude coordinates" or by providing the user's "full address…including street address, city, state and zip code," or the location may be specified "less precisely" "by providing a range of latitude and longitude coordinates" or "by only providing the city name, state name or zip code." *Id*.; *see also id*. ¶¶82-92. Paretti's "user location information" is the claimed "context parameter associated with the requested context information" and its "latitude"-"longitude coordinates" versus "range of latitude"-"longitude coordinates" and/or its "full address" versus "city name, state name or zip code" is the claimed "level of specificity of the context characteristic." Ex-1002 ¶¶116-126. Accordingly, Paretti discloses retrieving context data identified by the determined level of specificity of the context characteristic for the context parameter associated with the requested context information. *Id.*

g. Element 1[f]/21[e]/25[c][iv]: respond[ing] to the request for context information with the [determined] retrieved context data.

Paretti discloses responding to the request for context information with the retrieved context data.

After enforcing any privacy policies by applying the location reporting methodology to the location information, Paretti's visibility manager "will provid[e] the…location information to [the requesting] context-aware application[]." Ex-1005 ¶¶75, 81, 91, Figure 4; *see also id*. ¶¶36-44, 48-52, 70-73, 82-96; Ex-1002 ¶¶127-130.

2. Claim 3: wherein the establishing the context policy enforcement engine comprises establishing the context policy enforcement engine in software

Paretti discloses that "[e]ach of the elements of the various systems depicted in FIGS. 1, 2, 5, 7, 9, and 12 and each of the steps of flowcharts depicted in FIGS. 4, 6, 8, 10, and 11 may each be implemented by one or more processor-based computer systems," such as "computer system 1300…depicted in FIG. 13." Ex-1005 ¶164. Paretti discloses that computer system 1300 "includes a processing unit 1304 that includes one or more processors," "a main memory 1306, preferably random access memory (RAM), and may also include a secondary memory 1320." *Id*. ¶¶165-166. Paretti further discloses that "***[c]omputer programs***…are stored in main memory 1306 and/or secondary memory 1320," and, "***when executed, enable the***

computer system 1300 to implement features of the present invention as discussed herein." *Id*. ¶¶164-171 (emphasis added); Ex-1002 ¶¶131-137.

3. Claim 4: wherein receiving the request for context information comprises receiving the request for context information from a software application

Paretti discloses receiving a request "to access location information associated with the user" from a "context-aware application[]." Ex-1005 ¶¶36-44, 122, Figure 6; *see also, e.g.*, *id*. ¶¶47-52, 70-75, 82-92; Ex-1002 ¶¶138-146. Paretti further discloses that its "[c]ontext-aware applications…are intended to represent any application or service capable of consuming location information associated with a tracked entity and using such information to execute a function or perform a service on behalf of a user." Ex-1005 ¶41. Such applications "may include, for example, mobile communication or social networking applications that report location information about a user or a device associated with a user to other users" and "may include, for example, applications encompassed by or designed to operate in conjunction with the oneConnect™ mobile communication technology platform developed and commercialized by Yahoo! Inc." *Id*. ¶¶41-43; Ex-1002 ¶¶138-146.

4. Claim 5: wherein receiving the request for context information comprises receiving a request for at least one of: a location of the user, an activity of the user, an aspect of the environment in which the user is located, and biometric data related to the user

Paretti discloses receiving a request for a location of the user. For example, Paretti's Figure 6, at Step 602, discloses that the system receives a request "to access location information associated with the user." Ex-1005 ¶122, Figure 6; *see also, e.g.*, *id*. ¶¶36-44, 47-52, 70-75, 82-92; Ex-1002 ¶¶147-153.

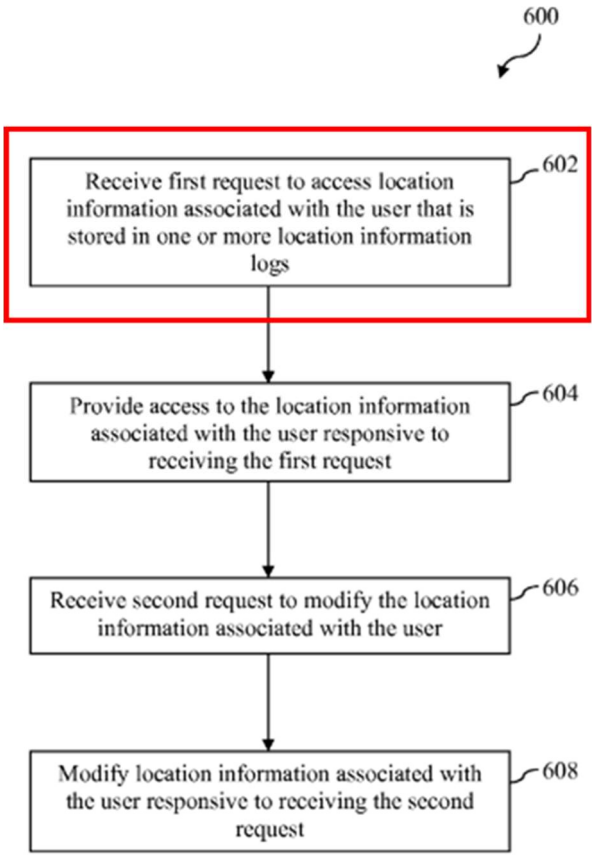

FIG. 6

5. Claim 7: wherein: the context policy data defines a context policy rule based on the identification of the requesting entity

Paretti discloses "access[ing] privacy policies" (i.e., the claimed "context policy data") that comprise "one or more conditions under which the location reporting methodology is to be enforced" as well as the "location reporting methodology" (i.e., the claimed "context policy rule") that "defines how location information…is to be provided to context-aware applications," including

"***selectively providing*** the user location information ***to certain applications***" and "***selectively modifying*** the content or granularity of the user location information ***based on a recipient application***" (i.e., the claimed "based on the identification of the requesting entity"). Ex-1005 ¶¶75, 84 (emphasis added); *see also id*. ¶¶82-99; Ex-1002 ¶¶154-157.

6. Claim 9: wherein the context policy data defines a rule based on a context parameter associated with the user

Paretti discloses that its "[p]rivacy policies [(i.e., the claimed "context policy data")] can be defined by a user in a highly flexible and context-specific manner such that the execution of a given privacy policy…is dependent on the existence of one or more social, topical, temporal or spatial conditions, which are also referred to herein as 'who, what, when and where' (W4) conditions [(i.e., the claimed "context parameter associated with the user")]."[4] Ex-1005 ¶¶36-44, 113-115; *see also id*. ¶¶82-92 ("The enforcement condition(s) associated with a location tracking privacy policy serve to specify a context within which the location reporting methodology is to be applied. The enforcement condition(s) may be based on any social, topical, temporal or spatial data or conditions associated with the user."). For example, "examples of privacy policies that are based on the location of a user include: a

[4] The '629 Patent discloses: "the context of the user may be defined by a plurality of context parameters (e.g., location, activity, environmental aspects, etc.)." Ex-1001, 5:38-54.

privacy policy that prevents location information from being reported about a user or that causes less granular location information to be reported about the user when the user is visiting a particular location…and does not want others to know that he/she is visiting the location." *Id*. ¶111; *see also id*. ¶¶100-115; Ex-1002 ¶¶158-164.

7. Claim 10: wherein the context policy data defines a rule based on the requested context information and a location of the user at the time of receiving the request for context information

Paretti discloses that its "[p]rivacy policies [(i.e., the claimed "context policy data")] can be defined by a user in a highly flexible and context-specific manner such that the execution of a given privacy policy…is dependent on the existence of one or more social, topical, temporal or spatial conditions." Ex-1005 ¶¶36-44, 113-115; *see also id*. ¶¶82-92. For example, "examples of privacy policies that are based on the location of a user include: a privacy policy that prevents location information from being reported about a user or that causes less granular location information to be reported about the user when the user is visiting a particular location…and does not want others to know that he/she is visiting the location" (i.e., the claimed "defines a rule based on the requested context information and a location of the user at the time of receiving the request for context information"). *Id*. ¶111; *see also id*. ¶¶100-115; Ex-1002 ¶¶165-168.

8. Claim 11: wherein the context policy data defines a rule based on the requested context information and the time of day at which the request for context information is received

Paretti discloses that its "[p]rivacy policies can be defined by a user in a highly flexible and context-specific manner such that the execution of a given privacy policy…is dependent on the existence of one or more social, topical, temporal or spatial conditions." Ex-1005 ¶¶36-44, 113-115; *see also id*. ¶¶82-92. For example, "a privacy policy may specify that during certain daytime hours, location information should be reported…at a first level of granularity but during evening hours, location information should be reported…at a second level of granularity." *Id*. ¶107; *see also id*. ¶¶100-115; Ex-1002 ¶¶169-172.

9. Claim 12: wherein the context policy data defines a rule based on the requested context information and an activity of the user

Paretti discloses that its "[p]rivacy policies can be defined by a user in a highly flexible and context-specific manner such that the execution of a given privacy policy…is dependent on the existence of one or more social, topical, temporal or spatial conditions." Ex-1005 ¶¶36-44, 113-115; *see also id*. ¶¶82-92. For example, "a user may enact a privacy policy that prohibits the reporting of location information…or that provides less granular location information…whenever the ***user is engaged in an activity*** associated with a certain topic." *Id*. ¶102 (emphasis added). "The user may set up such a privacy policy to take effect, for example,

whenever the user is engaged in an activity during which user privacy is important or during which the user wishes to avoid interruption by others;" "[s]uch activities may include any type of personal or professional activity." *Id*.; *see also id*. ¶¶100-115; Ex-1002 ¶¶173-177.

10. Claims 13, 22: wherein responding to the request comprises determining context data based on the set of rules of the context policy data

Paretti discloses that its "[p]rivacy policies can be defined by a user in a highly flexible and context-specific manner such that the execution of a given privacy policy…is dependent on the existence of one or more social, topical, temporal or spatial conditions, which are also referred to herein as 'who, what, when and where' (W4) conditions." Ex-1005 ¶¶36-44, 113-115; *see also id*. ¶¶82-92 ("The enforcement condition(s) associated with a location tracking privacy policy serve to specify a context within which the location reporting methodology is to be applied. The enforcement condition(s) may be based on any social, topical, temporal or spatial data or conditions associated with the user."). "[E]xamples of privacy policies that are based on the location of a user include: a privacy policy that…causes less granular location information to be reported about the user when the user is visiting a particular location…and does not want others to know that he/she is visiting the location." *Id*. ¶111; *see also id*. ¶¶100-115; Ex-1002 ¶¶178-182.

11. Claims 14, 23: wherein responding to the request further comprises retrieving the context data from a context database with the context policy enforcement engine based on the set of rules of the context policy data

Paretti's visibility manager "is configured to receive location information about a user from location tracking system interface" (i.e., the claimed "wherein responding to the request further comprises retrieving the context data from a context database with the context policy enforcement engine")[5] "and to automatically control how such…location information is to be provided to context-aware applications" (i.e., the claimed "based on the set of rules of the context policy data"). Ex-1005 ¶75; *see also id*. ¶¶36-44, 47-56, 70-73, 82-92, 116-117; Ex-1002 ¶¶183-190. This may include, for example, "providing the…location information in an unmodified fashion," "modifying the content of the…location information," "providing the…location information only at a specified level of granularity," and/or "selectively modifying the…granularity of the…location information based on a recipient application." Ex-1005 ¶84; *see also id*. ¶¶82-92; Ex-1002 ¶¶183-190.

[5] Paretti discloses that "[t]he user location information received in step 404 may be indicative of a past, current or future location of the user. Furthermore, the user location information received in step 404 may comprise actual location information (e.g., latitude/longitude coordinates, zip code, street address, or the like) as well as relative location information that indicates or identifies the proximity of the user to other users, devices, beacons, or the like." Ex-1005 ¶89. A POSITA would have found it obvious for retrieving said user location information to comprise retrieving from a context database. Ex-1002 ¶¶183-190.

12. Claim 15: wherein responding to the request further comprises transmitting the context data

After enforcing any privacy policies by applying the location reporting methodology to the location information, Paretti's visibility manager "will provid[e] the…location information to [the requesting] context-aware application[]." Ex-1005 ¶¶75, 81, 91, Figure 4; *see also id*. ¶¶36-44, 48-52, 70-73, 82-92, 93-99; Ex-1002 ¶¶191-195.

13. Claims 16, 24: wherein determining the context data comprises selecting context data from a plurality of datum defining a context parameter of the user, the plurality of datum having different levels of specificity defined in the set of rules of the context policy data

Paretti's visibility manager "is configured to receive location information [(i.e., the claimed "context parameter")] about a user from location tracking system interface" "and to automatically control how such…location information is to be provided to context-aware applications." Ex-1005 ¶75; *see also id*. ¶¶36-44, 47-52, 70-73, 82-92. This may include, for example, "providing the…location information in an unmodified fashion" and/or "providing the…location information only at a specified level of granularity." Ex-1005 ¶84; *see also id*. ¶¶82-92; Ex-1002 ¶¶196-200.

14. Claim 18: further comprising: receiving user-supplied context policy rule with the mobile computing device, and updating the context policy data with the user-supplied context policy rule with the context policy enforcement engine

Paretti discloses that its user interface allows a user to interact with the location tracking privacy engine to define "privacy policies" that govern how location information is provided to context-aware applications. Ex-1005 ¶¶44, 49; *see also id*. ¶¶36-52, 76-79, 100-104, 138-149, 155-159; Ex-1002 ¶¶201-207.

15. Claim 19: further comprising: receiving user-supplied context data related to the user with the mobile computing device, and updating a context database stored on the mobile computing device with the user-supplied context data

Paretti discloses that "[o]ther information…may be useful in specifying and/or enforcing a privacy policy" "(e.g., social information, topical information, temporal information or spatial information associated with the user)" and may be "provided by a user" "via user interface" and "stored in W4 data database." Ex-1005 ¶49; *see also id*. ¶¶39, 53-69, 100-115; Ex-1002 ¶¶208-216.

B. Ground 2: Claims 1, 3-5, 7-8, 13-16, 18, and 20-25 are rendered obvious by Parupudi in view of Nykanen.

1. A POSITA would have been motivated to combine Parupudi with Nykanen's teachings and would have had a reasonable expectation of success in doing so.

In addition to the reasons set out below with respect to specific claim elements, a POSITA would have been motivated to combine the teachings of

Parupudi and Nykanen and would have had a reasonable expectation of success in doing so, especially as each relates to the same technologies. Ex-1002 ¶¶217-219. In fact, both relate to identity-based privacy preferences in context-aware computer systems. Ex-1006, Abstract; Ex-1007, Abstract. And both describe using privacy policies to provide requesting entities with a device's location information at varying levels of specificity. Ex-1006, 23:65-67, 24:5-7, Figure 10; Ex-1007, Title, Abstract, 3:44-4:23, 4:24-5:38. Although Parupudi discloses allowing a user to assign privacy levels, which correspond to location data of varying levels of specificity, to location-requesting entities, Nykanen provides further details describing establishing, accessing, and utilizing a database in order to allow a user to "specify his privacy preferences to [a] database" with assurance that they will "be adhered to by all location providing sources," thus ensuring that the user will have "direct control over which applications and web services have access to data concerning [his] location." Ex-1007, Abstract.

A POSITA would have been motivated to apply Nykanen's additional teachings regarding allowing a user to "specify his privacy preferences to [a] database," and thus establishing, accessing, and utilizing said database accordingly, to Parupudi to enhance the privacy-protecting capabilities of the device. Ex-1002 ¶¶217-219. Indeed, Parupudi explains that "[i]t may be desirable, in some instances, to filter the information that is provided to various applications" as "it is entirely

likely that a user may not want their specific location information provided to untrusted applications" but, instead, "might just desire for location service module 602 to inform such applications that the user is in the State of Washington." Ex-1006, 24:8-25:45. And Parupudi recognized the privacy-protecting benefits of allowing a user to assign privacy levels, which correspond to location data of varying levels of specificity, to location-requesting entities as it discloses "address[ing]" "privacy issues" with a "privacy manager that functions to modulate the information that is provided to the various applications as a function of the applications' identities and security policies on the device." *Id*., 3:10-14; *see also id*., 24:8-25:45. Nykanen discloses a similar goal and method, describing a system in which "a user can specify his privacy preferences to one database" with assurance that they will "be adhered to by all location providing sources," thus ensuring that the user will have "direct control over which applications and web services have access to data concerning the location of his mobile." Ex-1007, Abstract; *see also id*., 2:35-37, 2:44-46. Based on the teachings of Nykanen, a POSITA would have recognized that incorporating a "database" allowing a user to "specify his privacy preferences" (and thus establishing, accessing, and utilizing said database accordingly) in Parupudi's disclosed system would have enhanced Parupudi's privacy-protecting benefits. Ex-1002 ¶¶217-219. This would provide a more user-friendly, feature-rich system, and thus design incentives and market forces would have motivated a POSITA to

apply the teachings of Nykanen to Parupudi. *Id*.; *Dystar Textilfarben Gmbh v. C.H. Patrick Co.*, 464 F.3d 1356, 1368 (Fed. Cir. 2006) (explaining that the Federal Circuit has "repeatedly held that an implicit motivation to combine exists not only when a suggestion may be gleaned from the prior art as a whole, but when the 'improvement' is technology-independent and the combination of references results in a product or process that is more desirable…because it is stronger, cheaper, cleaner, faster, lighter, smaller, more durable, or more efficient").

Moreover, implementing Nykanen's database-related mechanisms into Parupudi's system would have been a straightforward engineering task for a POSITA. Ex-1002 ¶¶217-219. Indeed, both Parupudi and Nykanen disclose general purpose computing devices that work in the same general way and that a POSITA would have understood were capable of using the same and/or similar programming languages and/or operating systems. *Id*. Accordingly, a POSITA would have had a reasonable expectation of success in implementing the approaches described in Nykanen into Parupudi's system as the implementation would have been a matter of straightforward engineering and thus would have yielded predictable results. *Id*. Indeed, a POSITA would have understood that numerous commercial and open-source database implementation methods were available and that their use involved only a straightforward engineering task. *Id*. Moreover, for example, a POSITA would have understood that the approaches described in Nykanen were all

straightforward programming tasks that would not differ substantially in implementation between computing devices, and, accordingly, would have found it a straightforward engineering task to implement the approaches in Parupudi's system. *Id*.

2. Independent Claims 1, 21, and 25

a. Element 1[pre]: A method comprising:

Parupudi discloses "identity-based context aware computing systems ***and methods***." Ex-1006, Title (emphasis added); *see also id*. Abstract, 24:9-25:45, Figure 10; Ex-1002 ¶¶220-224.

b. Element 1[a]/21[a]: establishing a context policy enforcement engine on a mobile computing device;

Element 25[pre]: A mobile computing device comprising:
Element 25[a]: a context policy enforcement engine;

Parupudi in combination with Nykanen teaches establishing a context policy enforcement engine on a mobile computing device.

Parupudi discloses "mobile computing devices (e.g. laptop computers and the like), and/or hand-held computing devices (e.g. palm PCs, wireless telephones and the like)" that include a "privacy manager" (i.e., the claimed "context policy enforcement engine") "that functions to modulate the information that is provided to…various applications as a function of the applications' identities and security policies on the device." Ex-1006, 3:10-15, 7:54-65, 24:10-19; *see also id*., Abstract,

18:53-67, 23:36-24:7 ("a security policy or privacy policy can be applied to the information before it is returned to the applications"); Ex-1002 ¶¶225-242.

Parupudi's privacy manager "determines what level of information to provide to applications that…request" "location information." Ex-1006, 6:59-67. Thus, the "privacy manager…addresses privacy concerns" as "it is entirely likely that a user may not want their specific location information provided to untrusted applications" (e.g., "[i]n these instances a user might just desire for location service module…to inform such applications that the user is in the State of Washington"). *Id*., 24:9-30. Accordingly, a "user is able to assign a privacy level to entities that might request location information" such that "[w]hen a query from an application is received, the privacy manager first determines who the query is from and the privacy level associated with the application." *Id*., 7:1-15.

Parupudi's Figure 10 depicts a flow diagram describing "the steps in a privacy protection method" implemented by the privacy manager. *Id*., 24:31-34.

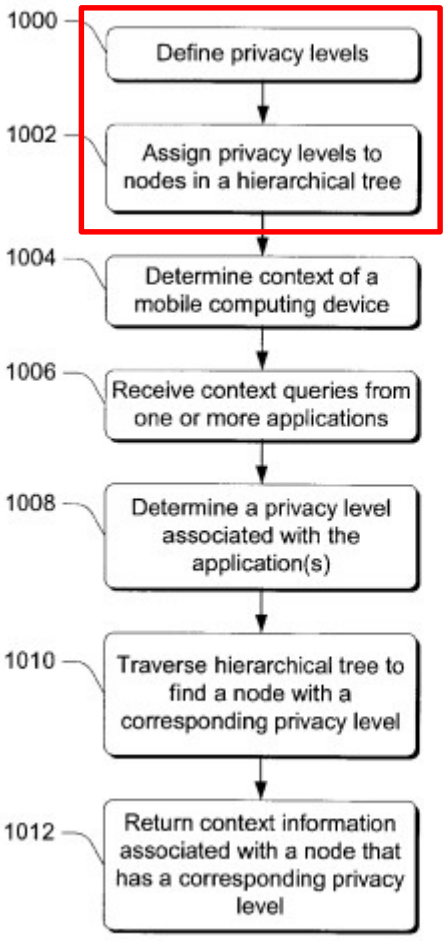

Fig. 10

At Steps 1000 and 1002, privacy levels (i.e., of the claimed "context policy enforcement engine") are defined and assigned. *Id*., Figure 10; Ex-1002 ¶¶225-242. A "scale of privacy levels are defined" such that "[e]ach level is defined to include more or less specific information about the location of [the] device." Ex-1006, 3:55-7:51. For example, "10 different privacy levels" may be defined such that "a privacy level of 0 means that no location information is returned" and a "privacy level of 90 means that very detailed location information is returned." *Id*., 24:55-25:45. Then, users may assign "various privacy levels" "to the individual nodes in one or more

hierarchical tree structures" (e.g., "each node of the Master World and the Secondary Worlds can have a privacy level associated with it" such that the "root node of the Master World tree structure might have a privacy level of 10, while the node that represents a current location in a Secondary World might have a privacy level of 90"). *Id*. For example, a user might assign "a web site that gives up to the minute weather of various locations" "a privacy level of 60" in order to "receive weather information [that] corresponds to [his] postal code" and "a corporation intranet web site that is a trusted web site" "a privacy level of 90" in order to "give them precise location information as to [his] whereabouts." *Id*.; *see also id*., Claims 1, 10, 14, 20, 25. Accordingly, Parupudi's privacy manager is a "context policy enforcement engine." Ex-1002 ¶¶225-242.

Although Parupudi discloses a "context policy enforcement engine," Nykanen provides further details describing establishing a context policy enforcement engine on a mobile computing device. Ex-1007, Abstract, 3:44-4:23, 4:24-5:38. Indeed, Nykanen discloses a system and method that allows a user to "specify his privacy preferences to [a] database" with assurance that they will "be adhered to by all location providing sources," thus ensuring that the user will have "direct control over which applications and web services have access to data concerning the location of his mobile." *Id*., Abstract. More specifically, Nykanen discloses with Figure 1 that its "privacy control module" "interfaces" with its "privacy profile database" and

"decides whether to allow or disallow" an application's request for location data. *Id*., 3:44-4:23. "To comply with one or more of the rules" concerning the user's privacy preferences, "privacy control…might instruct positioning service…to limit to a certain level the accuracy of the location information provided to [the] application." *Id*.; *see also id*., Figure 1, Claims 1, 9, 17, 19; Ex-1002 ¶¶225-242. Nykanen's privacy control module in the terminal (i.e., the claimed "mobile computing device") is "a context policy enforcement engine." Ex-1002 ¶¶225-242.

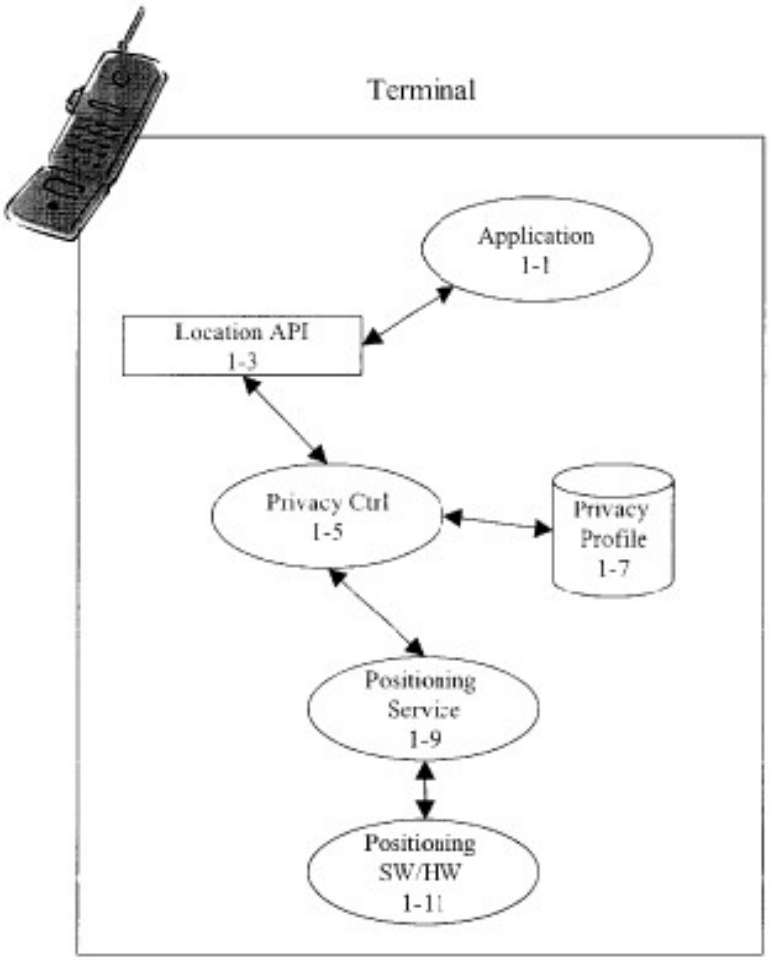

FIG. 1

Thus, for example, "when the rule 'AllowAllLocationRequests' is in effect," the terminal's location data is provided to any requesting application "so long as the requested level of accuracy is no greater than the level of accuracy specified in the 'Rule Variables' field" (e.g., "it may be specified that requestors only be able to determine the terminal's location to within a 250 meter radius" or "it may be specified that the requestors be allowed to determine the user's location with as much

accuracy as possible"). Ex-1007, 4:24-5:38. Similarly, the "rule 'AllowTheseRequestersDisallowOthers,' when in effect, allows access only to requesters that are noted in the 'Rule Variables' field (or that are members of the use groups specified in the 'Rule Variables' field) and that request a level of accuracy no higher than that specified for them," and the "rule 'DisallowTheseRequestersAllowOthers,' when in effect, behaves in a similar manner but disallows the specified requesters or use groups from accessing terminal location data…while allowing others so long as the[] requests do not exceed the specified allowed location accuracy." *Id*. Thus, the "'rule variables' field" may "contain an array of the names of applications or use groups" and "specif[y] for each the highest level of location accuracy that may be requested." *Id*. Accordingly, Nykanen discloses establishing a context policy enforcement engine on a mobile computing device. Ex-1002 ¶¶225-242.

A POSITA would have been motivated to apply Nykanen's additional teachings regarding establishing a context policy enforcement engine on a mobile computing device to Parupudi to enhance the privacy-protecting capabilities of the device. *Id*. In particular, a POSITA would have recognized that applying Nykanen's teachings regarding establishing a context policy enforcement engine on a mobile computing device to Parupudi's system would further Parupudi's privacy-protecting goals as it would provide further opportunities for ensuring that a user's "privacy

preferences" will "be adhered to by all location providing sources" (Ex-1007, Abstract), as taught by Nykanen. Ex-1002 ¶¶225-242. Indeed, Nykanen teaches that "[t]o have…control" over the "security and privacy" of his "location data," "a user must be able to make sure all sources of location information comply with his wishes concerning privacy." Ex-1007, 2:35-37, 2:44-46. To that end, Nykanen teaches establishing a local privacy-preference database and then mirroring its contents to one or more remote databases to ensure the user's privacy preferences are followed regardless of whether "the user is mostly making use of local location-based applications" or "he [i]s mostly using remote location-based applications and/or web services." *See, e.g.*, *id*., 10:15-12:6, Claim 1. Accordingly, a POSITA would have recognized, for example, that applying Nykanen's teachings regarding establishing a context policy enforcement engine on a mobile computing device to Parupudi's system would allow Parupudi's device to maintain its privacy preferences locally, for their application locally, in addition to allowing for their application remotely as well. Ex-1002 ¶¶225-242. A POSITA would have recognized that such expanding functionality for a privacy-preferences database would further Parupudi's privacy-protecting goals. *Id*.

Moreover, a POSITA would have had a reasonable expectation of success in implementing Nykanen's additional teachings regarding establishing a context policy enforcement engine on a mobile computing device into Parupudi's system as

the implementation would have been a straightforward engineering task. *Id*. In particular, a POSITA would have understood that both Parupudi and Nykanen disclose general purpose computing devices that work in the same general way and are capable of using the same and/or similar programming languages and/or operating systems and that Nykanen's approaches regarding establishing a context policy enforcement engine involved only straightforward programming tasks that would not differ substantially in implementation between computing devices. *Id*.

c. Element 21[pre]: A non-transitory, machine readable medium comprising a plurality of instructions, that in response to being executed, result in a computing device:

Element 25[b]: a processor; and
Element 25[c]: a memory device having stored therein a plurality of instructions, which when executed by the processor, cause the context policy enforcement engine to:

Parupudi discloses a non-transitory, machine readable medium comprising (or a memory device having stored therein) a plurality of instructions, that in response to being executed (by a processor), result in a computing device. Parupudi's disclosed "computing devices" may "include one or more processors, computer-readable media (such as storage devices and memory), and software executing on the one or more processors that cause the processors to implement a programmed functionality." Ex-1006, 7:54-65. Moreover, Parupudi discloses that its computing

devices may further comprise "system memory" (e.g., "read only memory (ROM)" and "random access memory (RAM)") wherein the "drives and their associated computer-readable media provide nonvolatile storage of computer-readable instructions, data structures, program modules and other data." *Id*., 7:67-9:36. Parupudi's invention "includes these and other various types of computer-readable storage media when such media contain instructions or programs for implementing the steps described…in conjunction with a microprocessor or other data processor" and "also includes the computer itself when programmed according to the methods and techniques described." *Id*., 9:15-30; *see also id*., 7:67-9:36, 24:9-25:45, Claims 10, 20, 25; Ex-1002 ¶¶243-249.

d. Element 1[b]: receiving, from a requesting entity, a request for context information related to a user of the mobile computing device,
Element 1[c]/21[b]/25[c][i]: retriev[e/ing] context policy data [] with the context policy enforcement engine [], the context policy data defining a set of rules for responding to context requests;

Parupudi discloses receiving, from a requesting entity, a request for context information related to a user of the mobile computing device. Parupudi discloses that "[i]ndividual applications...call [a] location service module." Ex-1006, 25:3-5; *see also id*., Abstract, 2:48-68, 3:55-7:51. Moreover, Parupudi discloses with Figure 10, at Step 1006, that "context queries from one or more applications" are received. *Id*., 25:8-10, Figure 10; *see also id*., 22:54-23:35, 23:36-24:7, 24:9-25:45, 17:37-18:51

("[T]he applications 608 can make calls to the device to ask the device where it is located. The device is configured to receive the calls and respond in an appropriate manner to the application."), Claim 1 ("receiving a query from an application that requests context information pertaining to the context of the computing device"), Claims 10, 14, 20, 25, 34; Ex-1002 ¶¶250-262.

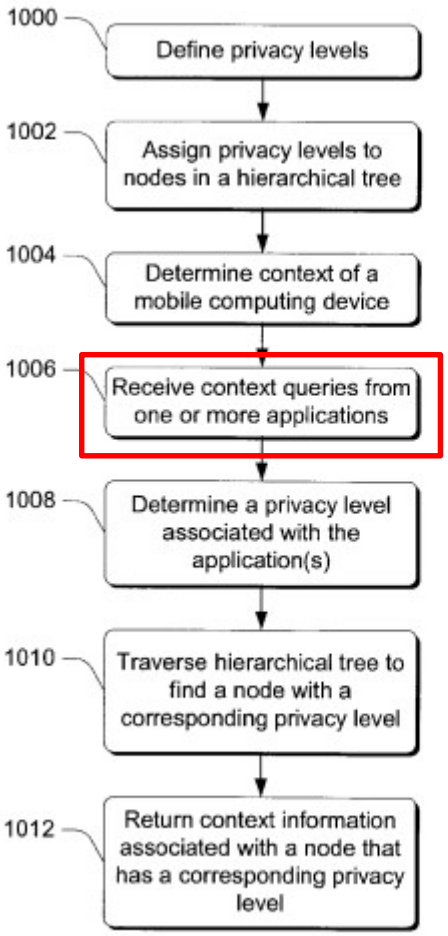

Fig. 10

Parupudi in combination with Nykanen teaches the context policy enforcement engine retrieving context policy data which defines a set of rules for responding to context requests.

Parupudi discloses "[w]hen a query from an application is received, the privacy manager first determines who the query is from and the privacy level associated with the application or entity" so that "a security policy or privacy policy can be applied to the information before it is returned to the applications," and thus Parupudi's system retrieves context policy data in response to receiving a request for context information related to a user of the computing device. Ex-1006, 7:1-15, 23:36-24:7; Ex-1002 ¶¶250-262. Indeed, as shown in Figure 10, at Step 1008, the system "determines the privacy level associated with the application or applications." Ex-1006, 25:11-13, Figure 10.

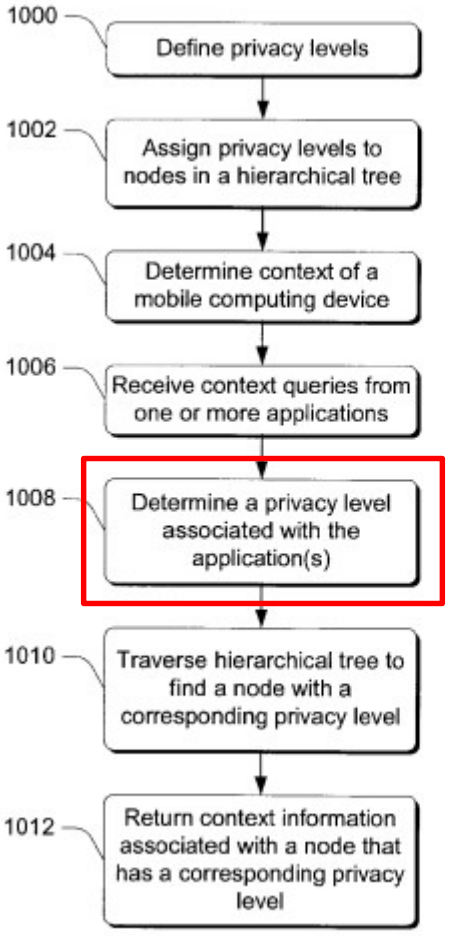

Fig. 10

These privacy levels may be defined such that, for example, "no location information is returned" or "very detailed location information is returned" (e.g., a user might assign "a web site that gives up to the minute weather of various locations" "a privacy level of 60" in order to "receive weather information [that] corresponds to [his] postal code" and "a corporation intranet web site that is a trusted web site" "a privacy level of 90" in order to "give them precise location information as to [his] whereabouts"). *Id*., 24:55-25:45.

Although Parupudi discloses retrieving context policy data in response to receiving a request for context information related to a user of the computing device, Nykanen provides further details describing retrieving context policy data with the context policy enforcement engine, the context policy data defining a set of rules for responding to context requests. Ex-1007, 4:5-8, 4:24-5:38, Claim 1. Indeed, Nykanen discloses that its privacy control module (i.e., the claimed "context policy enforcement engine") "interfaces with privacy profile database" to determine "whether to allow or disallow application['s] information request." *Id*., 4:5-8. More specifically, Nykanen discloses "receiving from a local application a request for location information concerning a terminal upon which it is stored," and, in response, "consulting a database containing privacy preferences." *Id*., Claim 1; Ex-1002 ¶¶250-262.

Nykanen's Figure 1-a "shows an example prototypical ruleset which could be implemented in profile database." Ex-1007, 4:24-5:38. The profile database comprises a "Rule Variables" field, which may "contain an array of the names of applications or use groups" and "specif[y] for each the highest level of location accuracy that may be requested." *Id*. And the ruleset may provide, for example, an "AllowAllLocationRequests" rule, in which the terminal's location data is provided to any requesting application "so long as the requested level of accuracy is no greater than the level of accuracy specified in the 'Rule Variables' field" (e.g., "within a 250

meter radius" or "with as much accuracy as possible"), and an "AllowTheseRequestersDisallowOthers" rule, in which the terminal's location data is provided only to "requesters that are noted in the 'Rule Variables' field (or that are members of the use groups specified in the 'Rule Variables' field) and that request a level of accuracy no higher than that specified for them." *Id*. Accordingly, Nykanen discloses retrieving context policy data with the context policy enforcement engine, the context policy data defining a set of rules for responding to context requests. Ex-1002 ¶¶250-262.

A POSITA would have been motivated to apply Nykanen's additional teachings regarding retrieving context policy data with the context policy enforcement engine, the context policy data defining a set of rules for responding to context requests, to Parupudi to enhance the privacy-protecting capabilities of the device. *Id*. In particular, a POSITA would have recognized that applying Nykanen's teachings regarding retrieving context policy data defining a set of rules for responding to context requests to Parupudi's system would further expand the functionality of a privacy-preferences database, which would further Parupudi's privacy-protecting goals. *Id*. And a POSITA would have had a reasonable expectation of success in implementing Nykanen's additional teachings regarding retrieving context policy data into Parupudi's system as the implementation would have been a straightforward engineering task. *Id*. In particular, a POSITA would

have understood that both Parupudi and Nykanen disclose general purpose computing devices that work in the same general way and are capable of using the same and/or similar programming languages and/or operating systems and that Nykanen's approaches regarding retrieving context policy data involved only straightforward programming tasks that would not differ substantially in implementation between computing devices. *Id*.

e. Element 1[d]/21[c]/25[c][ii]: determin[e/ing] a level of specificity of a context characteristic for a context parameter associated with the requested context information as a function of the context policy data and an identity of [the/a] requesting entity [that requested the context information];

Parupudi in combination with Nykanen teaches determining a level of specificity of a context characteristic for a context parameter associated with the requested context information as a function of the context policy data and an identity of the requesting entity.

Parupudi discloses that its privacy manager "functions to modulate the information that is provided to the various applications as a function of the applications' identities and security policies on the device." Ex-1006, 3:10-15; *see also id*., 23:36-24:7 ("a security policy or privacy policy can be applied to the information before it is returned to the applications"). As a result, the "privacy manager determines what level of information to provide to applications that might

request the information." *Id.*, 6:59-7:15 ("[A] scale of privacy levels are defined…to [each] include more or less specific information about the location of [the] device…. A user is able to assign a privacy level to entities that might request location information…. When a query from an application is received, the privacy manager first determines who the query is from and the privacy level associated with the application or entity."). Indeed, as shown in Figure 10, at Step 1008, the system "determines the privacy level associated with the application or applications." *Id.*, 25:11-13, Figure 10.

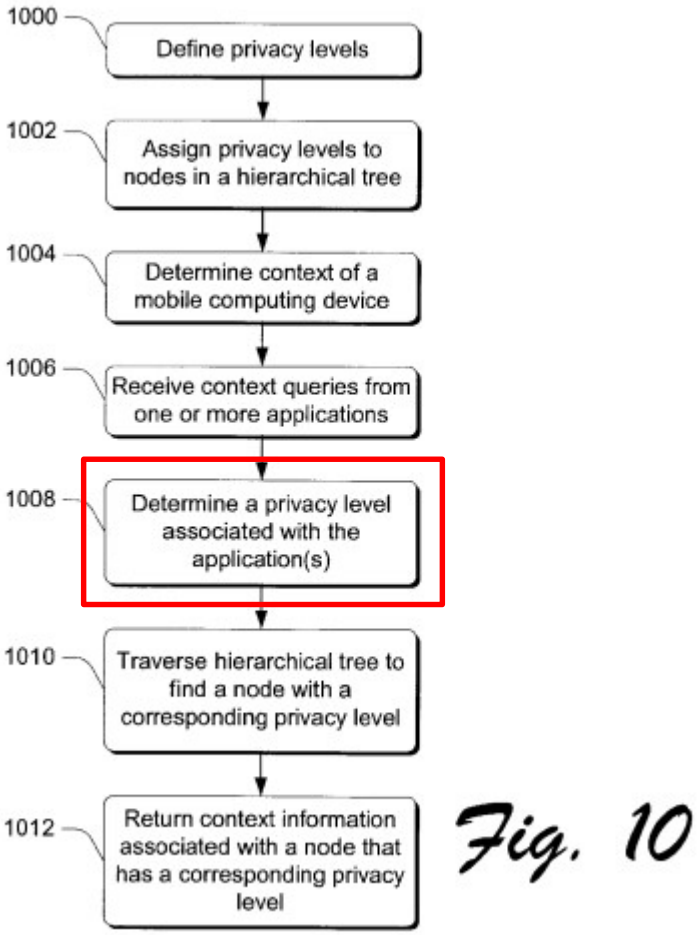

Fig. 10

For example, "a user may not want their specific location information [(i.e., the claimed "context parameter")] provided to untrusted applications" and instead "just desire for location service module" "to inform such applications that the user is in the State of Washington" [(i.e., the claimed "context characteristic")]. *Id*., 24:26-30; *see also id*., 12:62-13:47 ("For example, if a computing device determines that it is currently located at a node that corresponds to the City of Redmond, it can traverse the Master World tree structure to ascertain that it is in the State of Washington, Country of The United States, on the continent of North America."), 13:49-15:25 ("Master World 300 includes the following nodes: World, United States, Washington, Redmond, and Zip=98052. The exemplary Secondary World 302 is a hierarchical tree structure that has been defined by Microsoft Corporation and includes the following nodes: Microsoft, Redmond Campus, 1 Microsoft Way, Building 26, 3rd floor, Conference Room 3173, Building 24, 2nd floor, Conference Room 1342."). Accordingly, Parupudi discloses determining a level of specificity of a context characteristic. Ex-1002 ¶¶263-273.

Although Parupudi discloses determining a level of specificity of a context characteristic, Nykanen provides further details describing determining a level of specificity of a context characteristic for a context parameter associated with the requested context information as a function of the context policy data and an identity of the requesting entity. Ex-1007, 3:44-4:23, 4:24-5:38, Claim 1. Indeed,

Nykanen discloses that its "privacy control module" "interfaces" with its "privacy profile database" and "decides whether to allow or disallow" an application's request for location data. *Id*., 3:44-4:23. More specifically, Nykanen discloses "determining whether [an] application is entitled to receive the requested location information" [(i.e., the claimed "context parameter")] and "determining what source from a set of potential sources to use to provide said…application with the requested location information." *Id*., Claim 1. "To comply with one or more of the rules" concerning the user's privacy preferences, "privacy control…might instruct positioning service…to limit to a certain level the accuracy of the location information provided to [the] application." *Id*., 3:44-4:23. Thus, for example, if the "Rule Variables" field in the profile database corresponding to a particular application "specifies [that] the highest level of location accuracy that [it] may request[]" is "within a 500 meter radius," and the "AllowAllLocationRequests" rule is in effect, then the system will provide the application location information in response to requests for location data "within a 500 meter radius" (i.e., the claimed "context characteristic"). *Id*., 4:24-5:38. Or, for example, if the "Rules Variable" field of the profile database indicates that a particular application is able "determine the terminal's location to within a 250 meter radius" and the "AllowTheseRequestersDisallowOthers" rule is in effect, then the system will provide the application location information in response to requests for location

data "within a 250 meter radius" (i.e., the claimed "context characteristic"). *Id*. Accordingly, Nykanen discloses determining a level of specificity of a context characteristic for a context parameter associated with the requested context information as a function of the context policy data and an identity of the requesting entity. Ex-1002 ¶¶263-273.

A POSITA would have been motivated to apply Nykanen's additional teachings regarding determining a level of specificity of a context characteristic for a context parameter associated with the requested context information as a function of the context policy data and an identity of the requesting entity to Parupudi to enhance the privacy-protecting capabilities of the device. *Id*. In particular, a POSITA would have recognized that applying Nykanen's teachings regarding determining a level of specificity as a function of the context policy data and the identity of the requesting entity to Parupudi's system would further expand the functionality of a privacy-preferences database, which would further Parupudi's privacy-protecting goals. *Id*. And a POSITA would have had a reasonable expectation of success in implementing Nykanen's additional teachings regarding determining a level of specificity of a context characteristic into Parupudi's system as the implementation would have been a straightforward engineering task. *Id*. In particular, a POSITA would have understood that both Parupudi and Nykanen disclose general purpose computing devices that work in the same general way and

are capable of using the same and/or similar programming languages and/or operating systems and that Nykanen's approaches regarding determining a level of specificity of a context characteristic involved only straightforward programming tasks that would not differ substantially in implementation between computing devices. *Id*.

f. Element 1[e]/21[d]/25[c][iii]: retriev[e][ing] context data identified by the determined level of specificity of the context characteristic for the context parameter associated with the requested context information; and

Parupudi in combination with Nykanen teaches retrieving context data identified by the determined level of specificity of the context characteristic for the context parameter associated with the requested context information.

Parupudi discloses with Figure 10, at Step 1010, that the privacy manager "traverses…one or more hierarchical tree structures to find a node with a corresponding privacy level so that it can select the information that is associated with that node." Ex-1006, 25:16-19, Figure 10; *see also id*., 24:9-25:45, Abstract ("Device context information is then selected in accordance with the privacy level of the application from which the query was received."), Claims 1, 10, 25, 34.

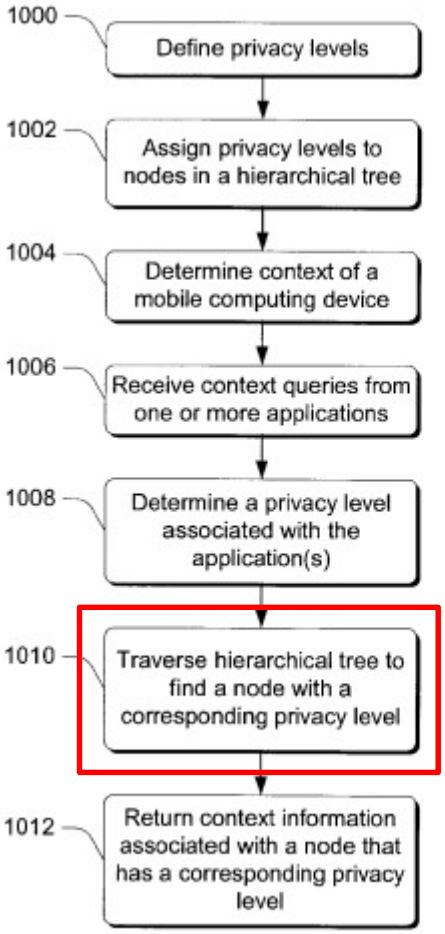

Fig. 10

This hierarchical tree structure "is useful because it can be used to determine the…location of a place anywhere in the world and at any definable granularity." *Id*., 3:55-4:5, Figures 2-3; *see also id*., 3:55-7:51 (describing the disclosed hierarchical tree structure wherein "each node of the Master World and a Secondary World can have a privacy level associated with it" such that the "privacy manager…evaluates one or more of the Master World and the Secondary World to find a node that has a corresponding privacy level" with "information at

that particular granularity"). Accordingly, Parupudi discloses retrieving appropriate context data. Ex-1002 ¶¶274-284.

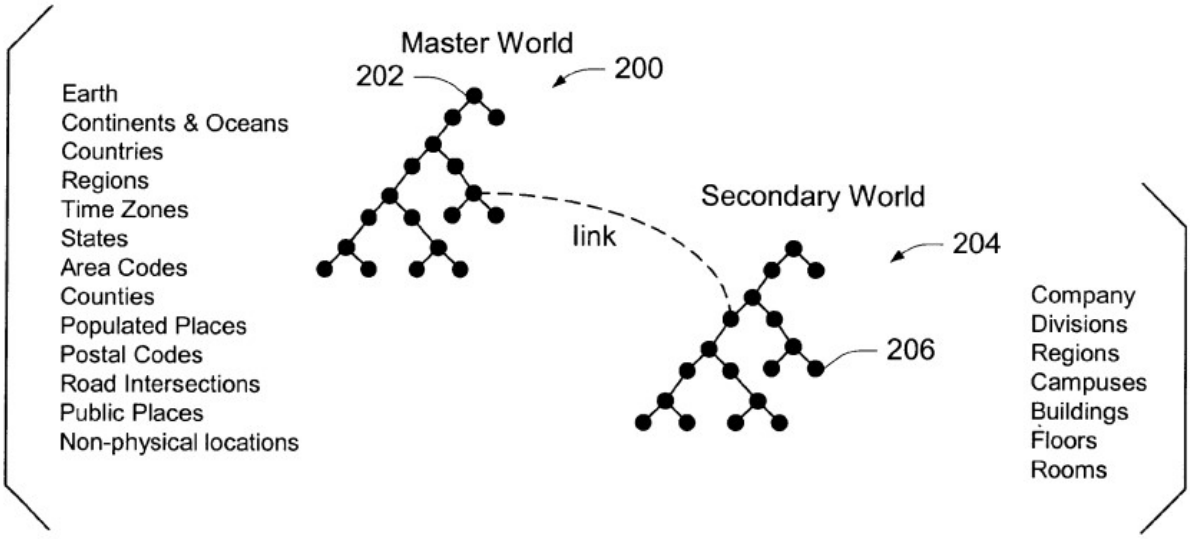

Fig. 2

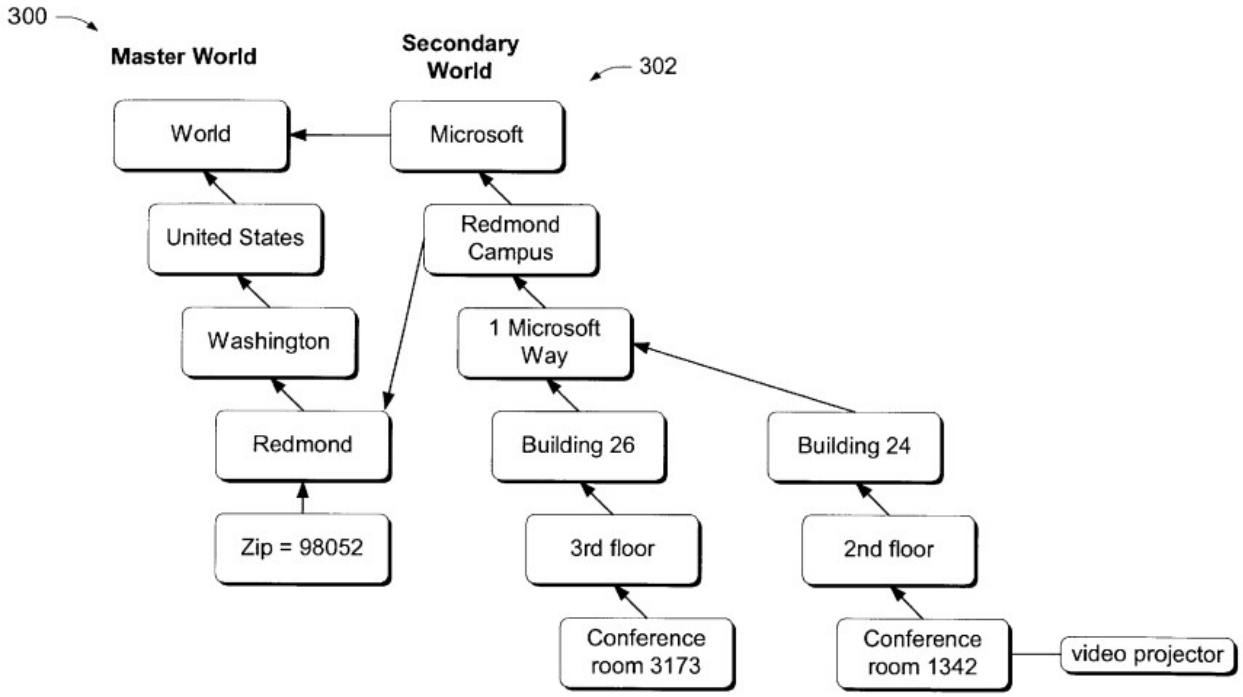

Fig. 3

Although Parupudi discloses retrieving context data, Nykanen provides further details describing retrieving context data identified by the determined level of specificity of the context characteristic for the context parameter associated with the requested context information. Ex-1007, 3:42-4:23, 4:24-5:38, Claim 1. Indeed, Nykanen discloses that, in order to comply with its privacy policy rules, "privacy control…might instruct positioning service…to limit to a certain level the accuracy of the location information provided to application." *Id*., 3:42-4:23. "This may be implemented by having positioning service…instruct positioning software/hardware…to provide it with a specified level of position accuracy, or by

having positioning service…alter the location information received from positioning SW/HW…before passing it on so as to limit the level of location accuracy." *Id*. Indeed, Nykanen discloses "determining what source from a set of potential sources to use to provide said local application with the requested location information" "and providing to said local application location information which originated from the determined source in the case where it is determined that said local application is entitled to receive it." *Id*., Claim 1. Thus, Nykanen's system may, for example, retrieve location data consistent with a determination that the "requestor[] [is] only…able to determine the terminal's location to within a 250 meter radius," or, for example, it may retrieve location data "with as much accuracy as possible." *Id*., 4:24-5:38.

"If privacy control module 1-5 decides to disallow application 1-1's request, it would inform application 1-1 of the decision and would not allow the application to receive the requested information." *Id*. More specifically, Nykanen discloses "determining whether [an] application is entitled to receive the requested location information" and "determining what source from a set of potential sources to use to provide said…application with the requested location information." *Id*., Claim 1. Accordingly, Nykanen discloses retrieving context data identified by the determined level of specificity of the context characteristic for the context parameter associated with the requested context information. Ex-1002 ¶¶274-284.

A POSITA would have been motivated to apply Nykanen's additional teachings regarding retrieving context data identified by the determined level of specificity of the context characteristic for the context parameter associated with the requested context information to Parupudi to enhance the privacy-protecting capabilities of the device. *Id*. In particular, a POSITA would have recognized that applying Nykanen's teachings regarding retrieving context data identified by the determined level of specificity to Parupudi's system would further expand the functionality of a privacy-preferences database, which would further Parupudi's privacy-protecting goals. *Id*. And a POSITA would have had a reasonable expectation of success in implementing Nykanen's additional teachings regarding retrieving context data identified by the determined level of specificity into Parupudi's system as the implementation would have been a straightforward engineering task. *Id*. In particular, a POSITA would have understood that both Parupudi and Nykanen disclose general purpose computing devices that work in the same general way and are capable of using the same and/or similar programming languages and/or operating systems and that Nykanen's approaches regarding retrieving context data identified by the determined level of specificity involved only straightforward programming tasks that would not differ substantially in implementation between computing devices. *Id*.

g. Element 1[f]/21[e]/25[c][iv]: respond[ing] to the request for context information with the [determined] retrieved context data.

Parupudi discloses responding to the request for context information with the retrieved context data. Parupudi discloses with Figure 10, at Step 1012, that the privacy manager "returns the context information (e.g. location information) associated with the node," such as by having "the location service module…inform the application that the user's location is the State of Washington." Ex-1006, 25:22-27, Figure 10; *see also id*., 2:20-3:21, 17:37-18:51, 23:36-24:7, Abstract ("The selected device context information is then returned to the application from which the query was received."), 7:1-15 ("When a corresponding node is found, information at that particular granularity is provided to the requesting application or entity."), 22:54-23:35 ("the device might respond to the query by returning the state in which the user is making the purchase"), Claim 1 ("returning the selected device context information to the application from which the query was received"); Ex-1002 ¶¶285-288.

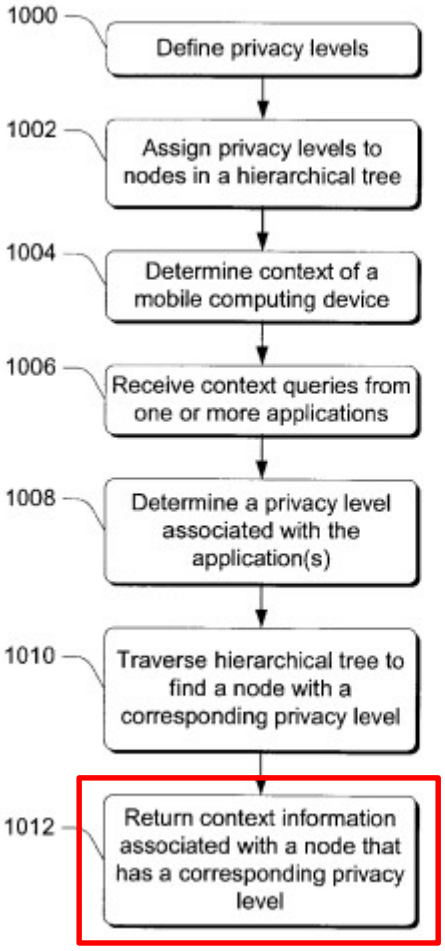

Fig. 10

3. Claim 3: wherein the establishing the context policy enforcement engine comprises establishing the context policy enforcement engine in software

Parupudi discloses "mobile computing devices" that include a "privacy manager that functions to modulate the information that is provided to…various applications as a function of the applications' identities and security policies on the device." Ex-1006, 3:10-15, 7:54-65, 24:10-19. These "computing devices" may "include one or more processors, computer-readable media (such as storage devices and memory), and software executing on the one or more processors that cause the

processors to implement a programmed functionality." *Id*., 7:54-65. Parupudi's invention "includes these and other various types of computer-readable storage media when such media contain instructions or programs for implementing the steps described…in conjunction with a microprocessor or other data processor" and "also includes the computer itself when programmed according to the methods and techniques described." *Id*., 9:15-30; *see also id*., 7:67-9:36, 24:9-25:45, Claims 10, 20, 25; Ex-1002 ¶¶289-293.

4. Claim 4: wherein receiving the request for context information comprises receiving the request for context information from a software application

Parupudi discloses receiving "queries from one or more applications." Ex-1006, 22:55-57; *see also id*., 17:37-18:51, 22:55-23:35, 23:36-24:7, 24:9-25:45, Figure 10. These applications may be "separate from the device" or they may be "executing on the device, e.g. a browser application." *Id*., 17:27-43. Or, for example, these applications may "include a web site application, an Outlook application, and a service discovery application." *Id*., 22:55-23:35; *see also id*., 7:54-65, 7:67-9:36, 24:9-25:45, Claims 10, 20, 25; Ex-1002 ¶¶294-299.

5. Claim 5: wherein receiving the request for context information comprises receiving a request for at least one of: a location of the user, an activity of the user, an aspect of the environment in which the user is located, and biometric data related to the user

Parupudi discloses receiving a request for a location of the user. Parupudi discloses that "[i]ndividual applications...call [a] location service module." Ex-1006, 25:3-5. Moreover, Parupudi discloses with Figure 10 that its privacy manager, after determining the privacy level associated with the application(s), "traverses…one or more hierarchical tree structures" "to find a node with a corresponding privacy level so that it can select the information that is associated with that node." *Id*., 25:16-19. When "the corresponding node is found," "the context information (e.g. location information) associated with the node" is returned to the requesting application, such as by having "the location service module…inform the application that the user's location is the State of Washington." *Id*., 25:22-27, Figure 10, Figure 6 (depicting an identity-based context aware computing system); Ex-1002 ¶¶300-304.

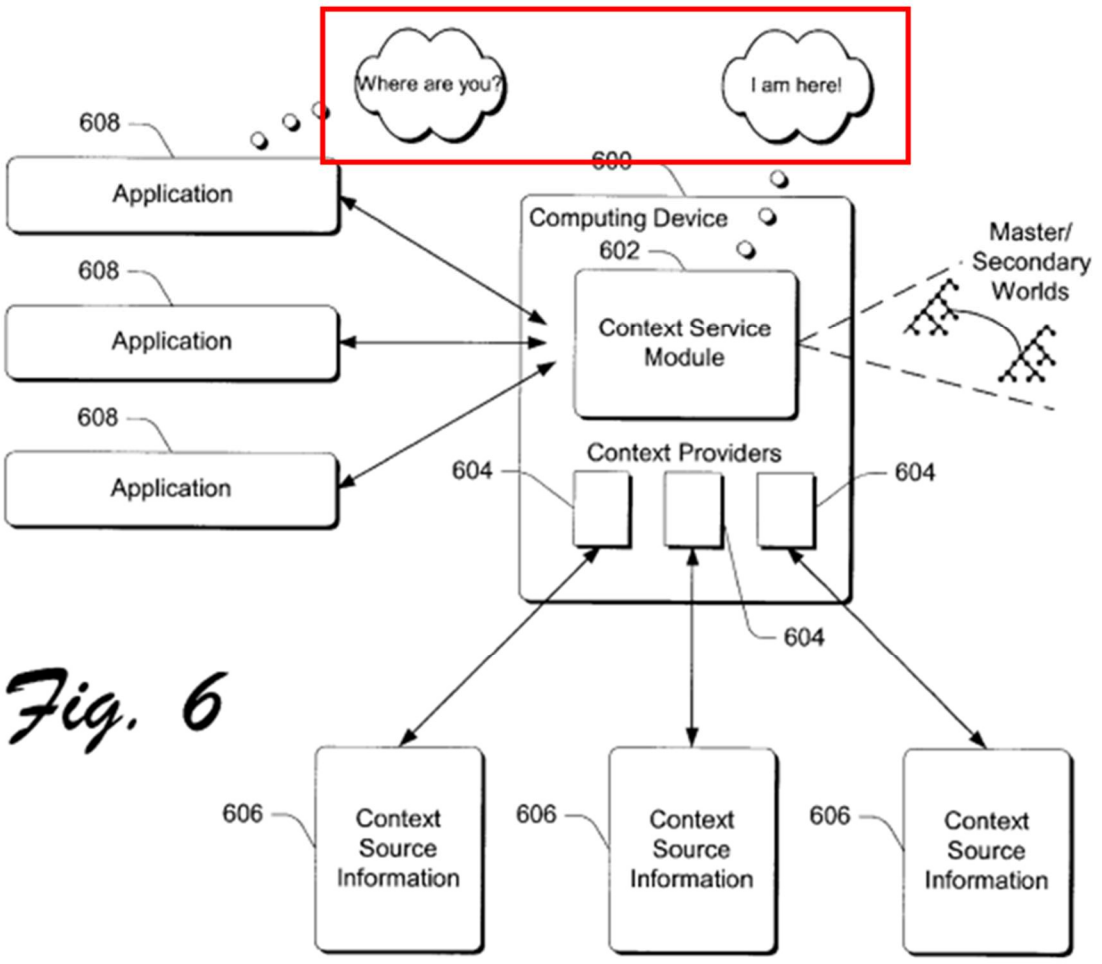

Fig. 6

6. Claim 7: wherein: the context policy data defines a context policy rule based on the identification of the requesting entity

Parupudi discloses that its privacy manager "functions to modulate the information that is provided to the various applications as a function of the applications' identities and security policies on the device." Ex-1006, 3:10-15; *see also id*., 6:59-7:15 ("When a query from an application is received, the privacy manager first determines who the query is from and the privacy level associated with the application or entity."), 25:11-13 (describing that the system "determines the

privacy level associated with the application or applications"), Figure 10; Ex-1002, ¶¶305-309.

7. Claim 8: wherein the context policy data defines a rule based on a predetermined group of requesting entities

Parupudi's below table describes "different privacy levels" and "associated approximate scale[s]" that can be assigned by users to individual applications that call a location service module such as "a privacy level of 0" (i.e., the claimed "predetermined group of requesting entities," which are assigned "a privacy level of 0"), which "means that no location information is returned" and "[a] privacy level of 90" (i.e., the claimed "predetermined group of requesting entities," which are assigned "a privacy level of 90"), which "means that very detailed location information is returned." Ex-1006, 24:56-60.

Privacy Level	Approximate Scale	Level of Revelation
0	—	No location information is returned
10	100,000 Km	Planet/Continent
20	1,000 Km	Country
30	100 Km	State
40	10–100 Km	City & County or Region
50	10 Km	Postal Code & Phone Area Code
60	1 Km	Full Postal Code (Zip + 4) & Area Code and Exchange
70	100 m	Phone Number & Building/Floor
80	10 m	Room #
90	1 m	Exact Coordinates

"For example, a trusted application might have a privacy level of 90, while an untrusted application might have a privacy level of 30." *Id*., 25:6-8; Ex-1002 ¶¶310-314.

8. Claims 13, 22: wherein responding to the request comprises determining context data based on the set of rules of the context policy data

Parupudi discloses that its privacy manager "functions to modulate the information that is provided to the various applications as a function of the applications' identities and security policies on the device." Ex-1006, 3:10-15; *see also id*., 23:36-24:7 ("a security policy or privacy policy can be applied to the information before it is returned to the applications"). As a result, the "privacy manager determines what level of information to provide to applications that might request the information." *Id*., 6:59-7:15 ("[A] scale of privacy levels are defined…to [each] include more or less specific information about the location of [the] device…. A user is able to assign a privacy level to entities that might request location information…. When a query from an application is received, the privacy manager first determines who the query is from and the privacy level associated with the application or entity."); Ex-1002 ¶¶315-319.

9. Claims 14, 23: wherein responding to the request further comprises retrieving the context data from a context database with the context policy enforcement engine based on the set of rules of the context policy data

Parupudi discloses with Figure 10, at Step 1010, that the privacy manager "traverses…one or more hierarchical tree structures [(i.e., the claimed "retrieving the context data from a context database with the context policy enforcement engine)"] to find a node with a corresponding privacy level [(i.e., the claimed "based on the set of rules of the context policy data")] so that it can select the information that is associated with that node." Ex-1006, 25:16-19, Figure 10; *see also id*., Abstract, 24:9-25:45, Claims 1, 10, 25, 34; Ex-1002 ¶¶320-324. This hierarchical tree structure "can be used to determine the…location of a place anywhere in the world and at any definable granularity." Ex-1006, 3:55-4:5, Figures 2-3; *see also id*., 3:55-7:51 (describing the disclosed hierarchical tree structure wherein "each node of the Master World and a Secondary World can have a privacy level associated with it" such that the "privacy manager…evaluates one or more of the Master World and the Secondary World to find a node that has a corresponding privacy level" with "information at that particular granularity"); Ex-1002 ¶¶320-324.

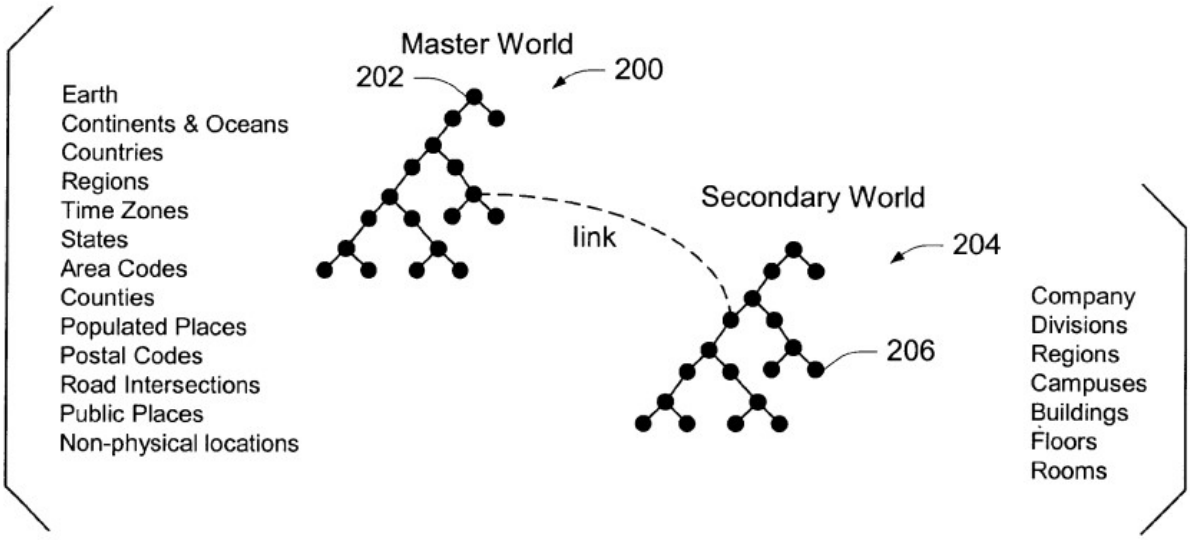
Master World
202
200
Earth
Continents & Oceans
Countries
Regions
Time Zones
States
Area Codes
Counties
Populated Places
Postal Codes
Road Intersections
Public Places
Non-physical locations
link
Secondary World
204
206
Company
Divisions
Regions
Campuses
Buildings
Floors
Rooms

Fig. 2

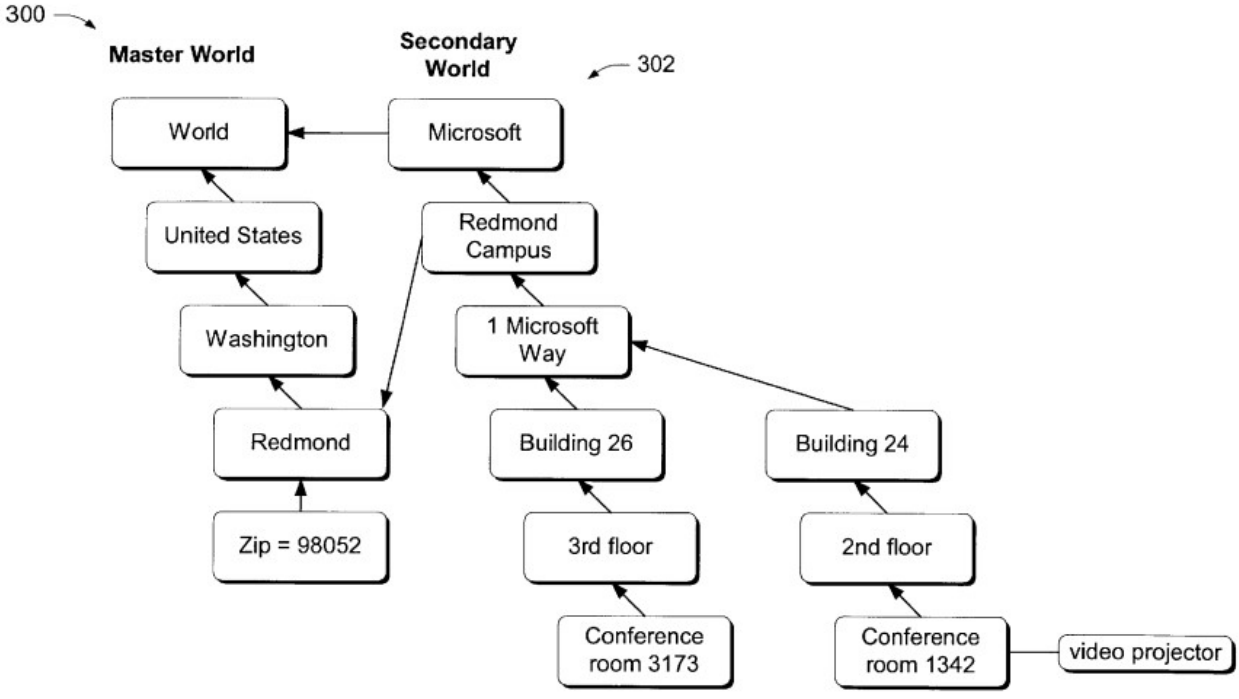
300
Master World
Secondary World
302
World
Microsoft
United States
Redmond Campus
Washington
1 Microsoft Way
Redmond
Building 26
Building 24
Zip = 98052
3rd floor
2nd floor
Conference room 3173
Conference room 1342
video projector

Fig. 3

10. Claim 15: wherein responding to the request further comprises transmitting the context data

Parupudi discloses with Figure 10 that its privacy manager, after determining the privacy level associated with the requestor, "traverses…one or more hierarchical tree structures" "to find a node with a corresponding privacy level so that it can select the information that is associated with that node." Ex-1006, 25:16-19. When "the corresponding node is found," "the context information (e.g. location information) associated with the node" is returned to the requestor, such as by having "the location service module…inform the application that the user's location is the State of Washington." *Id*., 25:22-27, Figure 10, Figure 6 (depicting an identity-based context aware computing system); Ex-1002 ¶¶325-328.

11. Claims 16, 24: wherein determining the context data comprises selecting context data from a plurality of datum defining a context parameter of the user, the plurality of datum having different levels of specificity defined in the set of rules of the context policy data

Parupudi discloses with Figure 10, at Step 1010, that the privacy manager "traverses…one or more hierarchical tree structures to find a node with a corresponding privacy level so that it can select the information that is associated with that node." Ex-1006, 25:16-19, Figure 10; *see also id*., Abstract, 24:9-25:45, Claims 1, 10, 25, 34. This hierarchical tree structure "can be used to determine the…location of a place anywhere in the world and at any definable granularity."

Id., 3:55-4:5, Figures 2-3; *see also id*., 3:55-7:51 (describing the disclosed hierarchical tree structure wherein "each node of the Master World and a Secondary World can have a privacy level associated with it" such that the "privacy manager…evaluates one or more of the Master World and the Secondary World to find a node that has a corresponding privacy level" with "information at that particular granularity"); Ex-1002 ¶¶329-333.

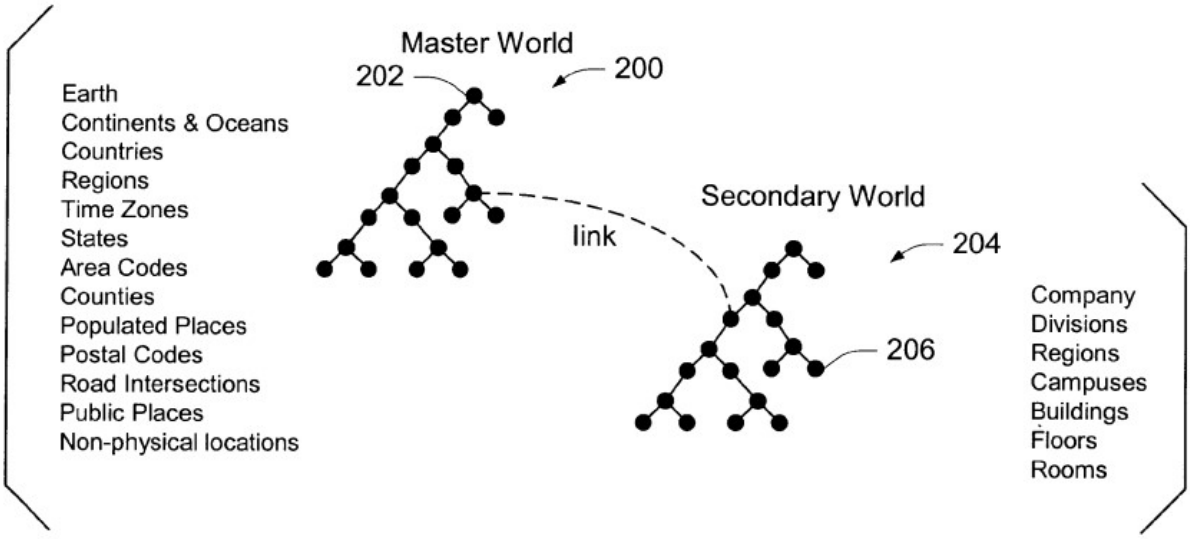

Fig. 2

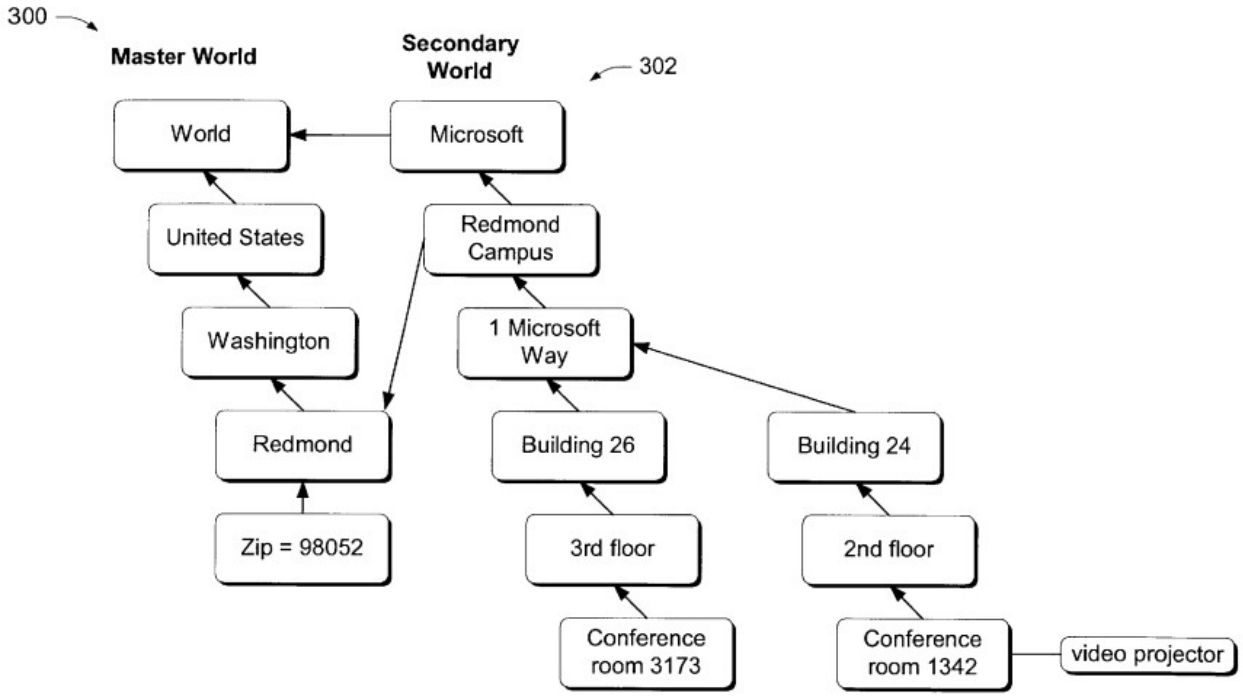

Fig. 3

12. Claim 18: further comprising: receiving user-supplied context policy rule with the mobile computing device, and updating the context policy data with the user-supplied context policy rule with the context policy enforcement engine

Parupudi's privacy manager allows a user to "assign a privacy level to entities that might request location information" such that "[w]hen a query from an application is received, the privacy manager first determines who the query is from and the privacy level associated with the application." Ex-1006, 7:1-15. Parupudi discloses with Figure 10, at Steps 1000 and 1002, that users may assign "various privacy levels" "to the individual nodes in one or more hierarchical tree structures."

Id., 24:31-34, 24:61-62. For example, a user might assign "a web site that gives up to the minute weather of various locations" "a privacy level of 60" in order to "receive weather information [that] corresponds to [his] postal code" and "a corporation intranet web site that is a trusted web site" "a privacy level of 90" in order to "give them precise location information as to [his] whereabouts." *Id*.; *see also id*., Claims 1, 10, 14, 20, 25; Ex-1002 ¶¶334-337.

13. Claim 20: further comprising: receiving context data related to the user from a source remote to the mobile communication device; and updating a context database stored on the mobile computing device with the user-supplied context data

Parupudi discloses a "context provider" to "receive information from sources…and convey the information to the context service module…so that the context service module can use the information to determine a current device context." Ex-1006, 17:3-11. The "sources of the information" may include, for example, "various information transmitters such as a GPS," though "a source of information…might [also] include a person who, for example, physically enters location information into the device 600 so that the device can process the information to determine its location." *Id*., 17:12-26; *see also id*., 17:27-44 ("When the device 600 receives the location information from the sources 606, it processes the information with the location providers 604 and provides the information to the location service module 602."); Ex-1002 ¶¶338-342.

XIII. THERE IS NO BASIS FOR ANY DISCRETIONARY DENIAL

The Board should decline to exercise its discretion to deny institution under 35 U.S.C. §314(a). While Director Vidal's June 21, 2022 Guidance made clear that "*Fintiv* is limited to facts of that case," for completeness, Petitioner addresses the factors set forth in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential). The six factors set out in *Fintiv* do not justify denying institution.

The **first *Fintiv* factor** is neutral because Samsung has not yet moved to stay the district court proceedings pending IPR, and the PTAB will not infer how the district court would rule should a stay be requested. *See, e.g., Hulu LLC v. SITO Mobile R&D IP, LLC et al.*, IPR2021-00298, Paper 11 at 10-11 (PTAB May 19, 2021).

For the **second *Fintiv* factor**, the district court has set a trial date for May 20, 2024. This timing does not tip in favor of denying the petition in this case. *See, e.g.*, *Apple Inc. v. Koss Corp.*, IPR2021-00305, Paper 14 at 13 (PTAB June 3, 2021). This Petition is filed in March 2023. An institution decision should be issued within six months of docketing, around September 2023. And a final written decision ("FWD") should be issued in September 2024. Thus, the trial date is likely around three months before the FWD. Recent PTAB cases analyzing similar schedules have weighed the second factor as neutral or, at most, slightly in favor of denial. *See, e.g.,*

Google LLC et al. v. Parus Holdings, Inc., IPR2020-00847, Paper 9 at 12 (PTAB Oct. 21, 2020) (trial scheduled for three months before FWD weighs "at best, neutral"); *Apple Inc. v. Koss Corp.*, IPR2021-00305, Paper 14 at 13-14 (PTAB June 3, 2021) (trial scheduled for two months before FWD weighs "at most, minimally in favor" of denial).

"The PTAB will also consider additional supporting factors such as the number of cases before the judge in the parallel litigation." Director Vidal's June 2022 Guidance. Here, the court has scheduled three other trials (2:22-cv-00312-JRG-RSP *Fleet Connect Sols. LLC v. Southern Tire Mart, LLC*; 2:22-cv-00322-JRG-RSP *Lionra Technologies Ltd. v. Fortinet, Inc.*; and 2:22-cv-00361-JRG-RSP *S3G Tech. LLC v. Nordstrom Inc.*) in the same week as the trial for this case.

If the median time to trial for civil actions in the Eastern District of Texas ("EDTX") is used to estimate the trial date (i.e., to account for potential delays, etc.), as advised by Director Vidal's June 2022 Guidance, trial should not be expected to occur until October 2024, *after* a FWD will issue. Ex-1021, at 35 (indicating a most-recent median time-to-trial for civil actions in EDTX of 24.5 months).

The **third *Fintiv* factor** weighs strongly against denial. No hearing has been set and no substantive activity has occurred in the case. Because the investment in the district court proceeding has been minimal and Petitioner acted diligently, this factor weighs strongly against discretionary denial. *See, e.g., Hulu*, Paper 11 at 13.

The **fourth *Fintiv* factor** also weighs against denial. As explained above, the median time-to-trial for civil actions in EDTX suggests that trial will not occur until after a FWD is issued. Thus, "there is a reasonable likelihood that the Board will address the overlapping validity issues prior to the district court reaching them at trial…, thereby providing the possibility of simplifying issues for trial." *Juniper Networks, Inc. v. Packet Intelligence LLC*, IPR2020-0039, Paper 21 at 18 (PTAB Sept. 10, 2020); *see also MED-EL Elektromedizinische Geraete GmbH v. Sonova AG*, IPR2020-00176, Paper 13 at 15 (PTAB June 3, 2020) ("As to the fourth factor, the parties do not dispute that overlap exists between the invalidity issues in this case and in the district court. This overlap may inure to the district court's benefit, however, by simplifying issues for trial should we reach our determination on the challenges raised in the Petition before trial.").

Moreover, Petitioner is challenging more claims than asserted in the district court litigation. PO's infringement contentions assert only Claims 1, 5, 21, and 25. This Petition challenges Claims 1, 3-5, 7-16, and 18-25. This IPR proceeding is thus the only venue in which the invalidity challenges against several claims in the '629 Patent will be adjudicated. Moreover, reviewing the challenged claims in this proceeding promotes efficiency in that many more claims will be addressed here, which will resolve disputes against future district court defendants. *See Fintiv*, Paper 11 at 4 ("the Board's cases addressing earlier trial dates as a basis for denial under

NHK have sought to balance considerations such as system efficiency, fairness, and patent quality."). Accordingly, challenging additional claims further weighs against denial. *See, e.g.*, *Vudu, Inc. v. Ideahub, Inc.*, IPR2020-01688, Paper 16 at 14-15 (PTAB April 19, 2021) ("differences in asserted claims" and claims challenged in the petition weighs against denial).

On the **fifth *Fintiv* factor**, the Board should give little weight to the fact that Petitioner and PO are the same parties as in district court. *See Weatherford U.S., L.P., v. Enventure Global Tech., Inc.*, Paper 16 at 11-13 (PTAB Apr. 14, 2021). Although Samsung is both Petitioner and litigation defendant, this factor does not outweigh the other factors that strongly weigh against discretionary denial.

"Other circumstances" under the **sixth *Fintiv* factor** further weigh against discretionary denial. The merits of the Petition are especially strong. *See Align Tech., Inc. v. 3Shape A/S,* IPR2020-01087, Paper 15 at 42-43 (PTAB Jan. 20, 2021). *See supra* Section XII.

Taken together holistically, the *Fintiv* factors strongly weigh against denial.

XIV. CONCLUSION

For the reasons given above, Petitioner requests institution of IPR for Claims 1, 3-5, 7-16, and 18-25 of the ’629 Patent based on each of the grounds specified in this Petition.

Respectfully Submitted,

/s/ *John Kappos*
John Kappos (Reg. No. 37,861)

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), Petitioner certifies that this petition includes 13,908 words, as measured by Microsoft Word, exclusive of the table of contents, mandatory notices under § 42.8, certificates of service, word count, and exhibits.

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e)(1))

The undersigned hereby certifies that the above document was served on March 20, 2023, by filing this document through the Patent Trial and Appeal Board P-TACTS System, as well as delivering a copy via express mail upon the following attorneys of record for the Patent Owner and Petitioner:

Barnes & Thornburg LLP
11 S. Meridian Street
Indianapolis, IN 46204

A courtesy copy was sent to the below counsel via electronic mail:

Garland T. Stephens
Blue Peak Law Group
2007 South Boulevard
Houston, TX 77098
Phone: (832) 387-7696
Email: garland@bluepeak.law

Anna Dwyer
Blue Peak Law Group
345 East 94th Street, Ste Apt 28g
New York, NY 10128
Phone: (772) 631-6460
Email: anna@bluepeak.law

Jeff Risher
Blue Peak Law Group
15226 Bluff View Ave.
Friant, CA 93626
Phone: (949) 690-1462
Email: jeff@bluepeak.law

Justin Lile Constant
Blue Peak Law Group

3139 W Holcombe Blvd., PMB 8160
Houston, TX 77025
Phone: (281) 972-3036
Email: justin@bluepeak.law

Kate S. Falkenstien
Robert Stephen Magee
Blue Peak Law Group
3790 El Camino Real, Ste PMB 846
Palo Alto, CA 94306
Phone: (281) 972-3036
Email: kate@bluepeak.law
Email: robert@bluepeak.law

Richard M. Koehl
Blue Peak Law Group
PO Box 20204
New York, NY 10001-0006
Phone: (917) 856-3872
Email: richard@bluepeak.law

Andrea Leigh Fair
Claire Abernathy Henry
Charles Everingham , IV
Ward, Smith & Hill, PLLC
1507 Bill Owens Parkway
Longview, TX 75604
Phone: (903) 757-2323
Email: andrea@wsfirm.com
Email: claire@wsfirm.com
Email: ce@wsfirm.com

Michael T. Renaud
Mintz Levin Cohn Ferris Glovsky & Popeo PC
One Financial Center, Suite 100
Boston, MA 02111
Phone: (617) 542-6000
Fax: (617) 542-2241
Email: mtrenaud@mintz.com

Dated: March 20, 2023

Respectfully submitted,

/s/ John Kappos

John Kappos (Reg. No. 37,861)
O'Melveny & Myers LLP
2501 North Harwood Street, Suite 1700
Dallas, TX 75201
Telephone: (972) 360-1900
Fax: (972) 360-1901
E-Mail: jkappos@omm.com
Attorney for Petitioner