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.

DECLARATION OF DR. BENJAMIN B. BEDERSON IN SUPPORT OF 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

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	INTENTIONALLY LEFT BLANK
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).

1. I, Benjamin B. Bederson, declare as follows:

I. INTRODUCTION

2. I have been retained by Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Samsung" or "Petitioner") as an independent expert consultant in this *inter partes* review ("IPR") proceeding before the United States Patent and Trademark Office ("PTO").

3. I have been asked by Samsung Counsel ("Counsel") to consider whether certain references teach or suggest the features recited in Claims 1, 3-5, 7-16, and 18-25 of U.S. Patent No. 8,359,629 ("the '629 Patent") (Ex-1001). My opinions and the bases for my opinions are set forth below.

4. I am being compensated at my ordinary and customary consulting rate for my work, which is $600 per hour. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other financial interest in this proceeding.

II. BACKGROUND AND QUALIFICATIONS

5. All of my opinions stated in this declaration are based on my own personal knowledge and professional judgment. In forming my opinions, I have relied on my knowledge and experience in designing, developing, researching, and teaching the technology referenced in this declaration.

6. I am over 18 years of age and, if I am called upon to do so, I would be competent to testify as to the matters set forth herein. I understand that a copy of my current curriculum vitae, which details my education and professional and academic experience, is being submitted as Ex-1003. The following provides a brief overview of some of my experience that is relevant to the matters set forth in this declaration.

7. I am currently Professor Emeritus of Computer Science at the University of Maryland ("UMD"). From 2014 to 2018, I was the Associate Provost of Learning Initiatives and Executive Director of the Teaching and Learning Transformation Center at the UMD. I am a member and previous director of the Human-Computer Interaction Lab ("HCIL"), the oldest and one of the best known Human-Computer Interaction ("HCI") research groups in the country. I was also co-founder and Chief Scientist of Zumobi, Inc. from 2006 to 2014, a Seattle-based startup that is a publisher of content applications and advertising platforms for smartphones. I am also co-founder and co-director of the International Children's Digital Library ("ICDL"), a web site launched in 2002 that provides the world's largest collection of freely available online children's books from around the world with an interface aimed to make it easy for children and adults to search and read children's books online. I am also co-founder and prior Chief Technology Officer of Hazel Analytics, a data analytics company to improve food safety and better

public health whose product sends alerts in warranted circumstances. In addition, I have for more than 25 years consulted for numerous companies in the area of user interfaces, including EPAM, Hillcrest Labs, Lockheed Martin, Logitech, Microsoft, NASA Goddard Space Flight Center, the Palo Alto Research Center, and Sony.

8. The devices and methods claimed in the '629 Patent generally relate to human-computer interaction with mobile electronic devices. For more than 30 years, I have studied, designed, and worked in the field of computer science and HCI. My experience includes 30 years of teaching and research, with research interests in HCI and the software and technology underlying today's interactive computing systems.

9. At UMD, I am focused primarily on the area of HCI, a field that relates to the development and understanding of computing systems to serve users' needs. Researchers and practitioners in this field are focused on making universally usable, useful, efficient, and appealing systems to support people in their wide range of activities. My approach is to balance the development of innovative technology that serves people's practical needs. Example systems following this approach that I have built include Cortex-I (1992 embedded computer vision system that sensed licensed plates with custom motor, camera and controller), Audio Augmented Reality (1995 embedded system for sensing a user's location and playing audio suited to that location), Fisheye Menus (2000 software for sensing movement within

and selection of linear list of items in a menu), PhotoMesa (2001 software for end users to browse personal photos), DateLens (2002 software for end users to use their mobile devices to efficiently access their calendar information), SlideBar (2005 linear sensor to control scrolling), LaunchTile (2005 "home screen" software for mobile devices to allow users to navigate apps in a zoomable environment), SpaceTree (2001 software for end users to efficiently browse very large hierarchies), ICDL (as described above), and StoryKit (a 2009 iPhone app for children to create stories).

10. LaunchTile led to my co-founding of Zumobi Inc. in 2006, where I was responsible for investigating new software platforms and developing new user interface designs that provided efficient and engaging interfaces to permit end users to access a wide range of content on mobile platforms (including the iPhone and Android-based devices). For example, I designed and implemented software called "Ziibii," a "river" of news for iPhone that used a capacitive sensor for controlling linear movement through news, software called "ZoomCanvas," a zoomable user interface for several iPhone apps, and iPhone apps including "Inside Xbox" for Microsoft and Snow Report for REI. I also worked on proximity-based user interfaces as described in U.S. Patent No. 8,261,211 where I am named inventor.

11. In 1995, I built an "audio augmented reality" system for use in an art museum that identified and announced which piece of art a person was standing in

front of. Ex-1022, 210-211. This worked by installing infrared (IR) transmitters in the ceiling above each piece of art which was identified by an infrared (IR) receiver controlled by a microcontroller. As depicted in Figure 1 below, a person wearing the receiver walked around, the microcontroller they were carrying would identify the code from the transmitter they were standing under.

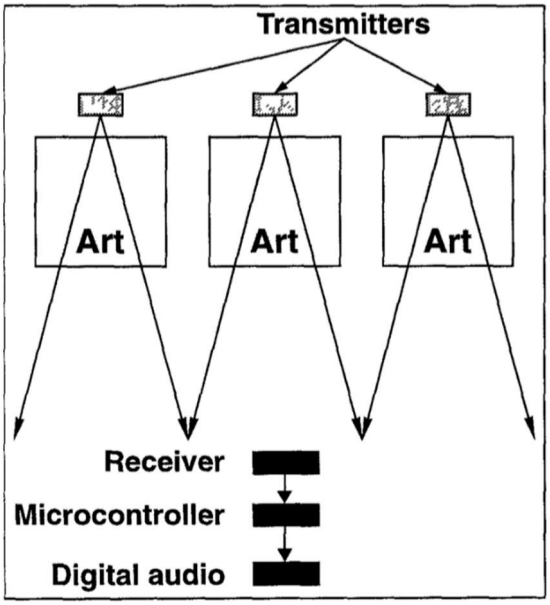

Figure 1: Schematic of automated tour guide prototype.

12. Another example of my work involved the tracking of a person's transportation routes and using that tracking to improving the human experience of in-car navigation systems. Ex-1023, 33-42. In particular, by analyzing the data associated with many routes over time, we provided improved ways of helping people track, share, and use their driving route history. As shown in Figure 4 below, the interface allowed a user to track, filter, and compare different driving routes.

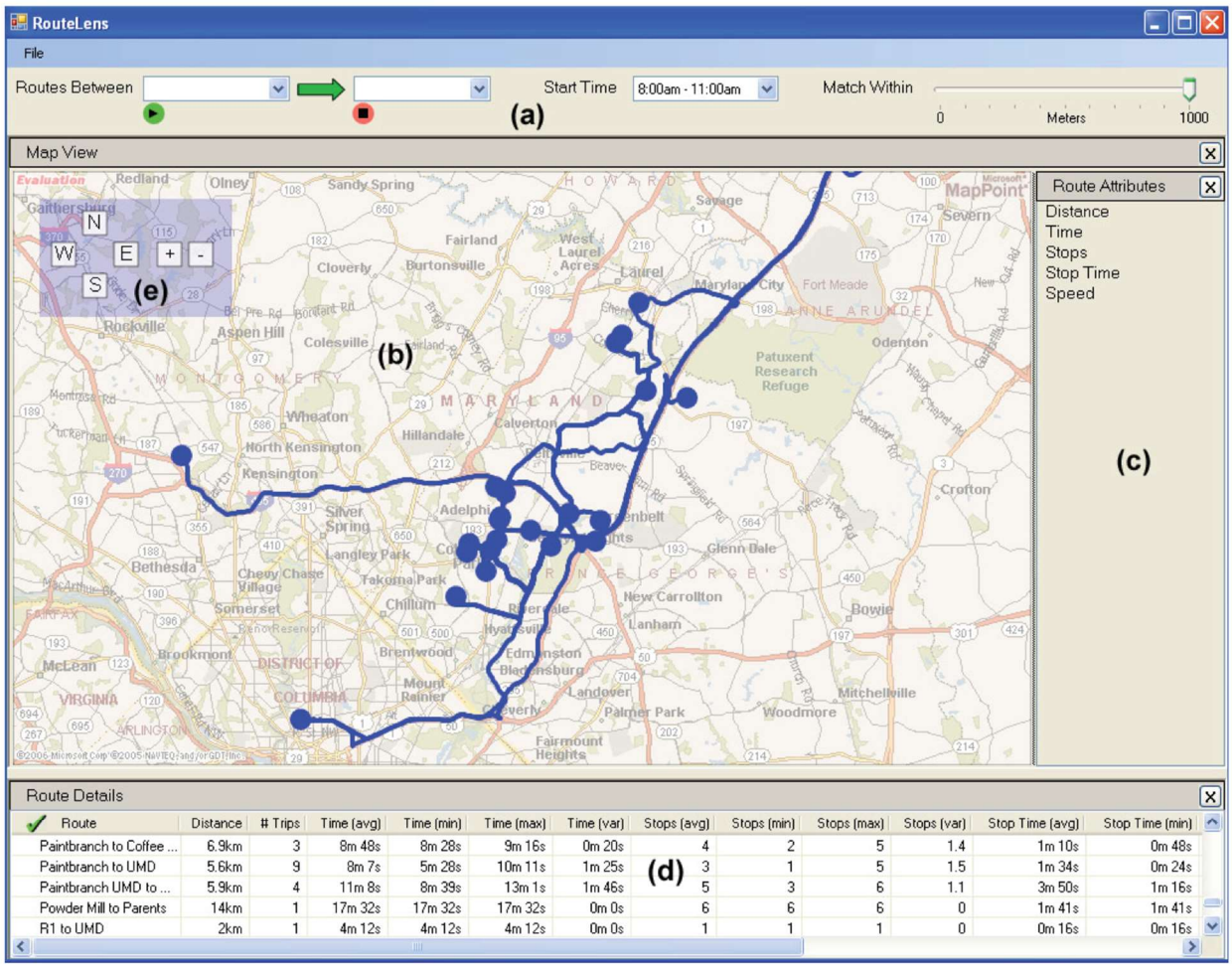

FIGURE 4 Desktop interface consists of components to (*a*) select routes, (*b*) browse data, (*c*) compare routes, (*d*) view detailed statistics, and (*e*) zoom and pan.

13. Starting in the mid-1990s and going through the 2000s, I worked on a range of "zoomable user interfaces" (ZUIs) that supported users in navigating large information spaces by zooming in and out of the information on the screen. These included both 2D and 3D environments. As an example of the 3D environments I developed, I gave a talk in 1993 to the University of Chicago Computer Science Department describing "PA3D: A Multiscale Hierarchical Sketchpad." I built several different ZUI systems over the years, including Pad++, Jazz and Piccolo. In

those systems, I used a range of solutions to allow users to control zooming through the information space. The most common approach for systems with 3 button mice was to use the middle button for zooming in and the right button for zooming out. The user would hold the button down, and the system would smoothly animate zooming in or out – so that the user controlled how much the system zoomed based on the duration that the button was pressed. *See* Ex-1024. I also used a commercial off the shelf touch screen for input to a zoomable image browser we built using Pad++, in or about 1998. The touch screen generated standard mouse signals, and I did not have to modify the zoomable image browser or Pad++ at all in order for it to operate with the touch screen. One project I worked on determined the trajectory of a pointer (such as a finger) as it approached a touch screen and modified the user interface on the touch screen in response to that approach. *See* Ex-1025.

14. At the ICDL, I have since 2002 been the technical director responsible for the design and implementation of the web site, www.childrenslibrary.org (originally at www.icdlbooks.org). In particular, I have been closely involved in designing the user interface as well as the software architecture for the web site since its inception in 2002.

15. Beginning in the mid-1990s, I have been responsible for the design and implementation of numerous other web sites in addition to the ICDL. For example, I designed and built my own professional web site when I was an Assistant Professor

of Computer Science at the University of New Mexico in 1995 and have continued to design, write the code for, and update both that site (which I moved to the UMD in 1998, currently at http://www.cs.umd.edu/~bederson/) as well as numerous project web sites, such as Pad++, http://www.cs.umd.edu/hcil/pad++/. I received the Janet Fabri Memorial Award for Outstanding Doctoral Dissertation for my Ph.D. work in robotics and computer vision. I have combined my hardware and software skills throughout my career in HCI research, building various interactive electrical and mechanical systems that couple with software to provide an innovative user experience.

16. My work has been published extensively in more than 160 technical publications, and I have given about 100 invited talks, including 9 keynote lectures. I have won a number of awards including the Brian Shackel Award for "outstanding contribution with international impact in the field of HCI" in 2007, and the Social Impact Award in 2010 from the Association for Computing Machinery's ("ACM") Special Interest Group on Computer Human Interaction ("SIGCHI"). ACM is the primary international professional community of computer scientists, and SIGCHI is the primary international professional HCI community. I have been honored by both professional organizations. I am an "ACM Distinguished Scientist," which "recognizes those ACM members with at least 15 years of professional experience and 5 years of continuous Professional Membership who have achieved significant

accomplishments or have made a significant impact on the computing field." I am a member of the "CHI Academy," which is described as follows: "The CHI Academy is an honorary group of individuals who have made substantial contributions to the field of HCI. These are the principal leaders of the field, whose efforts have shaped the disciplines and/or industry, and led the research and/or innovation in human-computer interaction." The criteria for election to the CHI Academy are: (1) cumulative contributions to the field; (2) impact on the field through development of new research directions and/or innovations; and (3) influence on the work of others. I have received two "Test of Time" awards from IEEE InfoVis for my 2001 and 2002 work on visualizing hierarchies, including those containing digital photos.[2]

17. I have appeared on radio shows numerous times to discuss issues relating to user interface design and people's use and frustration with common technologies, web sites, and mobile devices. My work has been discussed and I have been quoted by mainstream media around the world over 120 times, including by the New York Times, the Wall Street Journal, the Washington Post, Newsweek, the Seattle Post Intelligencer, the Independent, Le Monde, NPR's All Things Considered, New Scientist Magazine, and MIT's Technology Review.

[2] https://ieeevis.org/year/2021/info/awards/test-of-time-awards; https://ieeevis.org/year/2022/info/awards/test-of-time-awards

18. I have designed, programmed, and publicly deployed dozens of user-facing software products that have cumulatively had millions of users. My work is cited by several major companies, including Amazon, Apple, Facebook, Google, and Microsoft. I am a named inventor on 14 U.S. patents and 20 U.S. patent applications. The patents are generally directed to user interfaces and experience.

19. I received a B.S. degree in Computer Science with a minor in Electrical Engineering in 1986 from the Rensselaer Polytechnic Institute. I received M.S. and Ph.D. degrees in Computer Science in 1989 and 1992, both from New York University.

III. INFORMATION CONSIDERED

20. In preparation for this declaration, I have considered the materials discussed in this declaration, including, for example, the '629 Patent, the references cited by the '629 Patent, the prosecution history of the '629 Patent, various background articles and books referenced in this declaration, and the prior art references identified in this declaration. In addition, my opinions are further based on my education, training, experience, and knowledge in the relevant field.

IV. RELEVANT LEGAL STANDARDS

21. I am not an attorney and offer no legal opinions. For the purposes of this Declaration, I have been informed about certain aspects of the law that are relevant to my analysis, as summarized below.

A. Claim Interpretation

22. I have been informed and understand that claim construction is a matter of law and that the final claim constructions for this proceeding will be determined by the Patent Trial and Appeal Board.

23. To resolve the particular grounds presented in the Petition, I do not believe any term requires explicit construction. I ascribe the plain meaning to each claim term, as that plain meaning would have been understood by a POSITA in light of the specification.

B. Perspective of One of Ordinary Skill in the Art

24. I have been informed and understand that a patent is to be understood from the perspective of a hypothetical "person of ordinary skill in the art" ("POSITA"). Such an individual is considered to possess normal skills and knowledge in a particular technical field (as opposed to being a genius). I understand that in considering what the claims of a patent require, what was known prior to that patent, what a prior art reference discloses, and whether an invention is obvious or not, one must use the perspective of such a person of ordinary skill in the art.

C. Obviousness

25. I have been in informed and understand that a patent claim is obvious under 35 U.S.C. § 103, and therefore invalid, if the claimed subject matter, as a whole, would have been obvious to a person of ordinary skill in the art as of the

priority date of the patent based on one or more prior art references and/or the knowledge of one of ordinary skill in the art.

26. I understand that an obviousness analysis must consider (1) the scope and content of the prior art, (2) the differences between the claims and the prior art, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations, if any, of non-obviousness (such as unexpected results, commercial success, long-felt but unmet need, failure of others, copying by others, and skepticism of experts).

27. I understand that a single prior art reference can render a patent claim obvious under 35 U.S.C. § 103 if any differences between that reference and the claims would have been obvious to a person of ordinary skill in the art. Alternatively, I understand that a prior art reference may be combined with other references to disclose each element of the invention under 35 U.S.C. § 103. Thus the teachings of two or more references may be combined in the same way as disclosed in the claims, if such a combination would have been obvious to one having ordinary skill in the art. I understand that I understand that a reference may also be combined with the knowledge of a person of ordinary skill in the art, and that this knowledge may be used to combine multiple references. I further understand that a person of ordinary skill in the art is presumed to know the relevant prior art. I understand that the obviousness analysis may take into account the inferences and creative steps that a person of ordinary skill in the art would employ.

28. In determining whether a prior art reference would have been combined with other prior art or other information known to a person of ordinary skill in the art, I understand that the following principles may be considered:

a. whether the references to be combined involve non-analogous art;

b. whether the references to be combined are in different fields of endeavor than the alleged invention in the Patent;

c. whether the references to be combined are reasonably pertinent to the problems to which the inventions of the Patent are directed;

d. whether the combination is of familiar elements according to known methods that yields predictable results;

e. whether a combination involves the substitution of one known element for another that yields predictable results;

f. whether the combination involves the use of a known technique to improve similar items or methods in the same way that yields predictable results;

g. whether the combination involves the application of a known technique to a prior art reference that is ready for improvement, to yield predictable results;

h. whether the combination is "obvious to try";

i. whether the combination involves the known work in one field of

endeavor prompting variations of it for use in either the same field or a different one based on design incentives or other market forces, where the variations are predictable to a person of ordinary skill in the art;

j. whether there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention;

k. whether the combination requires modifications that render the prior art unsatisfactory for its intended use;

l. whether the combination requires modifications that change the principle of operation of the reference;

m. whether the combination is reasonably expected to be a success; and

n. whether the combination possesses the requisite degree of predictability at the time the invention was made.

29. I understand that in determining whether a combination of prior art references renders a claim obvious, it is helpful to consider whether there is some teaching, suggestion, or motivation to combine the references and a reasonable expectation of success in doing so. I understand, however, that a teaching, suggestion, or motivation to combine is not required.

V. LEVEL OF ORDINARY SKILL IN THE ART

30. I am familiar with the level of ordinary skill in the art with respect to the '629 Patent around its filing date. Based on my experience working, teaching, and conducting research in the relevant field, and based on my review of the '629 Patent specification, claims, file history, and prior art, I believe one of ordinary skill in the art around the time of the alleged invention of the '629 Patent 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.

31. In determining the level of ordinary skill in the art, I considered, for example, the type of problems encountered in the art, prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field.

32. I met the definition of a POSITA in 2009. I also had greater knowledge and experience than a POSITA. I worked with POSITAs in 2009, and I am able to render opinions from the perspective of a POSITA based on my knowledge and experience. My opinions concerning the '629 Patent claims and the prior art are from the perspective of a person of ordinary skill in the art, as set forth above.

VI. SUMMARY OF MY OPINIONS

33. I have been asked to consider whether the claims of the '629 Patent are obvious over certain prior art references. As explained below in detail in this declaration, it is my opinion that:

1: Claims 1, 3-5, 7, 9-16, 18-19, and 21-25 are obvious over Paretti (Ex-1005) in view of the knowledge of one of ordinary skill in the art;

2: Claims 1, 3-5, 7-8, 13-16, 18, and 20-25 are obvious over the combination of Parupudi (Ex-1006) and Nykanen (Ex-1007) in view of the knowledge of one of ordinary skill in the art.

VII. TECHNOLOGICAL BACKGROUND

34. As of the priority date, "[n]umerous systems and methods exist[ed] for automatically tracking the location of users." Ex-1005, ¶4; *see also* Ex-1006, 1:11-2:17. "Such tracking [was often] performed to support context-aware applications, to provide location-based services, or for a variety of other reasons." Ex-1005, ¶4; *see also* Ex-1006, 1:11-2:17. "Tracking of users [wa]s often performed by tracking the location of a device or object uniquely associated with the user;" "[f]or example, numerous mobile devices carried by users…include[d] technology that enables the location of such devices to be determined with varying degrees of accuracy." Ex-1005, ¶4; *see also* Ex-1006, 1:11-2:17. "Such technology…include[d] but is not

limited to Global Positioning System (GPS) technology, Wi-Fi technology, cellular telephony technology and Bluetooth™ technology." Ex-1005, ¶4.

35. "Information obtained from such devices may include actual location information, such as when the device has built-in GPS capability, or relative location information, such as proximity to other mobile devices, beacons, or other identifiable objects or locations." Ex-1005, ¶5; *see also* Ex-1006, 1:11-2:17. For example, prior art systems taught "establishing a proximity-based ad hoc network among a plurality of mobile devices by leveraging actual and relative location information obtained from such devices" such that the "proximity-based ad hoc network may then be used to track the locations of users associated with the devices." Ex-1005, ¶5. "[N]umerous other location tracking systems [also] exist[ed] in the art." Ex-1005, ¶5; *see also* Ex-1006, 1:11-2:17.

36. Indeed, "a number of methods of determining the location of a mobile terminal in a wireless network environment" "exist[ed] in the art." Ex-1007, 1:10-32. "Some of these methods [we]re terminal-based, while others [we]re network-based." Ex-1007, 1:10-32. "As an example of a terminal-based method, a terminal could contain Global Positioning System (GPS) hardware which allowed] it to determine its location using the established system of satellites equipped with radio transmitters and atomic clocks." Ex-1007, 1:10-32. "The terminal could then serve the determined location information to requesting parties, terminals, applications,

web services, and the like." Ex-1007, 1:10-32. "As an example of a network based method, time of arrival (TOA) measurements could be computed from access bursts generated by a mobile and used to determine the position of a terminal." Ex-1007, 1:10-32. Indeed, the "use of TOA, enhanced observed time difference (E-TOD), and the like to determine terminal location [wa]s noted in the Third Generation Partnership Project (3GPP)'s Location Services (LCS) specification documents TS 23.071 and TS 23.271." Ex-1007, 1:10-32. "As still another example, a terminal could contain Bluetooth hardware which allow[ed] it to determine its location by communicating with Bluetooth beacons in the vicinity of the terminal." Ex-1007, 1:10-32.

37. Further, the "location of a user may [have been] determined in many other ways beyond tracking the location of a device or object associated with a user." Ex-1005, ¶6; *see also* Ex-1006, 1:11-2:17. "For example, recorded information concerning a commercial transaction carried out by a user may place the user at a particular commercial establishment at a particular time." Ex-1005, ¶6. "As another example, when a user performs an activity on a networked computer having an IP address, location information associated with the IP address may be used to locate the user." Ex-1005, ¶6. Or, for example, a "user may also actively enter data (e.g., a zip code) into a networked computer or other device from which the location of the user may be inferred." Ex-1005, ¶6. Indeed, "numerous other methods for

tracking the location of a user are known." Ex-1005, ¶6; *see also* Ex-1006, 1:11-2:17.

38. As "many methods exist[ed] for tracking the location of a user," "user[s] [were] rightfully concerned about how information about his/her location is being tracked, the nature of such information, and to whom such information is being reported." Ex-1005, ¶7. "Unanticipated or unauthorized location tracking and reporting may [have] give[n] rise to fundamental concerns about user privacy and security." Ex-1005, ¶7. "Users may not [have] want[ed] certain entities or persons to know where they currently are, where they have been in the past, or where they are likely to be in the future for any number of reasons." Ex-1005, ¶7.

39. Indeed, as of the priority date, "security and privacy" was an "issue relevant to applications and web services which make use of location data." Ex-1007, 2:35-47. Despite the "great benefits to applications and/or web services that make use of location data" (e.g., "having location data allows a web service to provide interactive step-by-step driving directions to a user"), "the potential for abuse of location data by applications and web services exist[ed]." Ex-1007, 2:35-47. "Therefore, many users long[ed] for control over where location information concerning their terminals is transmitted" and to "be able to make sure [that] all sources of location information comply with his wishes concerning privacy." Ex-1007, 2:35-47.

40. "Users…concerned about location tracking may choose to divest themselves of technology that is capable of being used to track their location," but, "by so doing, such users…lose the benefits of that technology, including the benefits of applications and services premised on location tracking." Ex-1005, ¶8. "Additionally, by divesting themselves of such technology, such users may deprive systems that leverage location information obtained from a plurality of users…of valuable information." Ex-1005, ¶8.

41. Therefore, at the time of the alleged invention, a system for enabling a user to control the manner in which location information associated with the user is obtained, disseminated and/or reported by a location tracking system would have been considered highly desirable. *See* Ex-1005, ¶9. Indeed, "there exist[ed] a need for a system and method whereby a user could specify his privacy preferences to one database and be assured that his preferences would be adhered to by all location providing sources, thereby allowing the user to exact direct control over which applications and web services have access to data concerning the location of his mobile." *See* Ex-1007, 2:48-54.

42. As of the priority date, the use of databases, including in mobile computing devices, and including to solve such problems, was well-known. *See, e.g.*, Ex-1006, 1:10-2:17; Ex-1007, 1:10-2:54; Ex-1026, 17. For example, databases were well-known to provide many advantages for accessing such structured data,

such as compactness, speed, currency, protection, and less drudgery. *See, e.g.*, Ex-1026, 17.

VIII. THE '629 PATENT

A. Overview of the '629 Patent

43. 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; *see also id.*, 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).

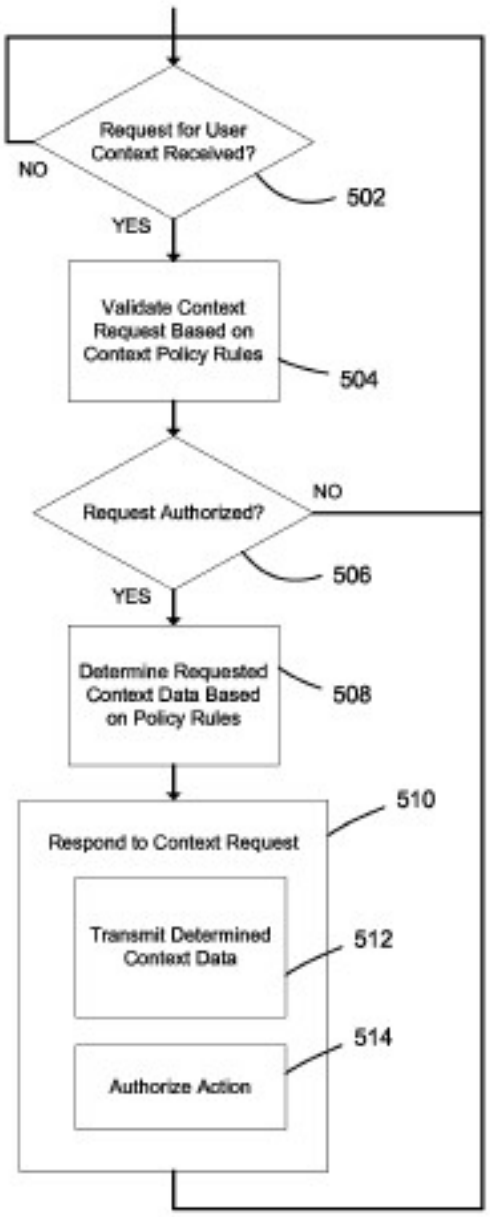

FIG. 5

B. Challenged Claims

44. The claims at issue are Claims 1, 3-5, 7-16, and 18-25 of the '629 Patent.

C. Prosecution History of the '629 Patent

45. The '629 Patent, filed as Application No. 12/567,386 on September 25, 2009, was allowed after two office actions.

46. 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, the 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.

47. 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, the 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.

48. 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.

49. As discussed below, 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.

D. Priority Date

50. I understand that for the purposes of this proceeding, Petitioner assumes that the '629 Patent is entitled to its earliest alleged priority date, September 25, 2009.

IX. THE PRIOR ART

A. Paretti

51. Paretti was filed September 23, 2008. Ex-1005, Cover.

52. I understand that Paretti is prior art under at least §102(e).

53. 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.

54. 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; *see also id.*, 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).

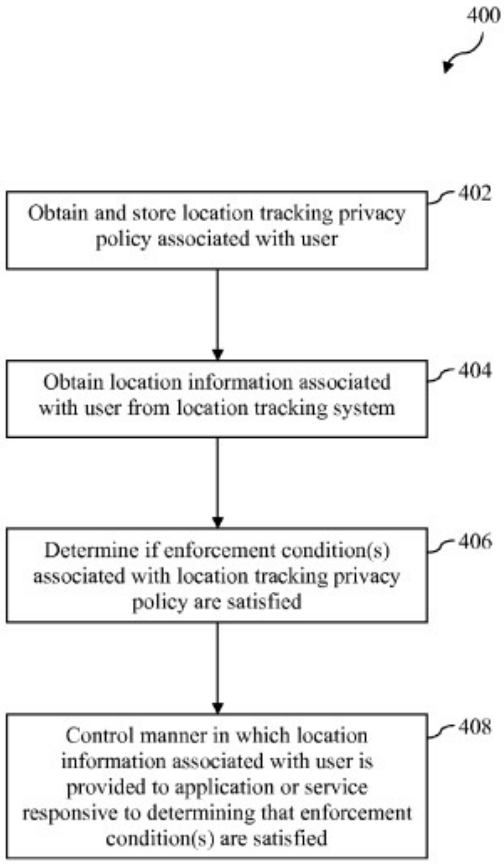

FIG. 4

55. 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

56. Parupudi issued on June 15, 2004. Ex-1006, Cover.

57. I understand that Parupudi is prior art under at least §102(b).

58. 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

59. Parupudi's Figure 10 below 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.

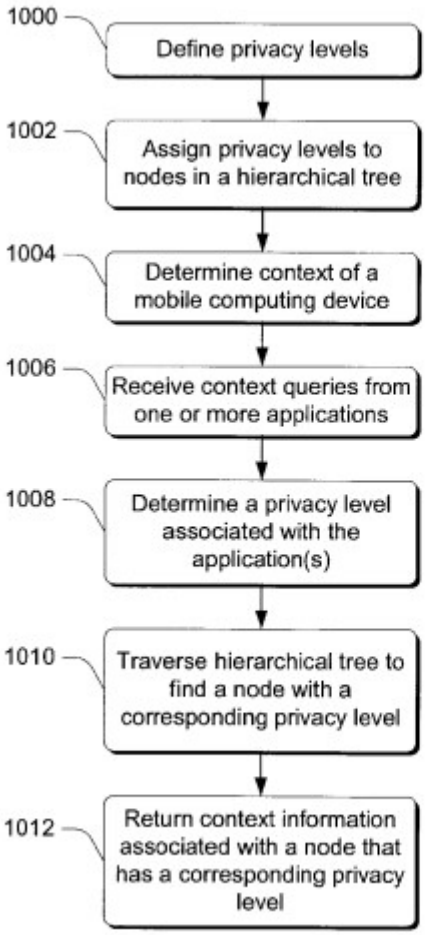

Fig. 10

60. At Steps 1000 and 1002, privacy levels are defined and assigned "to nodes in a hierarchical tree." *Id.*, Figure 10. 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.* 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

61. Nykanen issued on July 15, 2003. Ex-1007, Cover.

62. I understand that Nykanen is prior art under at least §102(b).

63. 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.

64. With respect to the "terminal" of its 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.

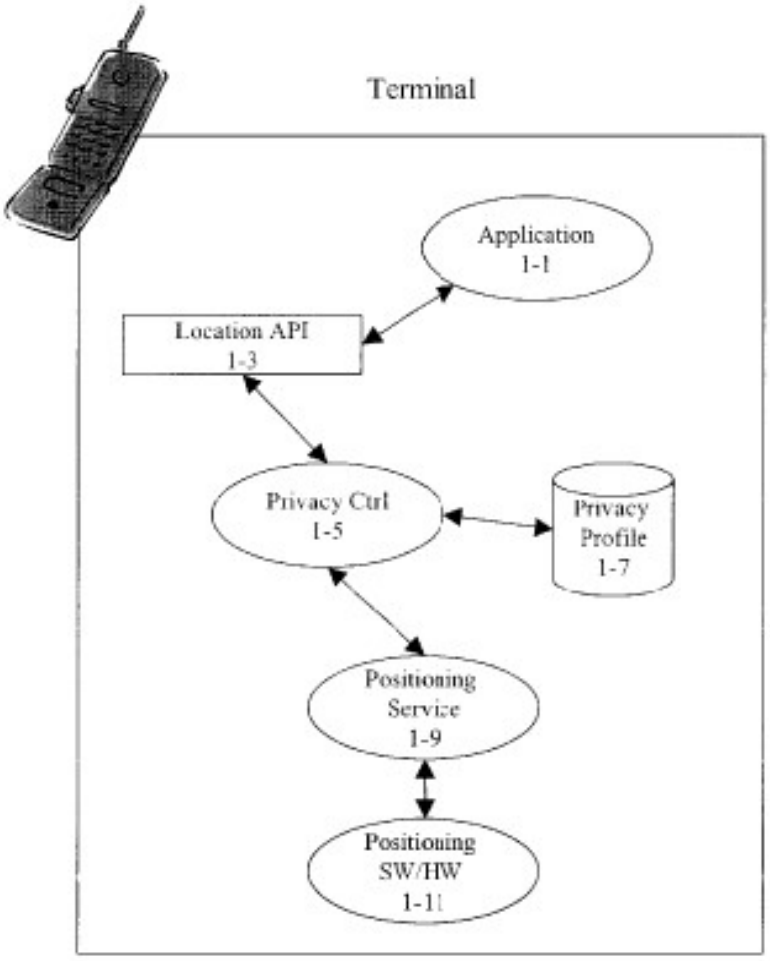

FIG. 1

65. 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; *see also id.*, Claim 1.

66. 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.

X. SPECIFIC BASES OF MY INVALIDITY OPINIONS

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[3]

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

67. Paretti discloses a method and therefore discloses the preamble of Claim 1, to the extent it is limiting.

[3] *See* Ex-1020.

68. For example, 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 (emphasis added), 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"), ¶11 ("a method for recommending a location tracking privacy policy to a user is described herein").

69. Indeed, Paretti discloses a "***method*** for automatically enacting a location tracking privacy policy for a user." *Id.*, ¶17 (emphasis added).

70. In fact, Paretti discloses a "location reporting ***methodology***" that "defines how location information received from location tracking system…is to be provided to context-aware applications/services." *Id.*, ¶84 (emphasis added).

71. Paretti additionally discloses, for example, a "method for enabling a user to modify logged location information associated with the user," a "manner in which visibility manager 208 operates to control both types of location information to protect the privacy and/or security of a user," a "method by which location tracking privacy engine 104 automatically recommends a location tracking privacy policy to a user," and a "method…in which visibility recommender 210 determines

a current context of a user." *Id.*, ¶¶121, 131, 138, 155, Figure 6, Figure 8, Figure 10, Figure 11.

72. Accordingly, Paretti discloses a method.

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;

73. Paretti discloses Elements 1[a], 21[a], 25[pre] (to the extent 25[pre] is limiting), and 25[a].

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

75. Paretti discloses "mobile user devices (e.g., mobile telephones, personal digital assistants, laptop and handheld computers…)." Ex-1005, ¶¶38-40, 52, 158-163, Figure 12.

76. Accordingly, Paretti discloses a mobile computing device.

77. Further, Paretti discloses that its "mobile user devices (e.g., mobile telephones, personal digital assistants, laptop and handheld computers…)" include a "location tracking privacy engine," which is "configured to control the manner in which…location information is provided to context-aware applications/services." *Id.*, ¶¶38-39, 52, 158-163, Figure 12.

78. Accordingly, Paretti discloses establishing a context policy enforcement engine on a mobile computing device as a POSITA would have understood that Paretti's location tracking privacy engine is "a context policy enforcement engine." *See* Section V.

79. Paretti discloses that its location tracking privacy engine comprises "user interface," "W4 data database," "privacy policies database," "visibility manager," and "location tracking system interface." *Id.*, ¶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.

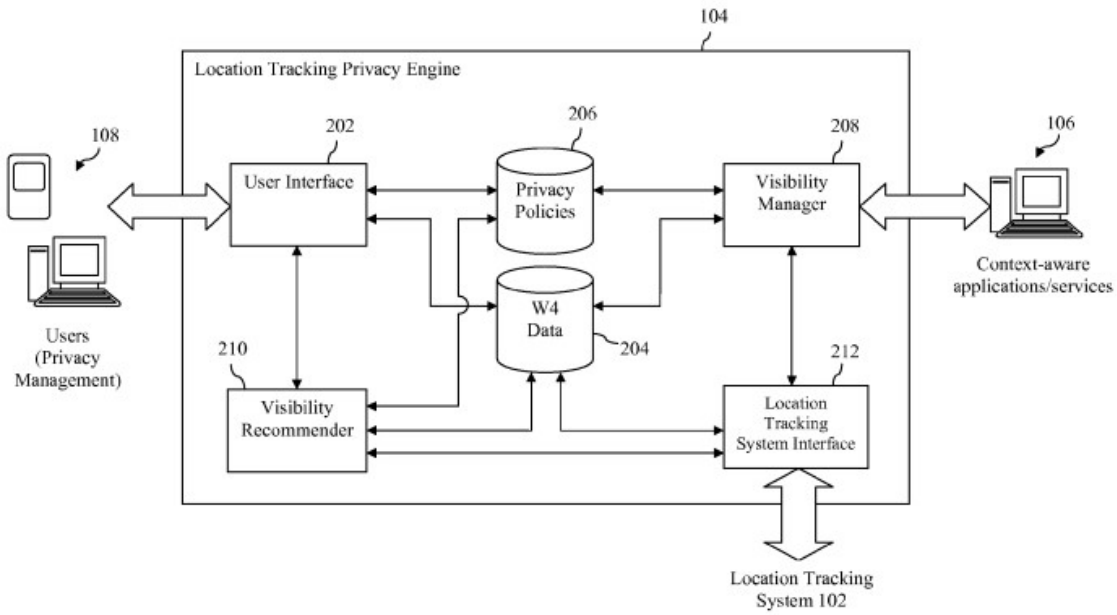

FIG. 2

80. Accordingly, Paretti discloses establishing a context policy enforcement engine.

81. For example, Paretti discloses a system wherein a "location tracking system" can "periodically log time-stamped location information" related to a user. *Id.*, ¶116. Because the context information "may be deemed extremely private to a user," the mobile computing device employs the "location tracking privacy engine," which "operates to protect a user's privacy and/or security by selectively applying location reporting methodologies to user location information received from location tracking system…before providing such location information to context-aware applications/services." *Id.*, ¶117. Operation of the "location reporting

methodologies" can result in "non-delivery or obscuring of such location information." *Id.; see also id.*, ¶118-125.

82. Accordingly, Paretti provides further disclosure regarding establishing a context policy enforcement engine.

83. 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. *Id.*, ¶¶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").

84. Thus, Paretti discloses a mobile computing device comprising the context policy enforcement engine.

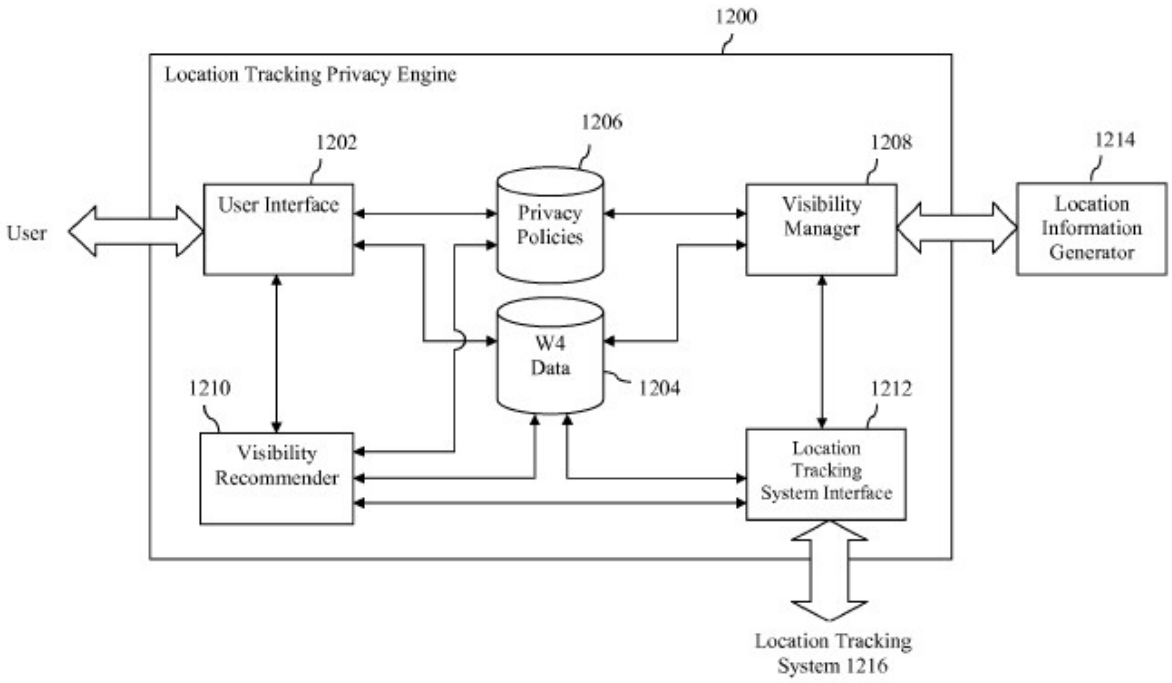

FIG. 12

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

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:

86. Paretti discloses Elements 21[pre] (to the extent it is limiting), 25[b], and 25[c].

87. Specifically, 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.

88. 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").

89. Accordingly, 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.

90. Indeed, Paretti discloses various machine readable, executable instructions, including, for example, relating to the "privacy policies" stored in "privacy policies database 206." *Id.*, ¶73. These privacy policies comprise instructions that "govern how location tracking privacy engine 104 provides location information about the user to context-aware applications/services." *Id.*, ¶71. Each privacy policy may "include a location reporting methodology and one or more conditions under which the location reporting methodology is to be enforced." *Id*., ¶75. Thus, Paretti provides further disclosure regarding the plurality of instructions.

91. Accordingly, 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.

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;

92. Paretti discloses Elements 1[b], 1[c], 21[b], and 25[c][i].

93. Paretti discloses receiving, from a requesting entity, a request for context information related to a user of the mobile computing device.

94. 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.

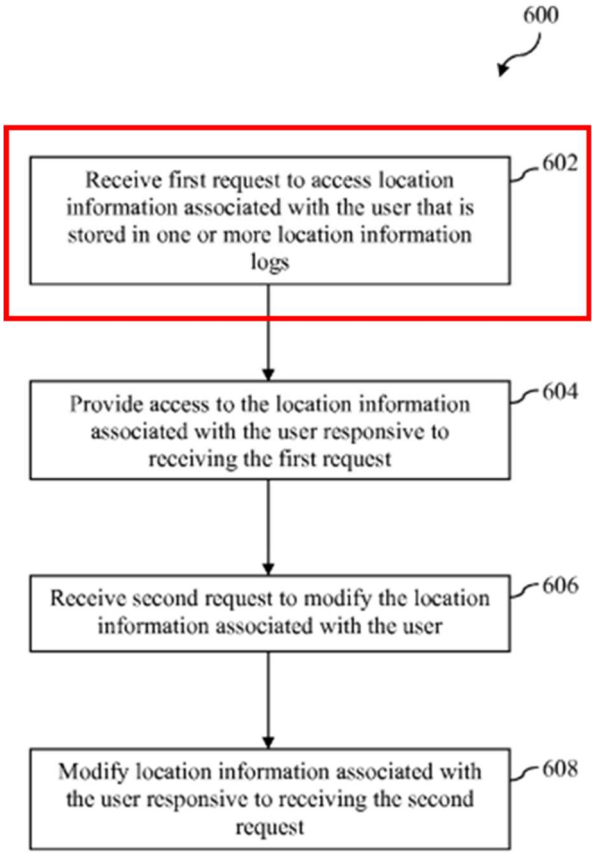

FIG. 6

95. Paretti also discloses the context policy enforcement engine retrieving context policy data which defines a set of rules for responding to context requests.

96. 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.

97. Accordingly, Paretti discloses the context policy enforcement engine retrieving context policy data.

98. Paretti further discloses that its 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." *Id.*, ¶¶70-73.

99. Accordingly, Paretti discloses context policy data which defines a set of rules for responding to context requests.

100. Indeed, Paretti's "privacy policies" (i.e., the claimed "context policy data") define rules for responding to context requests, including, for example, instructing the device to "substitut[e] new user location information for the user

location information obtained from location tracking system 102" and/or instructing the device to provide user information "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." *Id.*, ¶¶84-86.

101. Thus, Paretti provides further disclosure regarding context policy data which defines a set of rules for responding to context requests.

102. Accordingly, Paretti 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.

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];

103. Paretti discloses Elements 1[d], 21[c], and 25[c][ii].

104. Specifically, 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.

105. 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.

106. 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.

107. Indeed, Paretti discloses several exemplary privacy policies that comprise determining a level of specificity as a function of the identity of the requesting entity. For example, Paretti discloses a privacy policy in which "location information" may be shared with "persons or entities that share a topical nexus with the user"; under this policy, a "user interested in purchasing a car may enact a policy that allows location information about the user to be reported to car dealerships

and/or other persons and entities interested in selling cars." *Id.*, ¶103. Paretti's privacy policies may also "explicitly identify persons or categories of persons that should receive the most precise level of location information about the user, while specifying that other persons or categories of persons should receive less granular location information, modified location information or no location information at all." *Id.*, ¶95; *see also id*., ¶¶96-99. Illustratively, Paretti notes that "a user may specify that family members should always receive the most precise location information, co-workers should receive less precise location information, and everyone else should not receive any location information whatsoever." *Id*.

108. Thus, Paretti provides further disclosure 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 identity of the requesting entity.

109. Moreover, Paretti discloses that, after accessing the privacy policies, the 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.

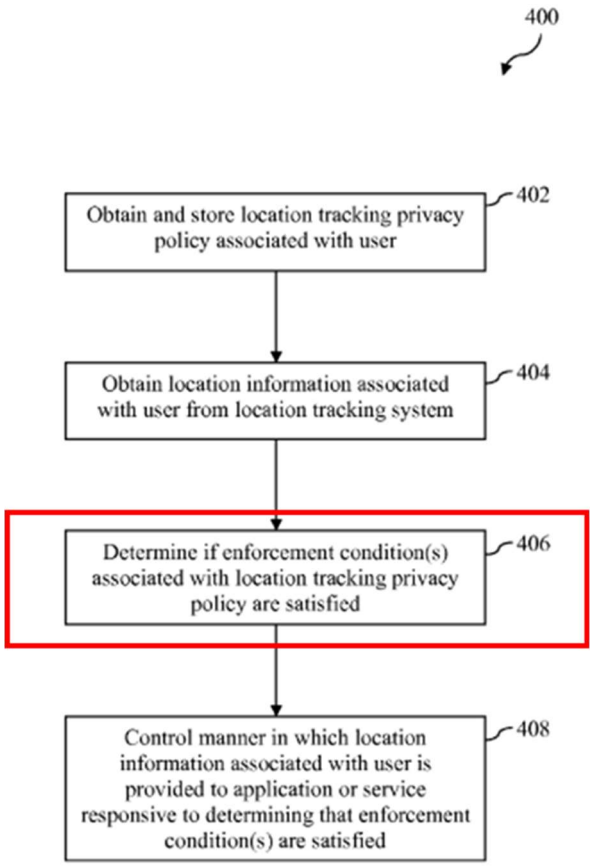

FIG. 4

110. 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.

111. 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." *Id.*, ¶88; *see also id.*, ¶¶82-92.

112. Accordingly, Paretti provides further disclosure 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.

113. 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").[4] *Id.*, ¶86 (emphasis added); *see also id.*, ¶¶82-92.

[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.), each having an associated characteristic (e.g., granularity, confidence, currency, etc.)."

114. Thus, Paretti provides further disclosure regarding determining a level of specificity of a context characteristic for a context parameter associated with the requested context information.

115. Accordingly, Paretti discloses determining a level of specificity of a context characteristic for a context parameter associated with the requested context

---

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 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.)."), 6:15-24 ("The illustrative context data structure 300 also includes a context data 304 that defines three levels of specificity for the confidence characteristic of the location context parameter. The illustrative confidence characteristic includes a high granularity level indicating the user swiped his RFID tag at an entry door to a particular room, which provides a high degree of confidence that the user is actually within the room or at a GPS coordinate within the room. The illustrative confidence characteristic also includes a middle granularity level indicating that the user swiped his RFID inside at an entry door to a particular building at work, which provides a degree of confidence that the user is within that particular building. Additionally, the illustrative confidence characteristic includes a low confidence level indicating the user accessed a wireless access point that includes the building (but may include other buildings within the work campus area).").

information as a function of the context policy data and an identity of the requesting entity.

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

116. Paretti discloses Elements 1[e], 21[d], and 25[c][iii].

117. Specifically, 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.

118. Paretti discloses a system in which a device can obtain context data with varying levels of specificity. For example, "location tracking system 102 may be premised on any of a variety of well-known technologies for producing such location information, including but not limited to Global Positioning System (GPS) technology, Wi-Fi technology, cellular telephony technology and/or Bluetooth™ technology." Ex-1005, ¶37. As a result of the differences between these types of technology, the "location tracking system 102" may "track the location of such mobile devices with varying degrees of accuracy." *Id*.

119. 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." *Id.*, ¶¶75, 81, 91, Figure 4; *see also id.*, ¶¶36-44, 48-52, 70-73, 82-92, Figure 4.

120. 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.

121. Paretti's disclosed "enforc[ing]" 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] context data identified by the determined level of specificity"). *Id.*, ¶84; *see also id.*, ¶¶82-92.

122. Accordingly, Paretti provides further disclosure 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.

123. 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 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.

124. 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."

125. Thus, Paretti provides further disclosure 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.

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.

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

127. Paretti discloses Elements 1[f], 21[e], and 25[c][iv].

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

129. 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. In addition to "context-aware applications," Paretti also discloses providing the location information to requesting "family members" or "co-workers," for example. *Id.*, ¶96.

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

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

131. Paretti discloses dependent Claim 3.

132. Specifically, Paretti discloses establishing the context policy enforcement engine in software.

133. 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).

134. Accordingly, Paretti discloses establishing the context policy enforcement engine in software.

135. Indeed, Paretti discloses that its "invention is [] directed to ***computer program products comprising software*** stored on any computer readable medium." *Id.*, ¶171 (emphasis added*); see also id*., ¶¶167-170.

136. Thus, Paretti provides further disclosure regarding establishing the context policy enforcement engine in software.

137. Accordingly, Paretti discloses establishing the context policy enforcement engine in software.

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

138. Paretti discloses dependent Claim 4.

139. Specifically, Paretti discloses receiving the request for context information from a software application.

140. 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.

141. Accordingly, Paretti discloses receiving the request for context information from a software application.

142. 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." *Id.*, ¶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; *see also id*., ¶43.

143. Thus, Paretti provides further disclosure regarding receiving the request for context information from a software application.

144. Indeed, Paretti explains that requesting software applications may include "any location-based or location aware-service," such as "personal navigation services, resource location services" (e.g., "providing an identification of a local

business"), "resource tracking services (e.g., tracking of objects such as packages and train boxcars), resource tracking services with dynamic distribution" (e.g., "fleet scheduling and tracking of taxis"), "proximity-based notification services" (e.g., "alerts or notices, such as notification of a sale on gas" or "warning of a traffic jam"), "location-based content delivery services (e.g., local weather, targeted advertising or coupons), location-based billing services (e.g., EZ pass and toll watch), and emergency services." *Id.*, ¶42.

145. Thus, Paretti provides further disclosure regarding receiving the request for context information from a software application.

146. Accordingly, Paretti discloses receiving the request for context information from a software application.

4. Dependent 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"

147. Paretti discloses dependent Claim 5.

148. Specifically, Paretti discloses receiving a request for a location of the user.

149. 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.

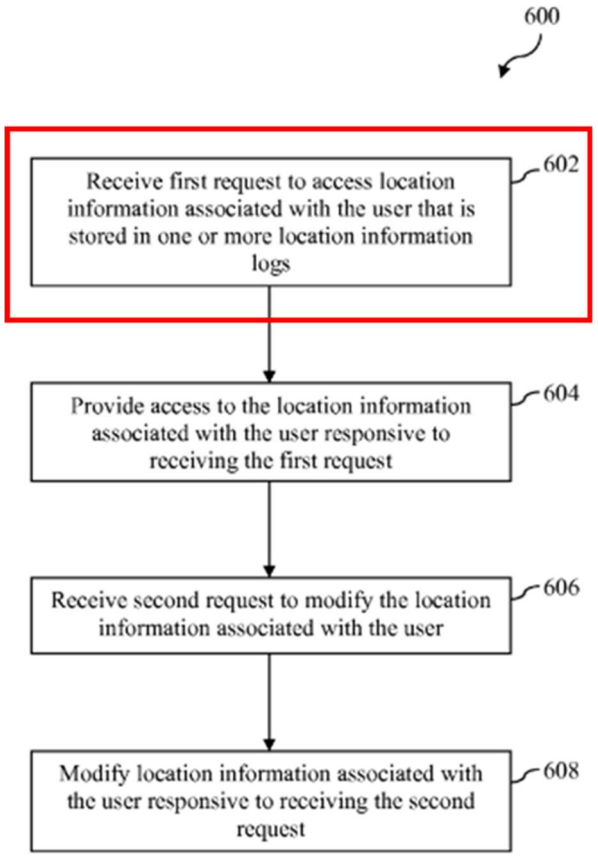

FIG. 6

150. Accordingly, Paretti discloses receiving a request for a location of the user.

151. Further, Paretti discloses that this location information can include both "actual location information," like "latitude/longitude coordinates, zip code, street address, or the like" and "relative location information that indicates or identifies the proximity of the user to other users, devices, beacons, or the like." *Id.*, ¶89.

152. Thus, Paretti provides further disclosure regarding receiving a request for a location of the user.

153. Accordingly, Paretti discloses receiving a request for a location of the user.

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

154. Paretti discloses dependent Claim 7.

155. Specifically, Paretti discloses context policy data that defines a context policy rule based on the identification of the requesting entity.

156. 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.

157. Accordingly, Paretti discloses context policy data that defines a context policy rule based on the identification of the requesting entity.

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

158. Paretti discloses dependent Claim 9.

159. Specifically, Paretti discloses context policy data that defines a rule based on a context parameter associated with the user.

160. 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")]."[5] 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

[5] 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. The '629 Patent further discloses: "Additionally, the context policy rules 400 may use any number of rule qualifiers to define the rule itself. For example, the context policy rule 412 defines context data that should be provided to a requesting application if the…user's activity is 'shopping' [and/or if] the user is currently located in a location identified as 'flower shop.' As shown, the context policy rule 412 provides a low granularity for the location parameter such that the requesting entity cannot determine exactly where the user is (e.g., so as not to run a well planned surprise)." *Id.*, 7:52-8:13.

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 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.

161. Accordingly, Paretti discloses context policy data that defines a rule based on a context parameter associated with the user.

162. Paretti also discloses privacy policies that are defined based on a determination "that the user is engaging in an activity associated with a particular topic." *Id.*, ¶101. In this embodiment, the "context parameter" is the user's current activity. Paretti further discloses that the visibility manager may dictate that when a user is partaking in a particular "personal or professional activity" "during which user privacy is important or during which the user wishes to avoid interruption by others," the device should enforce a privacy policy that either "prohibits the reporting of location information about the user" or "provides less granular location information about the user." *Id.*, ¶102.

163. Thus, Paretti provides further disclosure regarding context policy data that defines a rule based on a context parameter associated with the user.

164. Accordingly, Paretti discloses context policy data that defines a rule based on a context parameter associated with the user.

7. Dependent 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"

165. Paretti discloses dependent Claim 10.

166. Specifically, Paretti discloses context policy data that 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.

167. 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. Indeed, Paretti's visibility manager may determine that a particular privacy policy should be enforced based on the user's location. *Id*., ¶110. The conditions for enforcing a certain privacy policy may include, for example, "determining whether a location of the user matches a specified location or is within a predefined area, or by determining whether the user is proximate to a specified location, area, person, device or object." *Id*., ¶110. 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.

168. Accordingly, Paretti discloses context policy data that 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.

8. Dependent 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"

169. Paretti discloses dependent Claim 11.

170. Specifically, Paretti discloses context policy data that defines a rule based on the requested context information and the time of day at which the request for context information is received.

171. 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. Indeed, Paretti's visibility manager may determine that a particular privacy policy should be enforced based on "[t]emporal data" or "time-based data (e.g. time

stamps)…that relate to specific times and/or events associated with a user." *Id*., ¶65. Such temporal data may include "passively-collected time data (e.g., time data from a clock resident on an electronic system/device, or time data from a network clock), or actively-collected time data, such as time data entered by the user." *Id*. 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.

172. Accordingly, Paretti discloses context policy data that defines a rule based on the requested context information and the time of day at which the request for context information is received.

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

173. Paretti discloses dependent Claim 12.

174. Specifically, Paretti discloses context policy data that defines a rule based on the requested context information and an activity of the user.

175. 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."[6] *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.

176. Indeed, Paretti discloses that its privacy policies may be defined based on an activity of the user, including, for example, a user's attendance at a "geographically defined event," "interactions and connections between the user and the intended recipient," a user's designation of days as "vacation days," and a user's attendance "of a conference." *Id.*, ¶¶98-107. Thus, for example, in the example of a user's attendance "of a conference," "a privacy policy may specify that for the duration of a conference attended by a user, location information about the user

[6] The '629 Patent discloses: "Additionally, the context policy rules 400 may use any number of rule qualifiers to define the rule itself. For example, the context policy rule 412 defines context data that should be provided to a requesting application if the…user's activity is 'shopping' [and/or if] the user is currently located in a location identified as 'flower shop.' As shown, the context policy rule 412 provides a low granularity for the location parameter such that the requesting entity cannot determine exactly where the user is (e.g., so as not to run a well planned surprise)." Ex-1001, 7:52-8:13.

should be reported to any persons attending the conference." *Id.* Additionally, Paretti discloses that privacy policies may be defined based on deduced "activity information, such as past activity information, present activity information, and predicted future activity information." *Id.*, ¶68.

177. Accordingly, Paretti discloses context policy data that defines a rule based on the requested context information and an activity of the user.

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

178. Paretti discloses dependent Claims 13 and 22.

179. Specifically, Paretti discloses determining context data based on the set of rules of the context policy data.

180. 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.

181. Indeed, Paretti discloses the use of "deduced information" in determining context data. *Id.*, ¶67. This information "may be deduced based on one or more of social data 302, topical data 304, temporal data 306, and social data." *Id*. Such "deduced information" may include, for example, "primary user location, secondary user location, past locations, present location," "predicted future location," "past activity information, present activity information," "predicted future activity information," "cultural preferences and/or buying preferences information." *Id*., ¶¶67-69.

182. Accordingly, Paretti discloses determining context data based on the set of rules of the context policy data.

11. Dependent 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"

183. Paretti discloses dependent Claims 14 and 23.

184. Specifically, Paretti discloses 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.

185. 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")[7] "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, 47-52, 70-73, 82-92. In particular, the "location tracking privacy engine 104 is configured to obtain location information about tracked entities 110 from location tracking system 102 and to provide such information to context-aware applications and services 106" "in accordance with privacy policies set by users associated with the tracked entities." *Id.*, ¶40. 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

[7] 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. *See, e.g.*, Section VII.

"selectively modifying the…granularity of the…location information based on a recipient application." *Id.*, ¶84; *see also id.*, ¶¶82-92.

186. Indeed, Paretti discloses that "[l]ocation tracking system 102 is intended to broadly represent any system capable of automatically tracking the location of certain entities." *Id.*, ¶37. "Generally speaking, location tracking system 102 is configured to obtain location information about a plurality of tracked entities 110, wherein such location information may be indicative of a current, past or future location of each of tracked entities 110." *Id.; see also id.*, ¶89 ("location information associated with the user may be obtained from location tracking system 102 by location tracking system interface 212;" "[t]he user location information received in step 404 may be indicative of a past, current or future location of the user"). "For example, mobile devices that incorporate such technology may provide information to location tracking system 102 that can be used to track the location of such mobile devices with varying degrees of accuracy." *Id.*, ¶37. "However, this example is not intended to be limiting, and location tracking system 102 may utilize other methods for tracking the location of tracked entities 110." *Id.*

187. Indeed, "location tracking system 102 shown in FIG. 1 may include or maintain one or more logs that store location information." *Id.*, ¶116. "Such location information may be periodically provided by or obtained from devices and objects associated with users as well as by other objects and devices" (e.g., "the location

tracking system [may be] configured to periodically log time-stamped location information received from the sensor-enabled devices" where "[t]he time stamp may indicate when such location information was generated or obtained"). *Id.*, ¶116. "Such logged location information represents information that may be deemed extremely private to a user, since the logged location information may be used to determine the location of the user at various points in time, including during the past, the present, and potentially the future (based on some form of extrapolation)." *Id.*, ¶117. Accordingly, "location tracking privacy engine 104 operates to protect a user's privacy and/or security by selectively applying location reporting methodologies to user location information received from location tracking system 102 before providing such location information to context-aware applications/services 106, wherein the application of the location reporting methodologies may result in the non-delivery or obscuring of such location information." *Id.* "However, the application of such location reporting methodologies does not in any way affect the logged location information stored by location tracking system 102." *Id.*

188. Indeed, further detail about location tracking privacy engine 104 is shown in FIG. 2. *Id.,* ¶47.

189. Moreover, Paretti discloses that its "W4 data database 204 is configured to store data associated with users of location tracking privacy engine 104." *Id.,* ¶54.

"The data stored in W4 data database 204 is also used by location tracking privacy engine 104." *Id.* "As shown in FIG. 3, the data stored in W4 data database 204 may include social data 302, topical data 304, temporal data 306 and spatial data 308." *Id.,* ¶56.

190. Accordingly, Paretti discloses 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.

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

191. Paretti discloses dependent Claim 15.

192. Specifically, Paretti discloses a method wherein responding to the request further comprises transmitting the context data.

193. 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. This may include, for example, transmission through "an interface" which comprises an "an application programming interface (API)" that "that can be used to build applications or processes by which a context-aware application/service can interact with location tracking privacy engine 104." *Id.*, ¶43.

194. Moreover, Paretti discloses that "[b]ecause an embodiment of the present invention allows a user to associate any of a plurality of different location reporting methodologies with any number of persons or categories of persons, it advantageously allows a user to exercise a significant degree of control over who will receive location information about the user and what type of location information will be received." *Id.*, ¶96. "Thus, for example, a user may specify that family members should always receive the most precise location information, co-workers should receive less precise location information, and everyone else should not receive any location information whatsoever." *Id.*; *see also id.*, ¶¶93-99.

195. Accordingly, Paretti discloses a method wherein responding to the request further comprises transmitting the context data.

13. Dependent 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"

196. Paretti discloses dependent Claims 16 and 24.

197. Specifically, Paretti discloses 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.

198. 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." *Id.*, ¶84; *see also id.*, ¶¶82-92.

199. Indeed, when Paretti's location tracking system determines a user's location, it may "include actual location information, such as a geographical identifier of a location of an entity (including but not limited to longitude/latitude coordinates, street address, city name, zip code, or the like) or relative location information, such as proximity to certain identifiable entities including but not limited to other tracked entities." *Id.*, ¶37. Paretti's location tracking system may "be premised on any of a variety of well-known technologies for producing such location information, including but not limited to Global Positioning System (GPS) technology, Wi-Fi technology, cellular telephony technology and/or Bluetooth™ technology." *Id.* Accordingly, "mobile devices that incorporate such technology may provide information…with varying degrees of accuracy."[8] *Id.* For example, a

[8] The '629 Patent discloses: "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

POSITA would have understood that a device using cellular telephony technology and GPS technology would gather location information at both a more approximate and more precise scale. *See* Section V.

200. Accordingly, Paretti discloses 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.

14. Dependent 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"

201. Paretti discloses dependent Claim 18.

---

defines three levels of specificity for the granularity characteristic of the location context parameter." Ex-1001, 5:34-65. The '629 Patent also discloses: "The illustrative context data structure 300 also includes a context data 304 that defines three levels of specificity for the confidence characteristic of the location context parameter. The illustrative confidence characteristic includes a high granularity level indicating the user swiped his RFID tag at an entry door to a particular room, which provides a high degree of confidence that the user is actually within the room or at a GPS coordinate within the room. The illustrative confidence characteristic also includes a middle granularity level indicating that the user swiped his RFID inside at an entry door to a particular building at work, which provides a degree of confidence that the user is within that particular building. Additionally, the illustrative confidence characteristic includes a low confidence level indicating the user accessed a wireless access point that includes the building (but may include other buildings within the work campus area)." *Id.*, 6:15-24.

202. Specifically, Paretti discloses receiving a 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.

203. Paretti discloses a system that "enabl[es] a user to control the manner in which location information associated with the user is obtained, disseminated and/or reported." Ex-1005, ¶36; *see also id.*, ¶39 ("Tracked entities 110 are intended to broadly represent any entities that are capable of being tracked by a location tracking system. Such entities include, but are not limited to people, animals, mobile user devices (e.g., mobile telephones, personal digital assistants, laptop and handheld computers, media players, handheld navigation devices, handheld scanners), vehicles (e.g., automobiles, airplanes, trucks, trains), office equipment (e.g., computers, printers, copiers), appliances, inventory, freight, parcels, or commercial products, to name only a few."). Accordingly, 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.*, ¶¶36-43, 51-52. These "[p]rivacy policies specified by a user are stored in privacy policies database 206."[9] *Id.*, ¶¶44, 49; *see also id.*, ¶¶36-43, 51-52, 103.

[9] The '629 Patent discloses: "The user interface 210 may be configured, for example, to allow the user to add, delete, update, or otherwise modify the context policy rules included in the context policy rule database. For example, the user

204. Accordingly, Paretti discloses receiving a 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.

205. Moreover, Paretti additionally discloses that the user can enact new privacy policies using the visibility recommender. The visibility recommender helps the user to create new privacy policies as it is "configured to generate recommendations regarding the creation of new privacy policies or the modification of existing privacy policies for a user." *Id.*, ¶77. The recommendations may be provided in "respons[e] to a user request provided via user interface 202." *Id.*; *see also id.*, ¶¶78-79, 138-149, 155-159. Users may select and enact the recommended policy via the user interface 202. *See id.*, ¶¶49-50.

206. Thus, Paretti provides further disclosure regarding receiving a 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.

---

may decide to allow access all applications in the 'public' group to location context data having high granularity. If so, the user may interact with the user interface to update the associated context policy rule. Additionally, the user may define which requesting applications or entities below to which group or otherwise define groups or associations of applications and entities with which various context policy rules may be created and defined." Ex-1001, 8:14-32.

207. Accordingly, Paretti discloses receiving a 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.

15. Dependent 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"

208. Paretti discloses dependent Claim 19.

209. Specifically, Paretti discloses 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.

210. 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.*, ¶¶100-115.

211. Such information may include, for example, "location data entered into a system/device by a user," "calendar days designated as vacation days by a user," "the duration of a conference attended by a user," "metadata added by a user," and

"cultural preferences and/or buying preferences…provided by a user."[10] *Id.*, ¶¶62, 66, 69, 107.

212. "W4 data database 204 is configured to store data associated with users of location tracking privacy engine 104 that may be used by location tracking privacy engine 104 to determine when the proper conditions or context exist for enforcing a particular privacy policy for a user." *Id.*, ¶54; *see also id.*, ¶¶53-69. "The user data stored in W4 data database 204 may be actively provided by a user (such as via user interface 202) or provided by one or more networks, systems or databases that aggregate such data, or by a combination of the foregoing." *Id.*, ¶54. "Although W4 data database 204 is shown as a single database in FIG. 2, it is to be understood that depending on volume, the W4 data may be stored in numerous databases;" "[s]uch databases may be managed by numerous database servers in communication with location tracking privacy engine 104." *Id.*, ¶55.

[10] The '629 Patent discloses: "In some embodiments, the policy enforcement engine 102 may allow the user to update context data related to the user and stored in the context database. For example, in certain circumstances, some of the context data may be unavailable through automatic collection means (e.g., location via a GPS sensor). In such cases, the user may supply, update, modify, or correct the context data or otherwise add additional details related to the context data via use of the user interface. For example, if the user is at a particular flower shop, the user may enter the name of the flower shop rather than the generic 'flower shop' location tag such that authorized requesting applications have access to more specific or other an increased amount of context data." Ex-1001, 8:33-45.

213. "As shown in FIG. 3, the data stored in W4 data database 204 may include social data 302, topical data 304, temporal data 306 and spatial data 308;" "[s]uch categories of data are also respectively referred to herein as 'who, what, when and where' data, or W4 data." *Id.*, ¶56. "Spatial data 308 may be any information associated with a location of the user and/or an electronic system/device associated with the user." *Id.*, ¶66. "For example, spatial data 306 may include any passively-collected location data, such as cell tower data, GPRS data, GPS data, WI-FI data, personal area network data, IP address data and data from other network access points, or actively-collected location data, such as location data entered into a system/device by a user." *Id.* "In one embodiment, spatial data 308 is obtained, at least in part, from location tracking system 104 via location tracking system interface 212." *Id.*

214. Paretti further discloses that "[t]racked entities 110 are intended to broadly represent any entities that are capable of being tracked by a location tracking system." *Id.*, ¶39. "Such entities include, but are not limited to people, animals, mobile user devices (e.g., mobile telephones, personal digital assistants, laptop and handheld computers, media players, handheld navigation devices, handheld scanners), vehicles (e.g., automobiles, airplanes, trucks, trains), office equipment (e.g., computers, printers, copiers), appliances, inventory, freight, parcels, or commercial products, to name only a few." *Id.*

215. Thus, Paretti provides further disclosure regarding 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.

216. Accordingly, Paretti discloses 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.

B. Ground 2: Claims 1, 3-5, 7-8, 13-16, 18, and 20-25 are obvious over 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.

217. 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. *See* Section VII. 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..

218. 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. *See* Section VII. 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. *See* Section VII. 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. *See* Section VII.

219. Moreover, implementing Nykanen's database-related mechanisms into Parupudi's system would have been a straightforward engineering task for a POSITA. *See* Section VII. 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. *See generally* Ex-1006, Ex-1007. 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. *See* Section VII. 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. *See* Section VII. 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. *See* Section VII.

2. Independent Claims 1, 21, and 25[11]

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

220. Parupudi in combination with Nykanen discloses the preamble of Claim 1, to the extent it is limiting.

221. Specifically, Parupudi discloses a method.

[11] *See* Ex-1020.

222. In particular, 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.

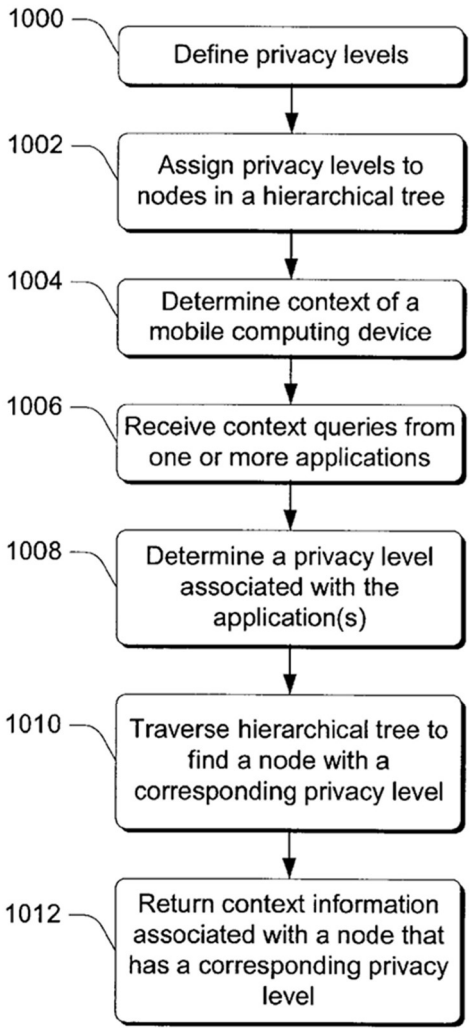

Fig. 10

223. Indeed, Parupudi discloses "***steps in a privacy protection method*** in accordance with the described embodiment;" "[t]hese steps can be implemented by

the privacy manager 704." *Id.*, 24:31-34 (emphasis added); *see also id*., Figures 4-5, 8-10.

224. Accordingly, Parupudi discloses a method, and thus Parupudi in combination with Nykanen discloses the preamble of Claim 1, to the extent it is limiting.

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;

225. Parupudi in combination with Nykanen teaches Elements 1[a], 21[a], 25[pre] (to the extent 25[pre] is limiting), and 25[a].

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

227. 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)." Ex-1006, 3:10-15, 7:54-65, 24:10-19; *see also id.*, Abstract, 18:53-67, 23:36-24:7. Parupudi's disclosed "computing device" can "refer generally to any type of computing device;" an exemplary computing device would "typically 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. This

computing device may be a "mobile computing device[]" and/or "hand-held computing device." *Id*.

228. Parupudi's disclosed "mobile computing devices" comprise 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." *Id.*, 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").

229. Parupudi's privacy manager "determines what level of information to provide to applications that…request" "location information." *Id.*, 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.

230. 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.

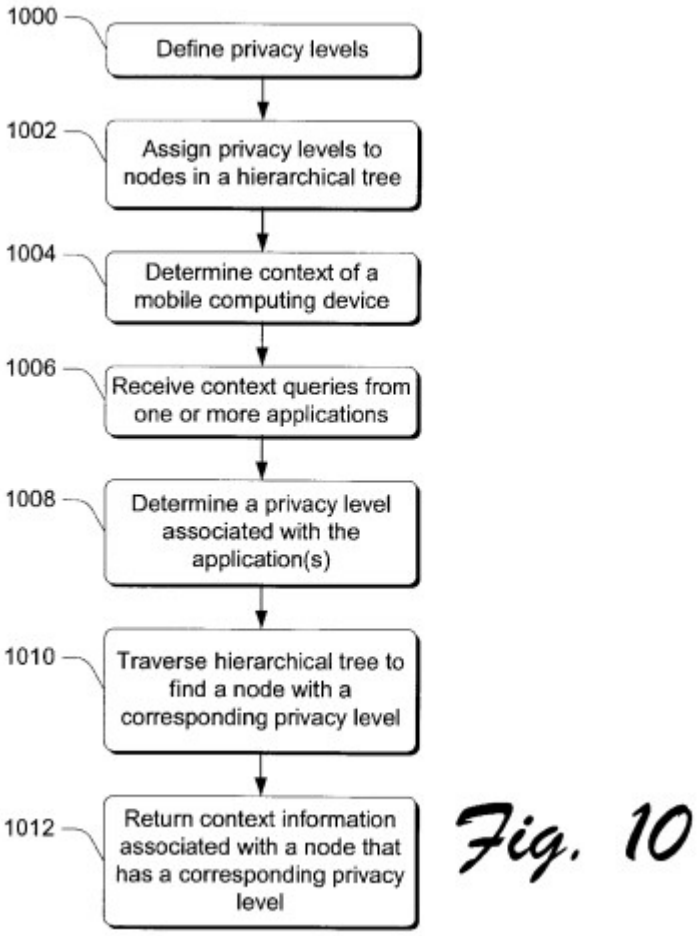

Fig. 10

231. At Steps 1000 and 1002, privacy levels (i.e., of the claimed "context policy enforcement engine") are defined and assigned. *Id.*, Figure 10. 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." *Id.*, 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.

232. Thus, Parupudi's privacy manager is a "context policy enforcement engine."

233. 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.

234. Indeed, Nykanen discloses "a mobile terminal in a wireless network environment." *Id.*, 1:10-31. The "mobile terminal" comprises "Global Positioning

System (GPS) hardware" as well as "Bluetooth hardware." *Id*. In "an exemplary embodiment of a terminal of the present invention," the device comprises "a processor designed for use in a mobile and/or portable environment," "wireless network interface 6-1, memory 6-5, GPS (global positioning service) hardware and interface 6-7, keypad interface 6-13, display interface 6-9, and audio interface 6-4." *Id*., 12:7-15; *see also id*., 12:16-13:28, Figures 1-7.

235. Accordingly, Nykanen discloses a mobile computing device.

236. Moreover, 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.

237. Thus, Nykanen's privacy control module in the terminal (i.e., the claimed "mobile computing device") is "a context policy enforcement engine."

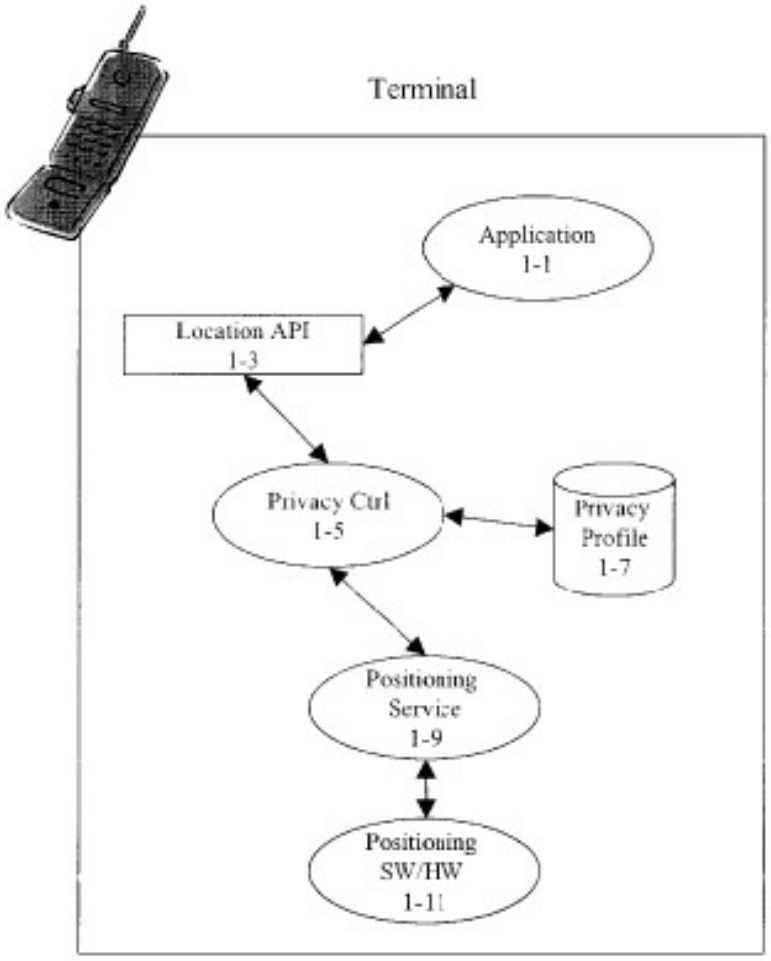

FIG. 1

238. 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"). *Id.*, 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.*

239. Accordingly, Nykanen discloses establishing a context policy enforcement engine on a mobile computing device.

240. 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. *See* Section VII. 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. *See* Section VII. 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. *See* Section VII. A POSITA would have recognized that such expanding functionality for a privacy-preferences database would further Parupudi's privacy-protecting goals. *See* Section VII.

241. 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. *See* Section VII. 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. *See* Section VII.

242. Accordingly, Parupudi in combination with Nykanen teaches establishing a context policy enforcement engine on a mobile computing device, and thus Parupudi in combination with Nykanen teaches Elements 1[a], 21[a], 25[pre] (to the extent 25[pre] is limiting), and 25[a].

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:

243. Parupudi in combination with Nykanen discloses Elements 21[pre] (to the extent it is limiting), 25[b], and 25[c].

244. Specifically, 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.

245. 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.

246. Accordingly, 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.

247. Indeed, Parupudi discloses a non-transitory, machine readable medium comprising (or a memory device having stored therein) a plurality of instructions as, for example, Parupudi discloses instructions to "call the API layer to ascertain location information from the location service module," instructions to determine "confidence and accuracy parameters that are assigned to the information," and instructions to determine "a measure of the trust that is associated with a particular location provider." *Id.*, 2:47-3:9.

248. Thus, Parupudi provides further disclosure regarding 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.

249. Accordingly, 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, and thus Parupudi in combination with Nykanen discloses Elements 21[pre] (to the extent it is limiting), 25[b], and 25[c].

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;

250. Parupudi in combination with Nykanen teaches Elements 1[b], 1[c], 21[b], and 25[c][i].

251. Parupudi discloses receiving, from a requesting entity, a request for context information related to a user of the mobile computing device.

252. 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.

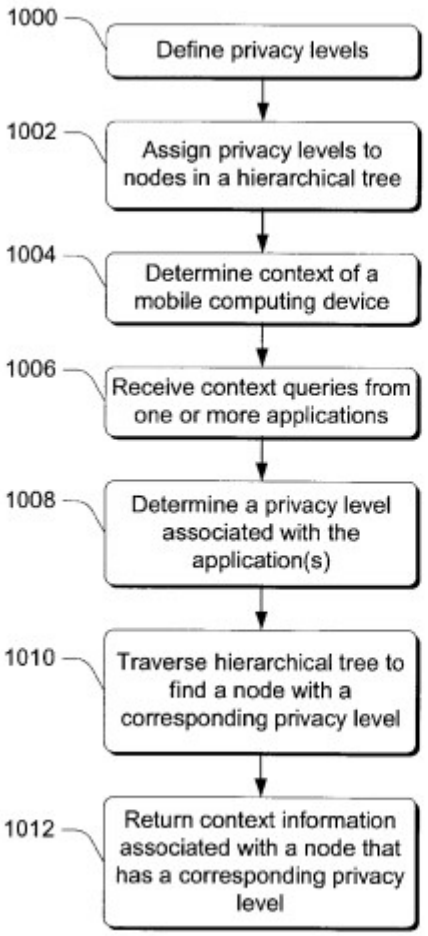

Fig. 10

253. Entities can make these requests for information "through one or more application program interfaces (APIs) and/or events," making "function calls on the API to query the location service module as to its current location," or "register[ing]

for a notification when the user changes their location." *Id.*, 23:36-24:7. The requested information may comprise "information that pertains to the device's current context or location." *Id*.

254. Accordingly, Parupudi discloses receiving, from a requesting entity, a request for context information related to a user of the mobile computing device.

255. 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.

256. 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. 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.

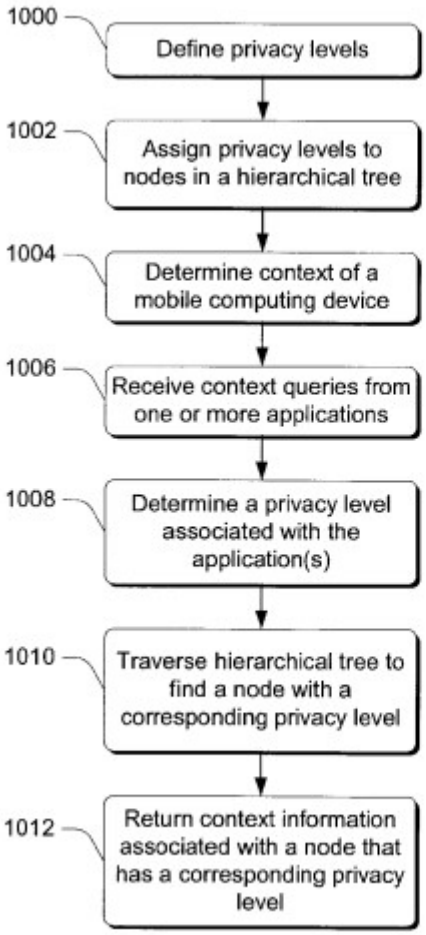

Fig. 10

257. 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.

258. 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.

259. Nykanen's Figure 1-a "shows an example prototypical ruleset which could be implemented in profile database." *Id.*, 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.*; *see also id.*, 3:48-4:4, 6:27-37.

260. 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.

261. 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. *See* Section VII. 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. *See* Section VII. 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. *See* Section

VII. 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. *See* Section VII.

262. Accordingly, Parupudi in combination with Nykanen teaches Elements 1[b], 1[c], 21[b], and 25[c][i].

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];

263. Parupudi in combination with Nykanen teaches Elements 1[d], 21[c], and 25[c][ii].

264. Specifically, 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.

265. 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.

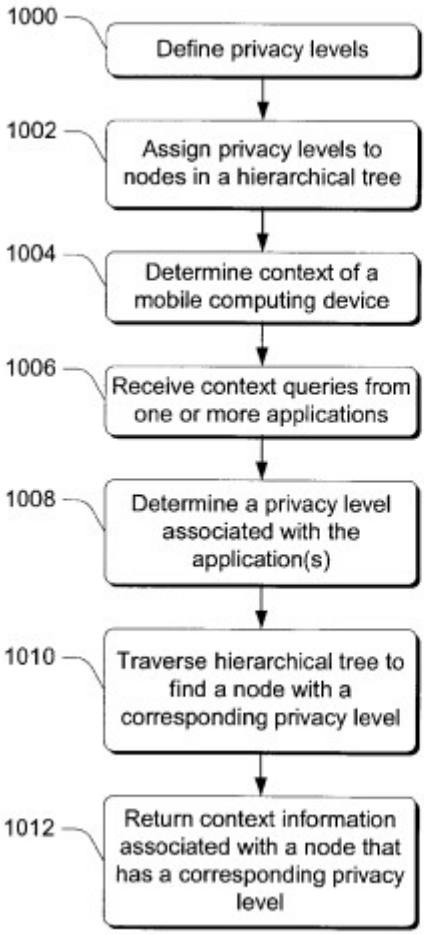

Fig. 10

266. 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.").

267. Or, for example, for "a web site that gives up to the minute weather of various locations…[the user] might assign…a privacy level of 60 so that [he] can receive weather information for the geographical area that corresponds to [his] present full postal code." *Id*., 25:27-37.

268. Accordingly, Parupudi discloses determining a level of specificity of a context characteristic.

269. 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.

270. 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").[12] *Id.*

[12] The '629 Patent discloses: "the context of the user may be defined by a plurality

271. 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.

---

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 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.)."), 6:15-24 ("The illustrative context data structure 300 also includes a context data 304 that defines three levels of specificity for the confidence characteristic of the location context parameter. The illustrative confidence characteristic includes a high granularity level indicating the user swiped his RFID tag at an entry door to a particular room, which provides a high degree of confidence that the user is actually within the room or at a GPS coordinate within the room. The illustrative confidence characteristic also includes a middle granularity level indicating that the user swiped his RFID inside at an entry door to a particular building at work, which provides a degree of confidence that the user is within that particular building. Additionally, the illustrative confidence characteristic includes a low confidence level indicating the user accessed a wireless access point that includes the building (but may include other buildings within the work campus area).").

272. 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. *See* Section VII. 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. *See* Section VII. 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. *See* Section VII. 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. *See* Section VII.

273. Accordingly, 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, and thus Parupudi in combination with Nykanen teaches Elements 1[d], 21[c], and 25[c][ii].

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

274. Parupudi in combination with Nykanen teaches Elements 1[e], 21[d], and 25[c][iii].

275. Specifically, 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.

276. 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.

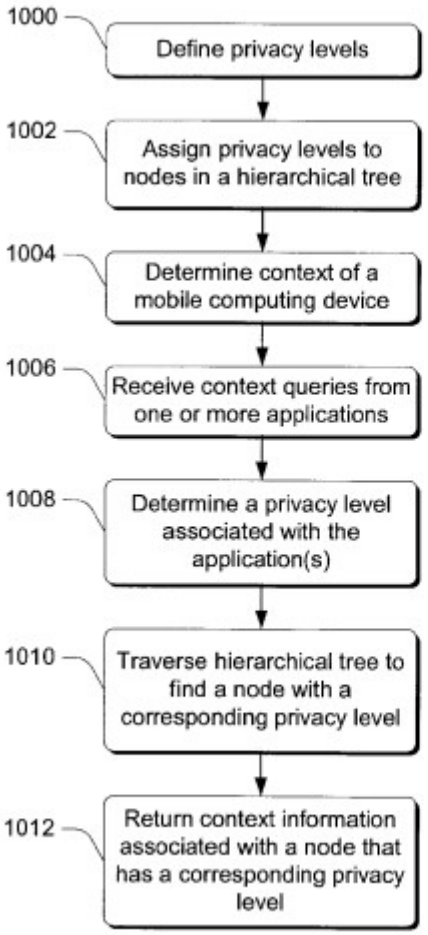

Fig. 10

277. 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").

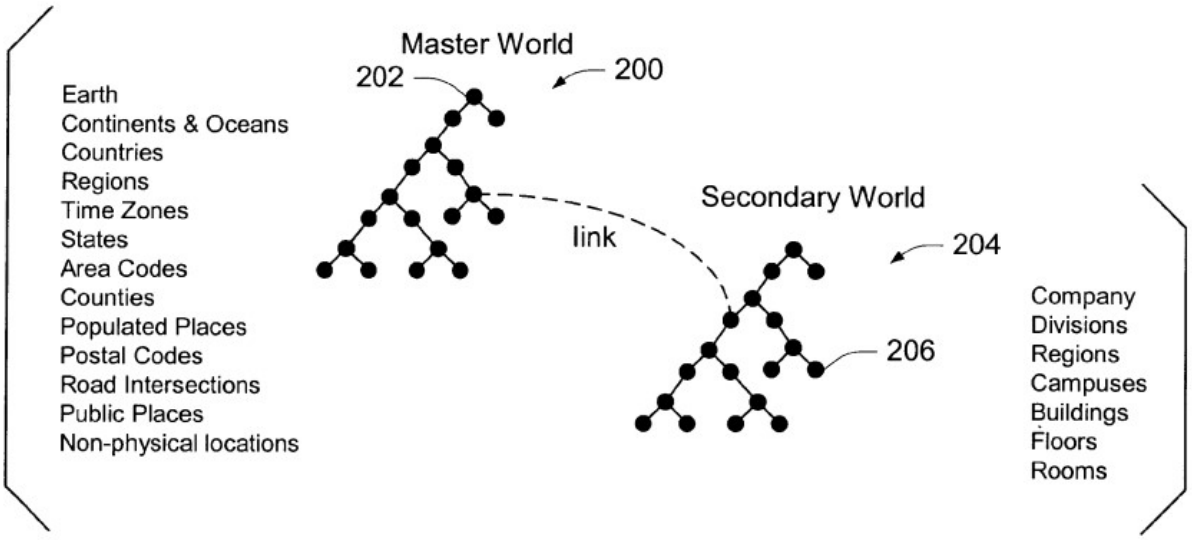
Master World
202
200
Earth
Continents & Oceans
Countries
Regions
Time Zones
States
Area Codes
Counties
Populated Places
Postal Codes
Road Intersections
Public Places
Non-physical locations
link
Secondary World
204
206
Company
Divisions
Regions
Campuses
Buildings
Floors
Rooms

Fig. 2

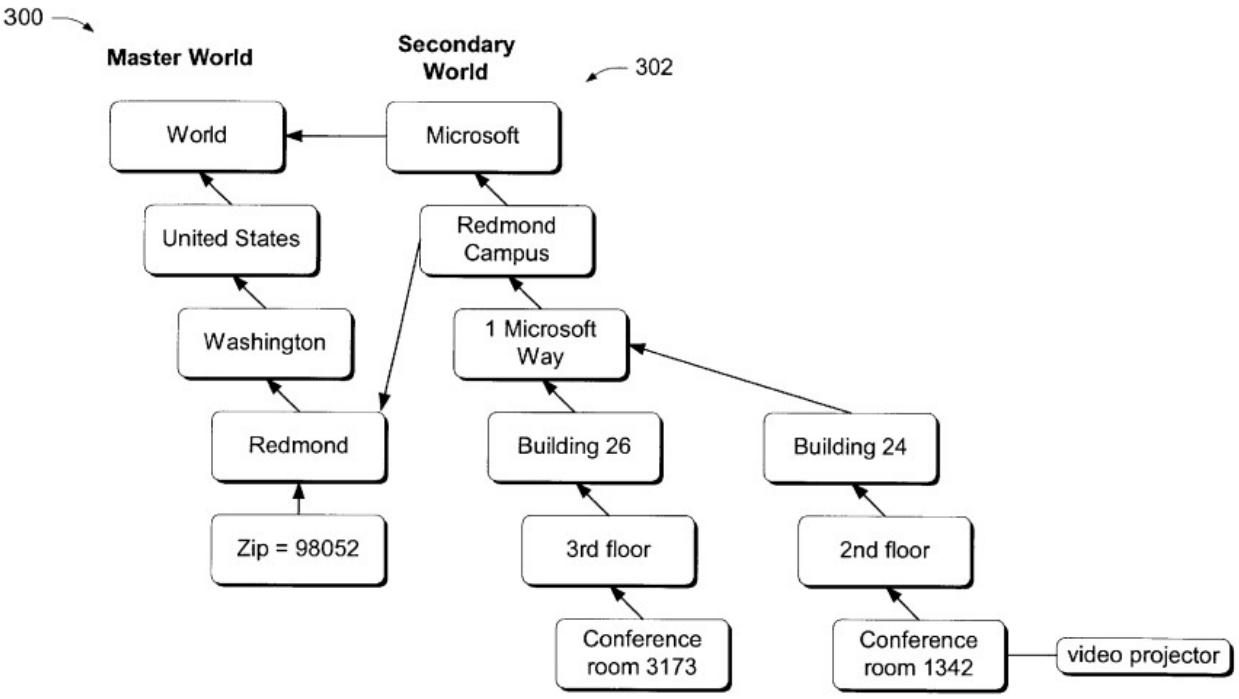
300
Master World
Secondary World
302
World
Microsoft
United States
Redmond Campus
Washington
1 Microsoft Way
Redmond
Building 26
Building 24
Zip = 98052
3rd floor
2nd floor
Conference room 3173
Conference room 1342
video projector

Fig. 3

278. For example, if a user were to access "Amazon.com's web site to buy a favorite book," Amazon would need to "compute the taxes that the user must pay" and "query device 602 to learn of the user's location." *Id*., 22:55-23:35. Thus, "the device might respond to the query by returning the state in which the user is making the purchase;" "[t]his functionality is made possible through the use of the Master World and one or more Secondary Worlds." *Id*.

279. Accordingly, Parupudi discloses retrieving appropriate context data.

280. 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.; see also id.*, 10:15-12:6. 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.

FIG.1A–1

RULE	RULE VARIABLES
AllowAllLocationRequests	ALLOWED ACCURACY (FULL; X METER RADIUS); NO
DisallowAllLocationRequests	YES; NO
AllowTheseRequestersDisallowAllOthers	NO; ARRAY LISTING ALLOWED REQUESTERS OR USE GROUPS AND ALLOWED ACCURACY (FULL; X METER RADIUS) FOR EACH
DisallowTheseRequestersAllowAllOthers	NO; ARRAY LISTING DISALLOWED REQUESTERS OR USE GROUPS, SPECIFICATION OF ALLOWED ACCURACY (FULL; X METER RADIUS) FOR "AllOthers"
AllowTheseRequestersQueryOnAllOthers	NO; ARRAY LISTING ALLOWED REQUESTERS OR USE GROUPS AND ALLOWED ACCURACY (FULL; X METER RADIUS) FOR EACH
DisallowTheseRequestersQueryOnAllOthers	NO; ARRAY LISTING DISALLOWED REQUESTERS OR USE GROUPS
QueryOnAllRequesters	YES; NO

281. "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.

282. 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.

283. 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. *See* Section VII. 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. *See* Section VII. 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. *See* Section VII. 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. *See* Section VII.

284. Accordingly, 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, and thus Parupudi in combination with Nykanen teaches Elements 1[e], 21[d], and 25[c][iii].

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

285. Parupudi in combination with Nykanen discloses Elements 1[f], 21[e], and 25[c][iv].

286. Specifically, Parupudi discloses responding to the request for context information with the retrieved context data.

287. 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"), Claim 10 ("return the selected device context information to the application from which the query was received"), Claim 14 ("information that is returned to the application as a function of the application's identity and a privacy level assigned hereto").

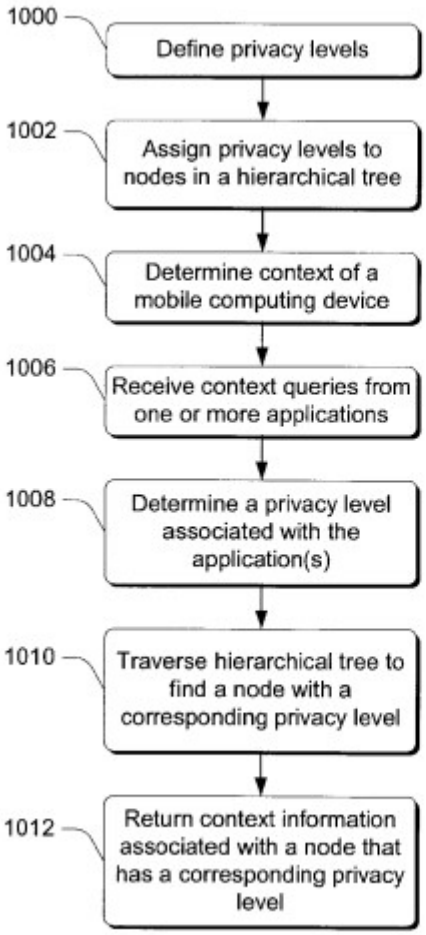

Fig. 10

288. Accordingly, Parupudi discloses responding to the request for context information with the retrieved context data, and Parupudi in combination with Nykanen discloses Elements 1[f], 21[e], and 25[c][iv].

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

289. Parupudi in combination with Nykanen teaches dependent Claim 3.

290. Specifically, Parupudi discloses establishing the context policy enforcement engine in software.

291. 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.

292. Moreover, Parupudi discloses its "privacy manager" as a "software module that is incorporated in the mobile computing device." *Id.*, 24:9-19. And, in service of the privacy manager, the device "executes software that traverses one or both of the tree structures to derive its context which, in this example, is the device's location." *Id*., 15:32-55.

293. Accordingly, Parupudi discloses establishing the context policy enforcement engine in software, and thus Parupudi in combination with Nykanen teaches dependent Claim 3.

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

294. Parupudi in combination with Nykanen teaches dependent Claim 4.

295. Specifically, Parupudi discloses receiving the request for context information from a software application.

296. 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.

297. For example, Parupudi's disclosed requesting applications may include "applications that can help [the user] find services, locate facilities (e.g. coffee shops, restaurants), give directions (e.g. how to get to [a] departure gate), update…on the status of [a] flight, and even check [the user] in automatically for [a] flight." *Id.*, 17:51-18:13.

298. Parupudi further provides the example of "Amazon.com's web site" as a software application that may request context information. *Id*., 22:54-23:32.

299. Accordingly, Parupudi discloses receiving the request for context information from a software application, and thus Parupudi in combination with Nykanen teaches dependent Claim 4.

5. Dependent 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"

300. Parupudi in combination with Nykanen teaches dependent Claim 5.

301. Specifically, Parupudi discloses receiving a request for a location of the user.

302. 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; *see also id.*, Figure 6 (depicting an identity-based context aware computing system).

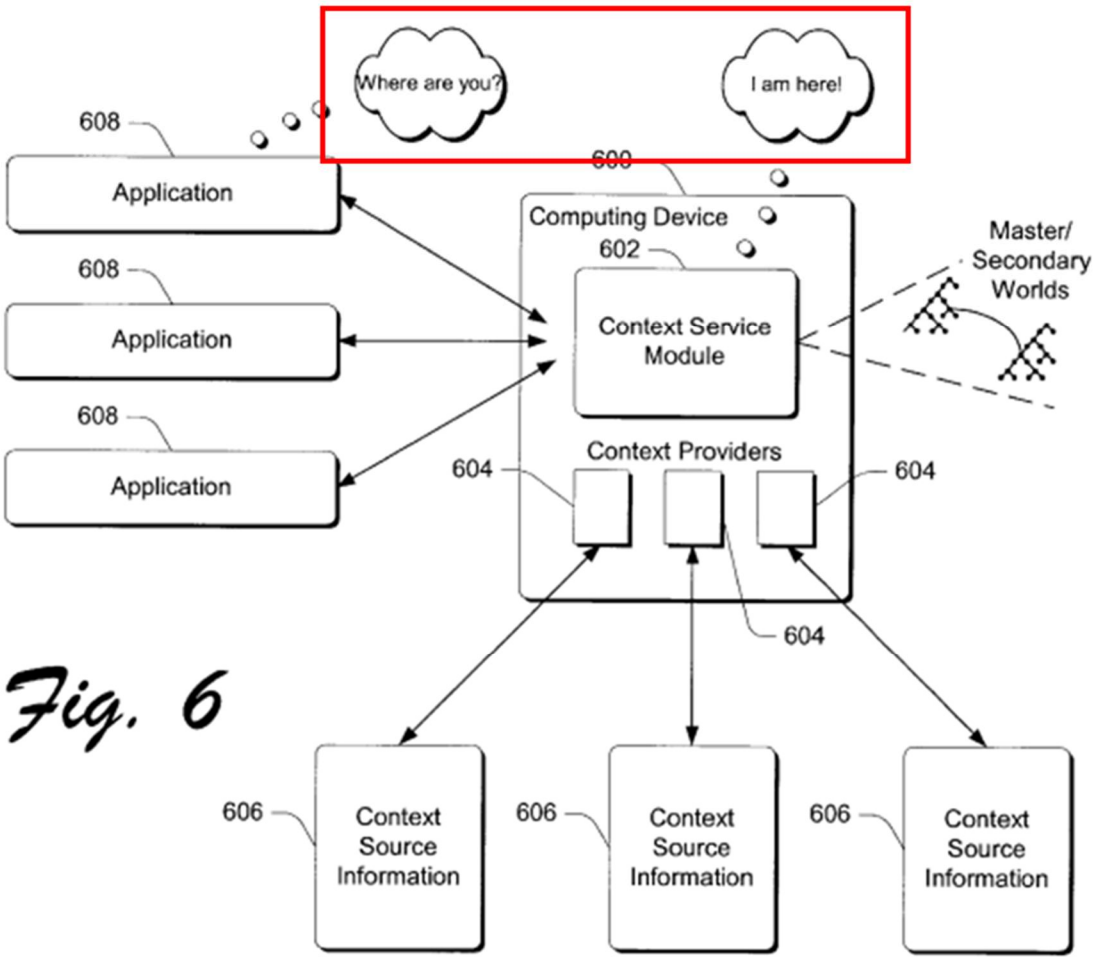

Fig. 6

303. Indeed, Parupudi discloses that entities can request "information that pertains to the device's current context or location" through a variety of requesting means, such as "through one or more application program interfaces (APIs) and/or events," making "function calls on the API to query the location service module as to its current location," or "register[ing] for a notification when the user changes their location." *Id.*, 23:36-24:7.

304. Accordingly, Parupudi discloses receiving a request for a location of the user, and thus Parupudi in combination with Nykanen teaches dependent Claim 5.

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

305. Parupudi in combination with Nykanen teaches dependent Claim 7.

306. Specifically, Parupudi discloses context policy data that defines a context policy rule based on the identification of the requesting entity.

307. 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.

308. For example, "a user may not want their specific location 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." *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.").

309. Accordingly, Parupudi discloses context policy data that defines a context policy rule based on the identification of the requesting entity, and thus Parupudi in combination with Nykanen teaches dependent Claim 7.

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

310. Parupudi in combination with Nykanen teaches dependent Claim 8.

311. Specifically, Parupudi discloses context policy data that defines a rule based on a predetermined group of requesting entities.

312. 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. "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.

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

313. Parupudi further discloses assigning privacy levels based on the level of specificity needed by the requesting entity, for example. Thus, for example, for "a web site that gives up to the minute weather of various locations…[the user] might assign…a privacy level of 60 so that [he] can receive weather information for the geographical area that corresponds to [his] present full postal code." *Id.*, 25:27-37

314. Accordingly, Parupudi discloses context policy data that defines a rule based on a predetermined group of requesting entities, and thus Parupudi in combination with Nykanen teaches dependent Claim 8.

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

315. Parupudi in combination with Nykanen teaches dependent Claims 13 and 22.

316. Specifically, Parupudi discloses determining context data based on the set of rules of the context policy data.

317. 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.").

318. For example, "if a untrusted application calls to request location information, the privacy manager…then traverses (step 1010) 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.*, 24:61-25:27.

319. Accordingly, Parupudi discloses determining context data based on the set of rules of the context policy data, and thus Parupudi in combination with Nykanen teaches dependent Claims 13 and 22.

9. Dependent 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"

320. Parupudi in combination with Nykanen teaches dependent Claims 14 and 23.

321. Specifically, Parupudi discloses 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.

322. 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. 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").

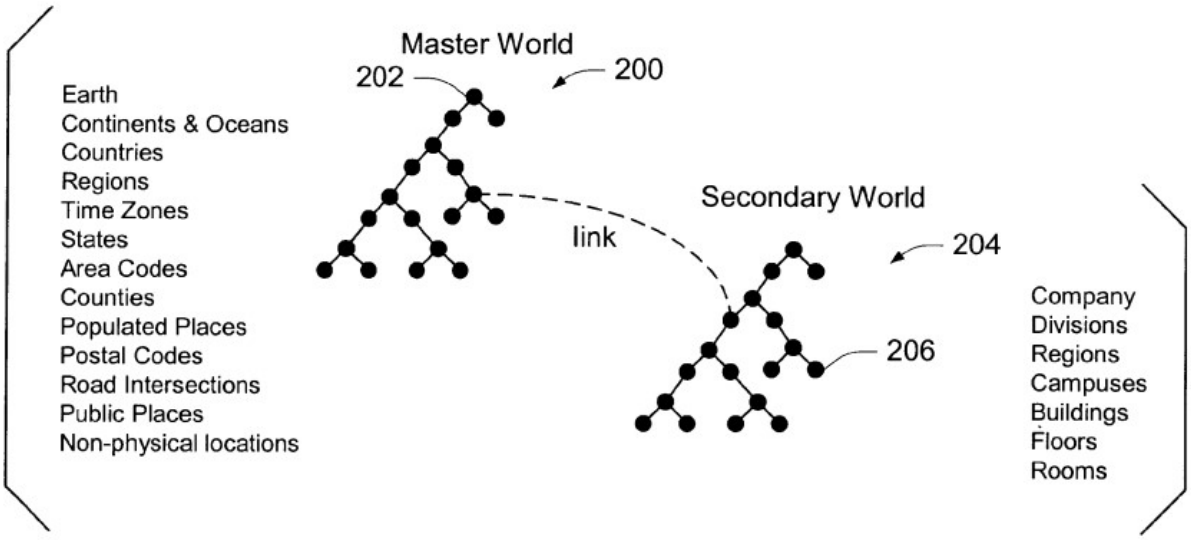

Fig. 2

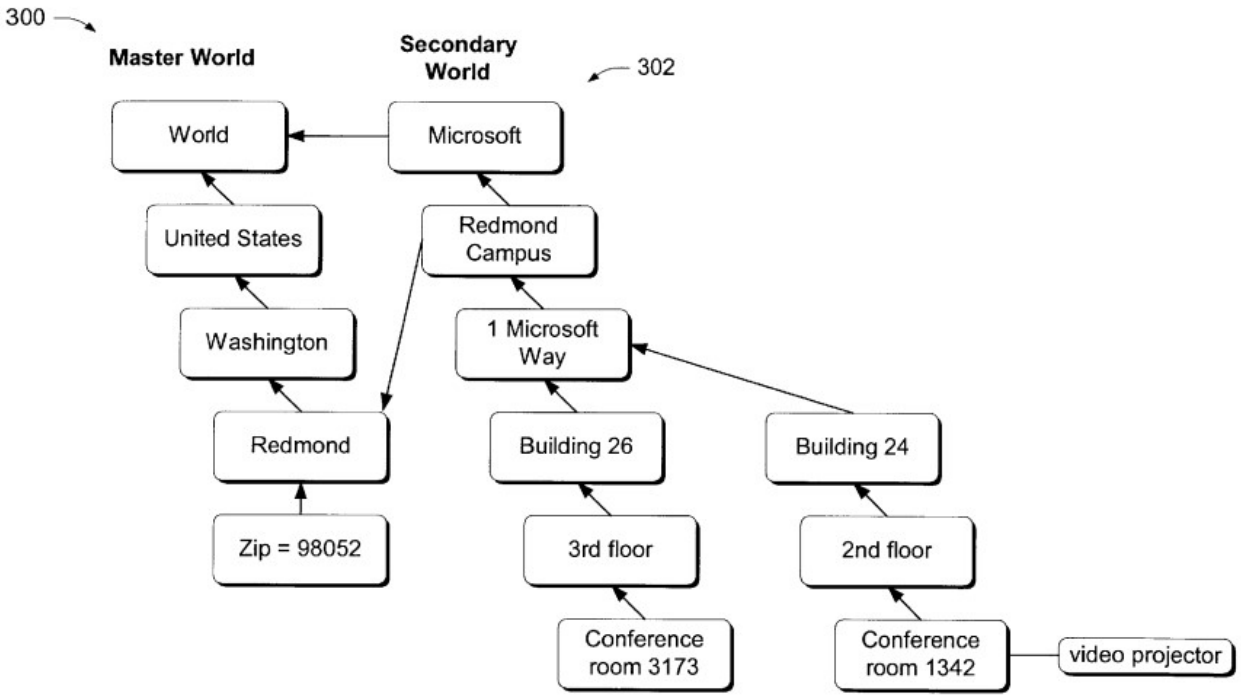

Fig. 3

323. For example, Parupudi discloses that if a user were to access "Amazon.com's web site to buy a favorite book," Amazon would need to "compute the taxes that the user must pay" and "query device 602 to learn of the user's location." *Id*., 22:55-23:35. Thus, "the device might respond to the query by returning the state in which the user is making the purchase." *Id.* Or, for example, for another purpose, such as "select[ing] an optimal shipping method (UPS or Express Mail)" for the user, a different context policy rule may apply and different context data may be retrieved. *Id*. "This functionality is made possible through the use of the Master World and one or more Secondary Worlds." *Id*.

324. Accordingly, Parupudi discloses 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, and thus Parupudi in combination with Nykanen teaches dependent Claims 14 and 23.

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

325. Parupudi in combination with Nykanen teaches dependent Claim 15.

326. Specifically, Parupudi discloses a method wherein responding to the request further comprises transmitting the context data.

327. Parupudi discloses with Figure 10 that its privacy manager, after determining the privacy level associated with the requesting entity, "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 requesting entity, 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; *see also id.*, Figure 6 (depicting an identity-based context aware computing system), 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"), Claim 10 ("return the selected device context information to the application from which the query was received"), Claim 14 ("information that is returned to the application as a function of the application's identity and a privacy level assigned hereto").

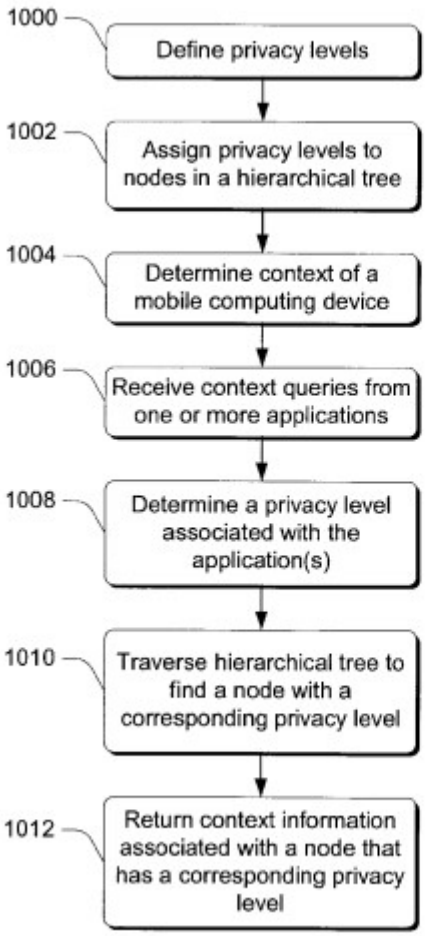

Fig. 10

328. Accordingly, Parupudi discloses a method wherein responding to the request further comprises transmitting the context data, and thus Parupudi in combination with Nykanen teaches dependent Claim 15.

11. Dependent 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"

329. Parupudi in combination with Nykanen teaches dependent Claims 16 and 24.

330. Specifically, Parupudi discloses 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.

331. Indeed, Parupudi discloses selecting user location information (i.e., the claimed "context parameter"), as the location information is available in numerous levels of specificity (e.g. "Planet/Continent," "State," "Room #") (i.e., the claimed "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"). *See* Ex-1006, 24:37-54.

332. More specifically, 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." *Id.*, 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."[13] *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").

[13] The '629 Patent discloses: "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." Ex-1001, 5:34-65. The '629 Patent also discloses: "The illustrative context data structure 300 also includes a context data 304 that defines three levels of specificity for the confidence characteristic of the location context parameter. The illustrative confidence characteristic includes a high granularity level indicating the user swiped his RFID tag at an entry door to a particular room, which provides a high degree of confidence that the user is actually within the room or at a GPS coordinate within the room. The illustrative confidence characteristic also includes a middle granularity level indicating that the user swiped his RFID inside at an entry door to a particular building at work, which provides a degree of confidence that the user is within that particular building. Additionally, the illustrative confidence characteristic includes a low confidence level indicating the user accessed a wireless access point that includes the building (but may include other buildings within the work campus area)." *Id.*, 6:15-24.

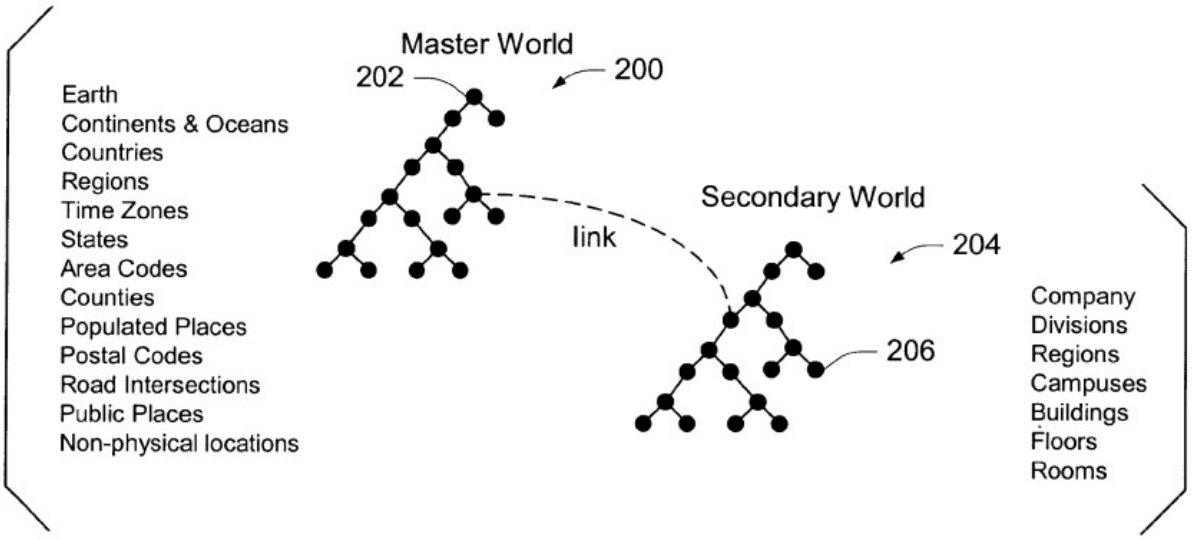
Master World
202
200
Earth
Continents & Oceans
Countries
Regions
Time Zones
States
Area Codes
Counties
Populated Places
Postal Codes
Road Intersections
Public Places
Non-physical locations
link
Secondary World
204
206
Company
Divisions
Regions
Campuses
Buildings
Floors
Rooms

Fig. 2

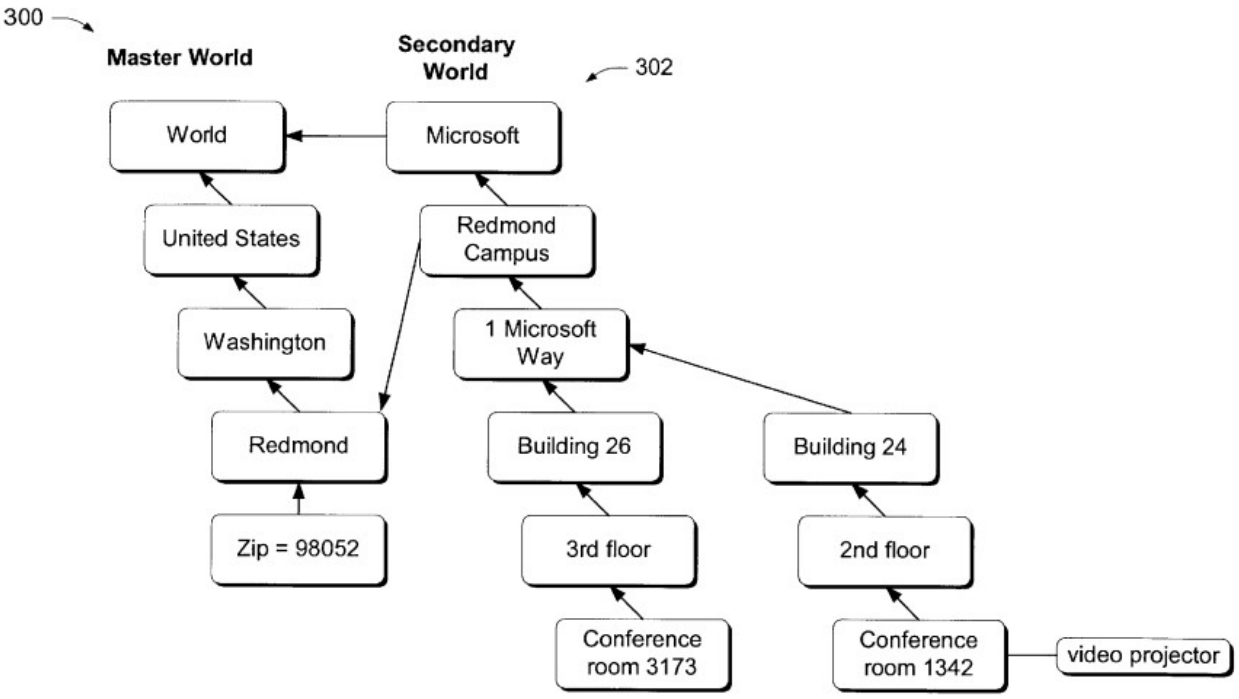
300
Master World
Secondary World
302
World
Microsoft
United States
Redmond Campus
Washington
1 Microsoft Way
Redmond
Building 26
Building 24
Zip = 98052
3rd floor
2nd floor
Conference room 3173
Conference room 1342
video projector

Fig. 3

333. Accordingly, Parupudi discloses 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, and thus Parupudi in combination with Nykanen teaches dependent Claims 16 and 24.

12. Dependent 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"

334. Parupudi in combination with Nykanen teaches dependent Claim 18.

335. Specifically, Parupudi discloses 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.

336. 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."[14] *Id.*; *see also id.*, Claim 1 ("assigning privacy levels to one or more applications that are configured to call a context service module on the computing device to obtain context information from the context service module"), Claim 34 ("The system of claim 34, wherein a privacy policy for an application can be selected by a user of the device."), Claim 10, Claim 14, Claim 20, Claim 25.

[14] The '629 Patent discloses: "The user interface 210 may be configured, for example, to allow the user to add, delete, update, or otherwise modify the context policy rules included in the context policy rule database. For example, the user may decide to allow access all applications in the 'public' group to location context data having high granularity. If so, the user may interact with the user interface to update the associated context policy rule. Additionally, the user may define which requesting applications or entities below to which group or otherwise define groups or associations of applications and entities with which various context policy rules may be created and defined." Ex-1001, 8:14-32.

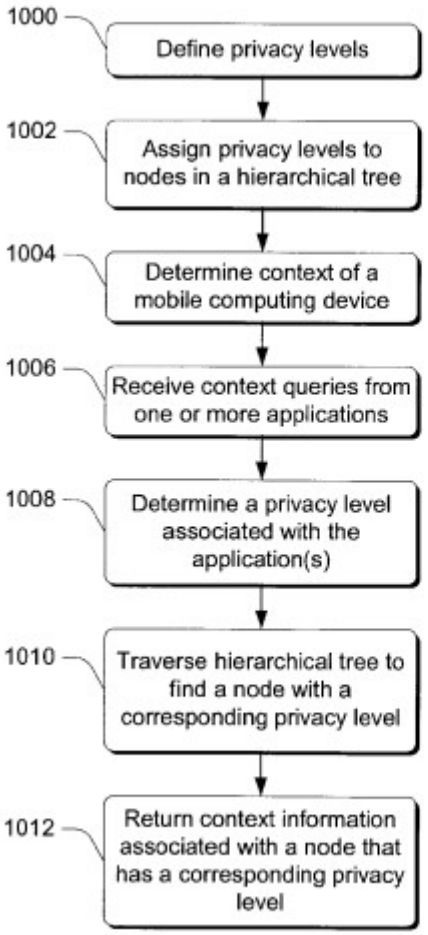

Fig. 10

337. Accordingly, Parupudi discloses 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, and thus Parupudi in combination with Nykanen teaches dependent Claim 18.

13. Dependent 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"

338. To the extent this claim can be understood (i.e., the claim recites "***the*** user-supplied context data," though the antecedent basis for "the user-supplied context data" is unclear), Parupudi in combination with Nykanen teaches dependent Claim 20.

339. Specifically, Parupudi discloses 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.

340. 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.").

341. Indeed, Parupudi discloses updating a context database stored on the mobile computing device with user-supplied context data. More specifically, Parupudi discloses embodiments in which "the user enters the zip code or city that the device is currently in." *Id.*, 13:14-13:47. In fact, "information can come to the computing device in any suitable way, e.g. a user can enter the information through a User Interface (UI) or the location might be broadcast to the computing device by another computing device (e.g. through the use of Bluetooth technology or Universal Plug and Play (UpnP)." *Id*., 15:31-54; *see also id*., 19:11-37 ("a location User Interface (UI) might provide location information in the form of a user entry that specifies a city, street or building").

342. Accordingly, Parupudi discloses 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, and thus Parupudi in combination with Nykanen teaches dependent Claim 20.

XI. CONCLUSION

343. It is my opinion that Claims 1, 3-5, 7-16, and 18-25 of the '629 Patent are invalid as obvious over the prior art I discussed above.

344. In signing this declaration, I recognize that it will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place in the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

345. I reserve the right to supplement my opinions in the future to respond to any arguments that the Patent Owner raises and to take into account new information as it becomes available to me.

346. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Respectfully Submitted,

Dr. Benjamin B. Bederson

Date: March 20, 2023