

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TV MANAGEMENT, INC., D/B/A GPS NORTH AMERICA,
Petitioner,

v.

PERDIEMCO LLC,
Patent Owner.

Case IPR2016-01278
Patent 9,071,931 B2

Before WILLIAM V. SAINDON, CARL M. DEFRANCO, and
AMBER L. HAGY, *Administrative Patent Judges*.

HAGY, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

PerdiemCo LLC (“Patent Owner”) is the owner of U.S. Patent No. 9,071,931 B2 (Ex. 1001, “the ’931 patent”). TV Management, Inc., d/b/a GPS North America (“Petitioner”)¹ requested an *inter partes* review of claims 1–7, 12–16, 20, and 22–26 of the ’931 patent. Paper 5 (“Pet.”). We instituted *inter partes* review of all of the challenged claims (Paper 22, “Inst. Dec.”) based on our determination that Petitioner had demonstrated a “reasonable likelihood” of prevailing on those claims. 35 U.S.C. § 314(a).

After institution, Patent Owner filed a Patent Owner Response (Paper 30, “PO Resp.”), and Petitioner followed with a Reply (Paper 36, “Pet. Reply”). With Board authorization, the parties each filed additional briefing limited to addressing evidence submitted by Patent Owner in support of alleged prior invention. Papers 41–43. Each party had an opportunity to present its case in a hearing conducted on September 12, 2017, a transcript of which is in the record. Paper 50 (“Tr.”).²

We have jurisdiction over these proceedings under 35 U.S.C. § 6. After considering the evidence and arguments of the parties, we determine that Petitioner has proved by a preponderance of the evidence that the subject matter of claims 1–7, 12–16, 20, and 22–26 of the ’931 patent is

¹ On August 15, 2016, prior to institution, petitioners Teletrac Inc. and Navman Wireless North America, Ltd., moved to terminate the proceedings with respect to themselves only. Paper 9. The Board granted that motion on August 31, 2016. Paper 11. After institution, petitioner Geotab Inc. and Patent Owner jointly moved to terminate the proceedings as to Geotab Inc. only, Paper 24, and the Board granted that motion on December 29, 2016, leaving as sole petitioner TV Management, Inc., d/b/a GPS North America. Paper 27.

² An oral hearing in related Cases IPR2016-01061 and IPR2016-01064 occurred on the same day, with similar issues presented and argued.

unpatentable. See 35 U.S.C. § 316(e). We issue this Final Written Decision pursuant to 35 U.S.C. § 318(a).

A. Related Matters

The '931 patent is part of a family of patents that share a common specification and claim priority through a continuation chain to U.S. Patent No. 7,525,425, which in turn claims priority to a provisional application filed on December 23, 2005. Other patents in this family include U.S. Patent Nos. 8,149,113; 8,223,012; 8,493,207; 8,717,166; 9,003,499; 9,119,033; 9,319,471; 9,485,314; 9,621,661; and 9,680,941.

In addition to *inter partes* review of the '931 patent, the Board has instituted the following *inter partes* reviews ("IPRs") directed to certain claims of the following patents within this patent family:

1. IPR2016-01061 (the '012 patent);
2. IPR2016-01062 (the '207 patent);
3. IPR2016-01063 (the '166 patent);
4. IPR2016-01064 (the '499 patent);
5. IPR2017-00968 (the '314 patent);
6. IPR2017-00969 (the '113 patent);
7. IPR2017-00973 (the '471 patent);
8. IPR2017-01007 (the '033 patent); and
9. IPR2017-01269 (the '661 patent).

Subsequent to institution, two of those IPRs were terminated in an adverse judgment in view of Patent Owner's disclaimer of all challenged claims. IPR2016-01062 (Paper 29); IPR2016-01063 (Paper 30). The Board has issued Final Written Decisions in IPR2016-01061 (Paper 50), and in IPR2016-01064 (Paper 49).

The '931 patent, along with the '207, '012, '166, and '499 patents, was asserted in the following cases in the Eastern District of Texas, all of which have been terminated: *PerdiemCo LLC v. Geotab Inc. et al*, Case No. 2:15-cv-00726; *PerdiemCo, LLC. v. Industrack LLC*, Case No. 2:15-cv-00727; *PerdiemCo, LLC. v. Omnivations II, LLC D/B/A Fleetronix*, Case No. 2:15-cv-00729; *PerdiemCo, LLC. v. Teletrac, Inc. et al*, Case No. 2:15-cv-00730; *Perdiem Co LLC v. GPS Logic, LLC*, Case No. 2:15-cv-01216; *PerdiemCo LLC v. TV Management, Inc. d/b/a GPS North America*, Case No. 2:15-cv-01217; *PerdiemCo, LLC. v. thingtech LLC*, Case No. 2:15-cv-01218; *PerdiemCo, LLC. v. LiveViewGPS, Inc.*, Case No. 2:15-cv-01219.

The '931 patent, along with the '012, '499, '471, '113, '033, and '314 patents, is currently the subject of a co-pending lawsuit in the Eastern District of Texas, which was filed after institution of the present proceeding and after termination of the above-referenced cases: *PerdiemCo LLC v. Telular Corp. et al.*, 2-16-cv-01408. That district court case is currently stayed pending resolution of this IPR proceeding and the related IPR proceedings.

B. The '931 Patent (Ex. 1001)

The '931 patent relates to a location-tracking system for conveying information about the location of an object, such as a person, vehicle, or package, to a group of users. Ex. 1001, 1:8–12, 1:61–2:7. The group of users may include a family, a group of friends, or employees of a company. *Id.* at 5:27–33, 13:10–29. According to the '931 patent, various technologies, such as Global Positioning System (“GPS”) technology, may be used to track the location of the object. *Id.* at 6:9–18, Fig. 1. An object may be tracked relative to “user-defined zones.” *Id.* at 1:62–2:8, 5:7–26.

The system also monitors “events,” which are, for example, instances when a tracked object enters or exits a zone. *Id.*

In one exemplary scenario, a mother can track the location of an object (her daughter’s car) by equipping it with a tracking beacon and assigning it an identification code. *Id.* at 9:12–56. The mother may then use that identification code to set up “events” so that when her daughter’s car enters or leaves a pre-defined “zone,” the mother will receive an “alert” (such as an email). *Id.* The mother may also have the location of her daughter’s tracked car conveyed to one or more other specified users, such as another parent or a guardian, by assigning them identification codes and associating a particular level of access with each user’s identification code. *Id.* at 10:30–54.

Administrative functions may be performed within a group as, for example, a “family can set up its own information-sharing environment.” *Id.* at 5:62–65. Various levels of administrator privileges may exist. *Id.* at 5:51–54. In addition to associating identification codes with each user, the administrator can associate a level of access with the user, and thereby limit who receives the location information. *Id.* at 2:45–3:3, 5:39–54, 6:64–7:60.

C. Challenged Claims

Petitioner challenges claims 1–7, 12–16, 20, and 22–26, of which claim 1 is independent. Challenged claim 1 is reproduced below.³

1. [a] A location tracking system comprising:
 - [b] one or more servers capable of communicating with a plurality of mobile devices, each mobile device is associated with an identification (ID) and at least one location

³ For expediency, Petitioner and Patent Owner break claim 1 into limitations 1(a)–1(n). We adopt that format herein for ease of reference.

information source that provides location information for the mobile device;

[c] the one or more servers configured to:

[d] define first level administrative privileges to protect privacy of a group of multiple mobile devices;

[e] define second level administrative privileges to control conveyance of information regarding the group;

[f] check the first level administrative privileges before adding a mobile device to the group;

[g] provide one or more interfaces for setting a zone, an event, and an alert for the group;

[h] receive a request to set a zone for the group, the zone having a boundary that is independent of where the group's mobile devices are located;

[i] receive a request to set an event for the group;

[j] receive a request to set an alert for the group, the request identifying a recipient of the alert;

[k] check the second level administrative privileges before setting a zone, an event, or an alert for the group;

[l] store the group's zone, event and alert in one or more databases;

[m] receive IDs and location information for the multiple mobile devices in the group;

[n] compare the IDs and location information with the group's zone and event to determine whether to send the group's alert; and

cause the group's alert to be sent.

D. Instituted Grounds

We instituted *inter partes* review based on the following three references:

- (1) Fast, U.S. Patent No. 7,327,258 B2, filed January 31, 2005, and issued February 5, 2008 (“Fast”) (Ex. 1003);
- (2) Phillips, U.S. Patent No. 7,848,765 B2, filed May 27, 2005, and issued Dec. 7, 2010 (“Phillips”) (Ex. 1007); and
- (3) Zou, Pub. No. US 2005/0156715 A1, filed January 16, 2004, and published July 21, 2005 (“Zou”) (Ex. 1005).

The grounds on which we instituted review are as follows:

Reference(s)	Basis	Claims Challenged
Fast and Phillips (“Ground 1”)	§ 103	1–7, 12–16, 20, and 22–26
Fast (“Ground 2”)	§ 102(e)	1–7, 12–16, 20, and 22–26
Fast, Zou, and Phillips (“Ground 3”)	§ 103	1–7, 12–16, 20, and 22–26

Inst. Dec. 30.

II. ANALYSIS

Petitioner bears the burden of proving unpatentability of the challenged claims, and that burden never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail, Petitioner must establish the facts supporting its challenge by a preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

A. Claim Construction

In the Institution Decision, we concluded that no express construction of any of the claim terms was necessary for us to assess the reasonable

likelihood threshold for *inter partes* review. Inst. Dec. 11. Neither party challenged this conclusion in post-Institution briefing or argument.

Having considered the full record, we again conclude that no express construction of any of the claim terms is necessary for us to render a final written decision. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011) (noting that “claim terms need only be construed ‘to the extent necessary to resolve the controversy’”) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

B. Description of the Asserted Prior Art

Petitioner asserts that the subject matter of one or more of claims 1–7, 12–16, 20, and 22–26 is obvious in view of Fast and Phillips (“Ground 1”); is anticipated by Fast (“Ground 2”); and is obvious in view of Fast, Phillips, and Zou (“Ground 3”). Pet. 6–7. We provide an overview of each of these references before turning to the individual grounds.

1. Fast

Petitioner asserts that Fast, which was filed on January 31, 2005, and issued on February 5, 2008, is prior art under 35 U.S.C. § 102(e) (Pet. 5), and Patent Owner does not dispute that contention.

Fast describes a system for monitoring various parameters (such as speed, position, and threshold boundaries) of mobile items attached to tracking devices called “beacons.” Ex. 1003, Abstract, 1:61–63. Beacons communicate, *inter alia*, geographic location information to remote monitoring stations and/or devices through a server. *Id.* at 4:9–11, 8:38–9:9. Beacons may be “carried or worn by a person or attached to an object.” *Id.* at 9:31–32.

As an exemplary embodiment, Fast describes the Guardian Mobile Monitoring System (GMMS). Ex. 1003, Fig. 23, 2:63–67, 3:9–35. According to Fast, the GMMS is a hierarchical system with multiple levels of users, including wholesalers, retailers, and subscribers. *Id.* at 18:25–37. These multiple levels are depicted in Figure 22 of Fast, reproduced below:

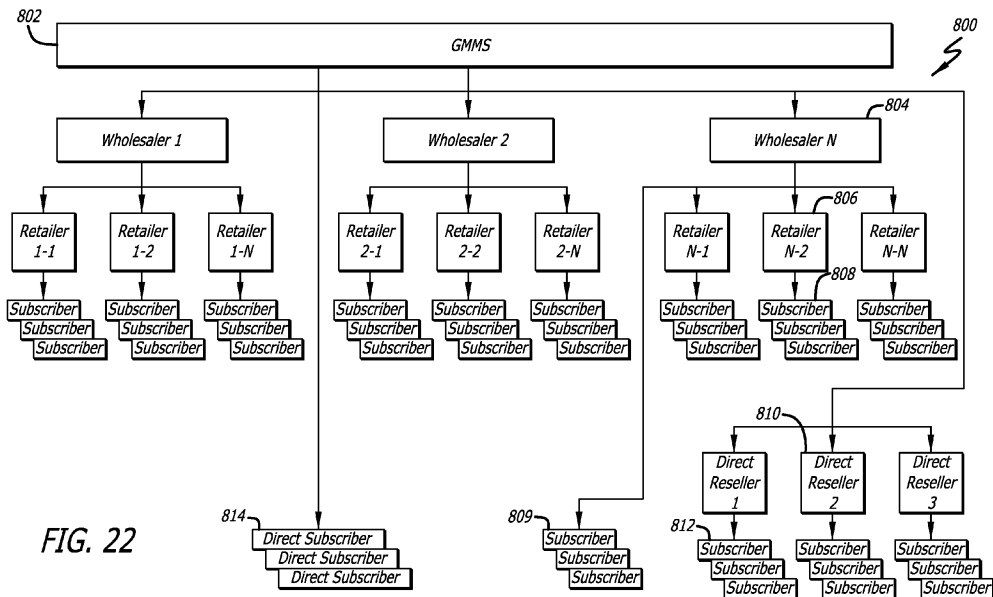


Figure 22 of Fast, reproduced above, is a schematic diagram showing the interrelationship between the GMMS, individual wholesalers, individual retailers, and individual subscribers in monitoring mobile items. Ex. 1003, 2:58–62. The GMMS refers to the overall system, within which wholesalers work with operators to provide wholesale and retail mobile monitoring services to subscribers. *Id.* at 16:13–17.

A subscriber may purchase multiple beacons to track multiple items using GMMS, such as individuals (e.g., members of a family) or objects (e.g., vehicles). Ex. 1003, 24:56–65, 33:1–17. The subscriber may create zones, such as “allowed or disallowed zones,” to allow monitoring of the tracked items in particular areas, which may be activated or deactivated

according to a schedule. *Id.* at 20:63–67. Subscribers may set up the GMMS software to automatically notify them upon certain conditions, such as a beacon reaching a specified location. *Id.* at 12:40–44.

According to Fast, the GMMS allows users to create various levels of access privileges. For example, a wholesaler may include an administrator, which has the highest level of access with unrestricted access to the wholesaler’s functions. Ex. 1003, 38:26–45. Each wholesaler may have its own portal, accessible through the Internet, with access restricted to users that are authorized by system administrators. *Id.* at 16:5–11, 37:44–38:54, Figs. 14-1, 14-2. Each wholesaler may provide monitoring services to multiple subscriber accounts. *Id.* at Fig. 22, 16:29–30.

Also according to Fast, each subscriber account in GMMS may be given access to a dedicated portal with a user ID and password required to log in. Ex. 1003, 6:21–23, 42:14–35, Figs. 16-1 and 16-2. The subscriber is offered “preference settings” for designating other users, such as other subscribers or guardians, with various levels of access privileges. *Id.* The subscriber may be considered to have the highest level of access within that portal, and has authority to manage other users, including the authority to add, update, and delete system users. *Id.* at Fig. 16-2. For example, a subscriber may designate a “guardian” to have temporary or permanent responsibility for an item—such as a “babysitter” designated to oversee a tracked child. *Id.* at 4:61–62, 39:6–12, 43:1–11. In adding users, the subscriber may indicate whether other users are restricted from using any functionality of the portal. *Id.* at 42:32–35, 42:48–52; Ex. 1010 ¶ 48.

A subscriber may purchase multiple beacons for tracking multiple items using GMMS, such as individuals (e.g., members of a family) or

objects (e.g., vehicles). Ex. 1003, 24:56–65, 33:1–17. Zones may be created, such as “allowed or disallowed zones,” to provide monitoring of the tracked items in particular areas, which may be activated or deactivated according to a schedule. *Id.* at 20:63–67, 35:9–36:41.

The GMMS software may be set up to send automatic notifications upon certain conditions, such as a beacon reaching a specified location. Ex. 1003, 12:40–44. In particular, using the GMMS subscriber portal, a subscriber (or other authorized user, such as a guardian if not restricted from this functionality by the subscriber) may build and manage “scenarios” to trigger alerts relating to tracked items. *Id.* at Fig. 16-1 (subscriber portal), Figs. 11-1 and 11-2 (Scenario Manager), 32:15–56, 35:8–36:41. Fast describes a “scenario” as “[a] set of monitoring parameters where events are monitored automatically according to a schedule,” and when a specified parameter “exceeds a specified threshold,” while the scenario is active, “specified notifications are automatically sent by the GMMS.” *Id.* at 5:42–45. For example, according to Fast, a scenario could be built to send a specified message to specified people if a certain tracked vehicle travels outside of a specified zone. *Id.* at 32:53–56; *see also id.* at 35:7–36:41.

One aspect of building a scenario within Fast’s “Scenario Manager” is the selection of a “notification scheme.” *See* Ex. 1003, Fig. 11-1 (boxes 272, 276, and 278). According to Fast, a notification scheme identifies a selected group of entities (*e.g.*, guardians, the subscriber herself, and/or other specified entities) who are notified when a scenario is triggered. *Id.* at 35:46–53; *see also id.* at 36:34–39. Fast explains that:

[t]he ultimate function of the Scenario Manager is to allow users to command the GMMS system to automatically monitor mobile events. An example would be “If the specified vehicle

is outside of the specified zone, at the specified time, send the specified message, to the specified people/places, using the specified communications methods.”

Id. at 32:51–56. Also according to Fast, “[n]otification schemes are named and saved for use in any number of scenarios.” *Id.* at 34:36–37.

2. Phillips

Petitioner asserts that Phillips is prior art under 35 U.S.C. § 102(e). Pet. 5. As discussed below, Patent Owner disputes whether Phillips is prior art to the ’931 patent. PO Resp. 29–30 and Ex. 2009.

Phillips discloses “location-based services” for tracking mobile devices, providing geofences, and providing location-based alerts. Ex. 1007, Abstract; 1:23–25. Phillips discloses that a portable electronic facility (“PEF”) sends location information to a server, and this location information may be used by the server in both a geofence application and an alert application. *Id.* at 2:12–18, 4:11–22, 8:42–53, 8:64–67, 9:53–67. The PEF may be, for example, a mobile phone or a mobile device equipped with GPS. *Id.* at 1:34–43. Phillips discloses an application server that provides an “application based service” to PEF users via a web interface, such as a web browser. *Id.* at 6:63–7:3. The application server may “host a geospatial application” to provide geo-coding, mapping, and routing functionality. *Id.* at 9:37–39. The server may also host an “alert application” that may, in response to the occurrence of an event, “transmit the alert to a user.” *Id.* at 9:54–57.

3. Zou

Petitioner contends Zou is prior art under 35 U.S.C. § 102(e) and is a printed publication under 35 U.S.C. § 102(a). Pet. 6. Patent Owner does not dispute these contentions.

Zou describes a fleet manager using mobile GPS tracking devices referred to as “telemetry devices.” Ex. 1005 ¶ 9. Each telemetry device is assigned to a tracked object, *id.* ¶ 12, communicating with a Network Operations Center (“NOC”), *id.* ¶ 9; *see also id.* at Fig. 3. A user of the system communicates with the NOC over a network such as the Internet. *Id.* at Fig. 3. A user’s desktop client interfaces to the NOC through a presentation server. *Id.* ¶ 113, Fig. 3. The presentation server provides functions including fleet and asset tracking and “general purpose I/O monitoring and control.” *Id.* ¶ 111. The server also maintains a database “for user accounts and other related data (e.g., configuration data, user management information, device management, and data acquired from the devices **103**).” *Id.* Zou’s user interfaces “manage and control user administration.” *Id.* ¶ 9.

Zou describes an “exemplary system” that “includes a GeoFence Violation Report.” Ex. 1005 ¶ 171. According to Zou, “[t]his report will detail each time a vehicle entered or exited a GeoFence set for that vehicle. It will also report the date, time, speed, direction, and location of the vehicle when the GeoFence was violated.” *Id.* Zou also describes how users may “organize the exemplary system to meet specific needs. Options here allow the user to group vehicles into fleets, edit system user authority levels, and customize the way telemetry devices record and transmit data.” *Id.* ¶ 189. Within a given fleet, a manager can select specific permissions for authorizing users to view fleets, build alert templates, and manage other users. *Id.* ¶¶ 191–193, 202, 203, Figs. 18a and 18e.

*C. Ground # 3: Obviousness of Claims 1–7, 12–16, 20, and 22–26
in View of Fast, Phillips, and Zou*

For the reasons expressed below, having considered the full record, we are not persuaded by Petitioner’s arguments of unpatentability on Ground 1 (obviousness over Fast and Phillips) or Ground 2 (anticipation by Fast), but we are persuaded on Ground 3 (obviousness over Fast, Phillips, and Zou). We address Ground 3 first, and then provide our analysis and reasoning on Grounds 1 and 2.

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person of ordinary skill in the art at the time the invention was made. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). Obviousness is resolved based on underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

In Ground 3, Petitioner challenges claims 1–7, 12–16, 20, and 22–26 as unpatentable in view of Fast combined with Phillips and Zou. Pet. 19–54 (arguing claims over combination of Fast and Phillips); Pet. 56–63 (arguing claims over the combination of Fast, Phillips, and Zou, building on earlier arguments). For the reasons discussed below, we are persuaded that Petitioner has demonstrated by a preponderance of the evidence, including annotated figures, a detailed claim analysis, and expert testimony, that the challenged claims would have been obvious in view of Fast, Phillips, and Zou.

Patent Owner raises several points of contention with Petitioner's combination of Fast, Phillips, and Zou: (1) "Phillips is not prior art" (PO Resp. 29–30); (2) the combination of Fast, Phillips, and Zou does not teach at least the server-based threshold monitoring limitation and the "group" elements "that are recited throughout '931 claim 1" (PO Resp. 16–26, 29–32); (4) a skilled artisan would not have had reason to combine Fast and Zou as argued by Petitioner (PO Resp. 31–32); and (5) "the secondary consideration of licensing amply rebuts the obviousness case" (PO Resp. 32–34). We address each of these contentions below.

1. Phillips as Prior Art Under 35 U.S.C. § 102(e)

a. Parties' Arguments

Before addressing the combination of Fast, Phillips, and Zou, we consider Patent Owner's argument that "Phillips is not prior art." PO Resp. 29–30. In particular, Patent Owner asserts that the inventor named on the '931 patent, Darrell Diem, "conceived of the '931 claims before Phillips' priority date of May 27, 2005." *Id.* at 29. In support of this assertion, Patent Owner presents a declaration from Mr. Diem, which includes Exhibits A–I. *See Ex. 2009.*

Petitioner challenges Mr. Diem's declaration as an improper incorporation by reference, noting that Patent Owner does not present argument in its Patent Owner Response but instead refers wholesale to Mr. Diem's declaration. Pet. Reply 12. Petitioner also challenges Mr. Diem's declaration on several substantive bases.⁴ *Id.* at 12–14.

⁴ Prior to the oral hearing, Petitioner also objected to certain pages of Patent Owner's demonstrative exhibits on the basis that those pages contained arguments outside of Patent Owner's briefing. Paper 49. This objection was overruled at the oral hearing and the slides were allowed, with the comment

Shortly after Petitioner filed its Reply, the parties sent an email to the Board, in which Patent Owner requested authorization to file a sur-reply to address Petitioner's alleged new allegations concerning Mr. Diem's conception of the invention disclosed in the '931 patent. In the same email, Petitioner requested authorization to file a motion to strike Patent Owner's conception argument for improper incorporation by reference under 37 C.F.R. § 42.6(a)(3). In an Order issued July 26, 2017, the Board authorized Patent Owner to file a sur-reply and also authorized Petitioner to file a sur-sur-reply. Paper 41, 5. The Board denied Petitioner's request to file a motion to strike. *Id.* at 6. Patent Owner's sur-reply was filed August 2, 2017 (Paper 42 ("PO Sur-reply")), and Petitioner's sur-sur-reply was filed August 7, 2017 (Paper 43 ("Pet. Sur-sur-reply")).

In his declaration, Mr. Diem states that he "had written much of the computer code" for his proposed system by "late 2004." Ex. 2009 ¶ 6. As support for that assertion, Mr. Diem provides Exhibits A, C, and E–G to his declaration, which he characterizes as "computer code" or "source code" files that he states were last modified in December 2004. *Id.* ¶¶ 6, 8, 10, 11. Mr. Diem also provides Exhibit B, which he characterizes as a "manual" that was "last modified on December 30, 2004 (*id.* ¶ 7), and Exhibit D, which he characterizes as "a brochure" that he "created to advertise [his] system" and which he says was "last modified on February 2, 2005" (*id.* ¶ 9).

Mr. Diem additionally provides Exhibit H to support his assertion of a specific date by which he had completed his conception. *Id.* ¶ 12. Mr. Diem characterizes Exhibit H as "a screenshot" showing his "registration of the

from the panel that the Board would rely only on what is in the briefing.
Tr. 4:20–5:2.

website name ‘perdiemco.com’ on May 13, 2005.” *Id.* According to his declaration, Mr. Diem did not register for this website until he had “fully conceived all elements” of his “location-tracking system.” *Id.*

Mr. Diem also states that he “continued to implement and commercialize [his] system throughout 2005.” *Id.* ¶ 13. As support for that assertion, Mr. Diem provides Exhibit I to his declaration, which he characterizes as “two screenshots with directory listings for project files on [his] system,” wherein the screenshots purportedly show “53 different files modified during that interval,” and that “at least one file has a last-modified date in every month from June 2005 to December 2005.” *Id.*

In challenging Mr. Diem’s declaration, Petitioner argues, *inter alia*: (1) Mr. Diem fails to provide corroborating evidence of alleged prior conception of *every limitation* of the ’931 patent claims (Pet. Reply 12–14); and (2) Patent Owner has not shown reasonable diligence from the alleged date of conception until reduction to practice (*id.* at 14).

b. Legal Standards for Antedating Prior Art Reference

Whether Phillips is prior art to the ’931 patent under 35 U.S.C. § 102(e) depends on whether the effective filing date of the Phillips patent (May 27, 2005) pre-dates the invention of the ’931 patent. *See* 35 U.S.C. § 102(e)(2)⁵: “A person shall be entitled to a patent unless . . . (e) the invention was described in . . . (2) a patent granted on an application for patent by another filed in the United States *before the invention by the applicant for patent*” (emphasis added).

⁵ Section 3(b) of the Leahy-Smith America Invents Act altered the § 102 conditions for patentability; novelty. Pub. L. No. 112-29, 125 Stat. 284, 285–287 (2011). Because the ’931 patent has a filing date before September 16, 2012 (effective date), we refer to the pre-AIA § 102(e) in this Decision.

Patent Owner bears the burden of producing evidence showing Mr. Diem's prior invention. *See Dynamic Drinkware, LLC v. National Graphics, Inc.*, 800 F.3d 1375, 1378–80 (Fed. Cir. 2015) (noting that the patent owner had the burden of going forward with evidence that the prior art did not anticipate). The ultimate burden of persuasion in an *inter partes* review, however, remains on the petitioner to prove unpatentability by a preponderance of the evidence and that burden never shifts to the patent owner. 35 U.S.C. § 316(e); *see also Dynamic Drinkware*, 800 F.3d at 1378.

To remove Phillips as a prior art reference, Patent Owner must produce evidence showing either (1) a conception and reduction to practice before the filing date of Phillips; or (2) a conception before the filing date of the Phillips patent combined with reasonably continuous diligence up to reduction to practice after that date. *See Taurus IP, LLC v. DaimlerChrysler Corp.*, 726 F.3d 1306, 1323 (Fed. Cir. 2013); *see also Perfect Surgical Techniques, Inc. v. Olympus America, Inc.*, 841 F.3d 1004, 1008 (Fed. Cir. 2016). Under either approach, Patent Owner must produce evidence showing that Mr. Diem's conception occurred prior to May 27, 2005 (the effective date of the Phillips reference). *See Taurus*, 726 F.3d at 1323.

Priority of invention and its constituent issues of conception and reduction to practice “are questions of law predicated on subsidiary factual findings.” *Singh v. Brake*, 317 F.3d 1334, 1340 (Fed. Cir. 2003). Conception is “the formation, in the mind of the inventor of a definite and permanent idea of the complete and operative invention, as it is thereafter to be applied in practice.” *Coleman v. Dines*, 754 F.2d 353, 359 (Fed. Cir. 1985) (citing *Gunter v. Stream*, 573 F.2d 77, 80 (CCPA 1978)) (emphasis omitted). This requires more than accidental creation; there must be

evidence that the inventor appreciated that he made “something new.” *Invitrogen Corp. v. Clontech Labs., Inc.*, 429 F.3d 1052, 1063–64 (Fed. Cir. 2005). The conception analysis “necessarily turns on the inventor’s ability to describe his invention with particularity. Until he can do so, he cannot prove possession of the complete mental picture of the invention.” *Burroughs Wellcome Co. v. Barr Labs., Inc.*, 40 F.3d 1223, 1228 (Fed. Cir. 1994).

Proof of conception cannot turn on the inventor’s testimony alone, but must include “corroborating evidence which shows that the inventor disclosed to others his ‘completed thought expressed in such clear terms as to enable those skilled in the art’ to make the invention.” *Coleman*, 754 F.2d at 359 (citing *Field v. Knowles*, 183 F.2d 593, 601 (CCPA 1950)); *see also Mahurkar v. C.R. Bard, Inc.*, 79 F.3d 1572, 1577 (Fed. Cir. 1996) (noting that corroboration requirement “arose out of a concern that inventors testifying in patent infringement cases would be tempted to remember facts favorable to their case by the lure of protecting their patent or defeating another’s patent”) (citations omitted). The sufficiency of corroboration is determined according to a “rule of reason.” *Price v. Symsek*, 988 F.2d 1187, 1195 (Fed. Cir. 1993) (citation omitted). This, however, does not dispense with the requirement that some independent evidence must provide corroboration. *Coleman*, 754 F.2d at 360; *see also In re NTP, Inc.*, 654 F.3d 1279, 1291–92 (Fed. Cir. 2011) (noting requirement of evidence corroborating inventor testimony).

c. Analysis

We conclude that Patent Owner has not come forward with sufficient evidence of alleged prior invention to remove Phillips as a prior art reference. First, Patent Owner’s evidence does not show that Mr. Diem conceived of

every element of the invention recited in the '931 patent by the critical date. Mr. Diem does not provide a claim chart or an element-by-element discussion of any claim of the '931 patent as compared to his evidence of alleged corroboration, but instead provides a general discussion of several portions of source code for his “proposed system” that he avers he had written as of December 2004. Ex. 2009 ¶¶ 6, 8, 10, 11. That general discussion fails, for example, to address the tiered levels of “administrative privilege,” as recited in claim 1 of the '931 patent—specifically, the “first” and “second” level administrative privileges. In describing the functionality purportedly depicted in Exhibits A, C, and E–G, Mr. Diem does not mention administrative privileges at all, but asserts that these exhibits demonstrate that his system employed a server to “store location data” (Exhibits B, D, and D) and to “store data regarding zones created by users” (Exhibits A and D), and also that the “server would control access with codes” (Exhibits B, D, and D). Ex. 2009 ¶ 11. Mr. Diem does not point to anything in the submitted portions of source code, or otherwise, to corroborate a pre-filing date conception of a server that “defines” and “checks” administrative privileges, as claimed.

In its sur-reply, Patent Owner argues that Mr. Diem cites “source code files” stating how functions are “controlled by ‘access codes.’” PO Sur-reply 2 (citing Ex. 2009 ¶¶ 6, 11). Patent Owner then argues “[t]hese access codes comprise the claimed first and second level of administrative privileges.” *Id.* Patent Owner’s argument is not itself evidence nor does it bridge the gap between an “access code,” not recited in the claims, and the two distinct levels of “administrative privileges,” as claimed. Contrary to Patent Owner’s argument, the '931 patent does not equate access codes with

“administrative privileges.” Rather, the ’931 patent specification describes “access codes” by stating that they “can be associated with information to manage the conveyance of the information to computing devices”; that is, “information is conveyed to those computing devices that are associated with the users having access to the information as specified by the access code.” Ex. 1001, 7:37–60. The ’931 patent specification separately describes administrative privileges as including privileges “to configure [an] information-sharing environment.” *Id.* at 5:39–41. Thus, the ’931 patent specification describes a system that uses tiered administrative privileges *and* access codes, confirming that they are not one and the same. Accordingly, Patent Owner has not demonstrated that the proffered evidence allegedly corroborating Mr. Diem’s pre-filing-date conception of “access codes,” not recited in the claims, also corroborates his conception of the tiered “first” and “second” level administrative privileges, as recited in the claims.

Mr. Diem’s declaration also does not provide evidence of a pre-filing-date conception of the ’931 patent claim limitations relating to a “group.” Although Mr. Diem identifies a “group” variable in the portion of source code purportedly shown in Exhibit A (*see* Ex. 2009 ¶ 6), Mr. Diem does not point to anything to corroborate his pre-filing-date conception of a server configured to “receive a request to set” a “zone,” an “event,” or an “alert” “*for the group*,” as required by claim 1. Notably, when challenging Petitioner’s unpatentability arguments, Patent Owner states that “[t]he ‘group’ recited by claim 1 of the ’931 Patent must be associated with a single unified event and a single unified alert.” PO Resp. 12. Patent Owner thus argues that setting a zone/event for a *device in a group* is not the same as

setting a zone/event for the *actual group*. But nothing in Mr. Diem's declaration or proffered portions of source code, including the "group" variable purportedly depicted in Exhibit A, shows a data structure or code that unifies an event and an alert under a group.

Patent Owner's purported corroborating evidence also raises evidentiary concerns. With regard to the "registration page" for the PerdiemCo website (Ex. 2009, Ex. H), which Mr. Diem relies upon to "refresh[]" his "recollection" that he had "fully conceived all elements" of his system by the date of that registration on May 13, 2005 (*id.* ¶ 13), Patent Owner's reliance on that evidence is circular. The registration page itself bears no description of any claimed invention, and any tie to Mr. Diem's conception of his invention is based only on his uncorroborated word. On this record, the registration page provides no independent corroboration of any act of conception. *See NTP*, 654 F.3d at 1293 (rejecting "circular logic" of using files to corroborate inventor testimony and using inventor testimony to corroborate the same files).

Not only has Patent Owner not met its burden of production to show prior conception of every element of Mr. Diem's claimed invention, but Patent Owner has not come forward with evidence to show reasonable diligence from the alleged date of conception (May 13, 2005) until at least a constructive reduction to practice (e.g., the filing date of the ancestor provisional application (December 23, 2005)). *See Teva Pharm. Indus. Ltd. v. AstraZeneca Pharms. LP*, 661 F.3d 1378, 1383 (Fed. Cir. 2011). Mr. Diem never states that he was "diligent" following his conception in reducing his system to practice; rather, Mr. Diem states that he "continued to work to implement and commercialize [his] system throughout 2005." Ex.

2009 ¶ 13. As support for that assertion, Mr. Diem relies on Exhibit I to his declaration, which he characterizes as screenshots of directory listings showing over 50 files that, according to Mr. Diem, were last modified between June 2005 and December 2005. *Id.* Mr. Diem states “these files corroborate my own recollection, which is that I worked *regularly to implement and commercialize my system* throughout 2005.” *Id.* (emphasis added).

Although Mr. Diem relies on the existence and dates of those “files” for corroboration of his continuing work on his system, neither Mr. Diem nor Patent Owner provides any evidence of what was contained in those files or when they were created. And, without more, a mere directory listing of files each bearing an obscure name and a “[d]ate modified” between June and December 2005 provides scant evidence of what work was done and when (to any degree), and thus does not support a finding of diligence. Moreover, many of the files listed in Exhibit I show a “[d]ate created” of May 28, 2005, or *later*—in fact, many of them are identified in Exhibit I as having been “created” on March 16, 2017. Mr. Diem’s declaration does not explain the latter discrepancy. Assuming these files to be material components of Mr. Diem’s system, as Mr. Diem’s declaration at least implicitly posits, this evidence undermines Patent Owner’s argument of conception prior to the critical date of May 27, 2005. In addition, neither Mr. Diem nor Patent Owner provide any evidence of the timing of Mr. Diem’s work toward preparing and filing his patent application or his diligence in engaging such activities. *See* Tr. 122:1–125:5. Although assumptions could be made in that regard, as Patent Owner’s counsel argued at the oral hearing (*see id.* at 122:1–14), no such evidence is before us.

Thus, Patent Owner’s “evidence” of alleged diligence is vague and equivocal at best, and we do not afford it substantial weight.

Accordingly, having considered fully the arguments and evidence provided by the parties, we are not persuaded that Patent Owner has come forward with sufficient evidence of conception or diligence to satisfy its burden of production that the ’931 claimed invention pre-dates Phillips.

2. Obviousness Analysis: Ground 3—Fast, Phillips, and Zou
a. Level of Ordinary Skill in the Art

According to Petitioner’s expert witness, Dr. Heppe, a person of ordinary skill in the art would, at the time of filing, have had a “Bachelor’s degree in Electrical Engineering and/or Computer Science with one or two years of experience in related fields such as (depending on the focus of the undergraduate degree) electronics, computer science, positioning technologies such as GPS, and radio communications.” Ex. 1011 ¶ 13. Dr. Heppe further opines that “[m]ore education could substitute for work experience, and more work experience could substitute (to a degree) for education.” *Id.*

The expert witness proffered by Patent Owner, Dr. Schonfeld, provides a similar description, stating that a person of ordinary skill at the time of filing would have had

- (a) a bachelor’s degree in electrical engineering, computer engineering, or computer science, or a closely related field, and at least two years of work or research experience in the field of information systems, including data networking or database management, or (b) a master’s degree in electrical engineering, computer engineering, or computer science, or a closely related field, and at least one year of work or research experience in that same field.

Ex. 2010 ¶ 16.

Based on Dr. Heppe's credible testimony, we find that a person of ordinary skill in the art would have met Dr. Heppe's description. We further find that Dr. Schonfeld's testimony on this issue does not differ materially from that of Dr. Heppe, and, in any event, our analysis in this Decision would be unchanged if we were to apply Dr. Schonfeld's description.

*b. Scope and Content of the Prior Art /
Differences Between Claimed Invention and the Prior Art*

We generally summarize the parties' arguments and evidence before turning to the parties' disputes.

(1) Petitioner's Arguments and Evidence

(a) Independent Claim 1

Stated generally, claim 1 of the '931 patent contemplates a tracking system in which one or more servers communicate with a group of mobile devices and associated location information sources, and in which the server defines at least two levels of administrative privilege to control conveyance of information privately to the group. Claim 1 further requires that the server provide an interface for allowing, with proper administrative privilege, a zone (having a boundary), an event, and an alert to be set for a group, which are stored in one or more databases. Claim 1 also requires the alert to specify a recipient of the alert, which will be sent by the server based on a comparison of IDs and location information for the mobile devices in the group with the group's zone and event.

In challenging claim 1 as unpatentable over the combination of Fast, Phillips, and Zou, Petitioner points to Fast's description of the Guardian Mobile Monitoring System (GMMS), in which servers communicate with a plurality of mobile devices (e.g., handsets / beacons) and in which each mobile device is associated with an identification (e.g., unique beacon ID

associated with a handset) and at least one location information source (e.g., a GPS receiver). Pet. 19–20 (citing Ex. 1003, 9:12–16, 9:55–60, 10:22–25, 27:2–5, 44:20–22; Ex. 1011 (Heppe Decl.) ¶¶ 78–80). With regard to the disputed “server” limitation, Petitioner points in particular to Phillips’ disclosure of a system in which portable electronic facilities, including mobile devices, contain a location information source (such as GPS), are associated with a unique identification (such as a phone number, where the PEF is a mobile phone), and communicate with an application server. Pet. 20 (citing Ex. 1007, 1:34–43, 10:47–50, 11:51–52; Ex. 1011 ¶¶ 81–82). Petitioner also relies on the Zou reference in particular with regard to the disputed “group” features of claim 1, asserting Zou “describes more detailed user interfaces in the context of implementing geofencing in fleet management.” Pet. 56 (citing Ex. 1005 ¶ 78 and Figs. 15g, 17a, 18b, 18c).

We now turn to Petitioner’s arguments and evidence regarding particular limitations of claim 1.

Limitations 1(a)–(c): servers and mobile devices

Petitioner asserts Fast, Phillips, and Zou each disclose application servers in communication with devices to be tracked. Pet. 21, 57. With regard to the claimed “mobile devices,” Petitioner argues Fast discloses “beacons,” which include “handset mobile devices.” *Id.* at 19–20 (citing Ex. 1003, 9:55–60); *see also* Ex. 1003, 9:10–11. Fast also discloses each beacon has a “Beacon ID,” which Petitioner argues is a unique ID used to communicate with the GMMS through the beacon controller interface. *Id.* at 20 (citing Ex. 1003, 44:20–22, 27:2–5; Ex 1011 ¶ 80). The beacons provide location information using, for example, GPS. *Id.* (citing Ex. 1003, 9:12–16, 10:22–25). Petitioner similarly argues that Phillips discloses “mobile

devices” as “portable electronic facilities” (“PEFs”), which each have “unique identification” and which may each contain a location information source such as GPS or an RFID. *Id.* at 20 (citing Ex. 1007, 1:34–43, 10:47–50, 11:51–52; Ex. 1011 ¶¶ 81–82). In addition, Zou’s mobile devices, according to Petitioner, are “telemetry devices that are installed on tracked vehicles,” which “have GPS modules and may have an associated name or a vehicle ID.” *Id.* at 57 (citing Ex. 1005 ¶¶ 9, 78–79, 95).

Petitioner also asserts that Fast discloses the servers recited in limitations 1(a), (b), and (c) by disclosing “one or more application servers” and describing embodiments “where these operations are performed on these servers, such as threshold monitoring in tracking mode by a beacon manager . . . or determining whether an event falls within a schedule.” Pet. 21 (citing Ex. 1003, Fig. 2, 27:45–58, 36:25–33; Ex. 1011 ¶¶ 41, 62). Petitioner also combines Fast’s teachings with Phillips, asserting Fast describes “embodiments where operations are performed in a beacon,” and further asserting “it would be obvious to a POSITA to perform the services performed on the beacons on the application server from Phillips instead.” *Id.* (citing Ex. 1011 ¶ 84). Petitioner also asserts “Phillips discloses an application server in communication with the PEF that hosts a geofencing application.” *Id.* (citing Ex. 1007, 9:53–63; Fig. 8, box 108). Petitioner further asserts Zou discloses one or more servers (such as the Network Operations Center) that enables communications with telemetry devices installed on tracked vehicles in support of fleet management. *Id.* at 57–58 (citing Ex. 1005 ¶¶ 9–10, 77–79, 204 and Figs. 1, 15g).

Limitations 1(d) and 1(e): first and second level administrative privileges

Limitations 1(d) and (e) recite that a server defines first and second level administrative privileges, wherein the first level is to “protect privacy of a group of mobile devices,” and the second level is to “control conveyance of information regarding the group.” Petitioner asserts Fast teaches these tiered administrative privileges by disclosing wholesalers and subscribers, which have separate access portals, wherein privacy of mobile devices is protected by requiring user names and passwords to gain access to the different portals (such as for each individual subscriber account) and by storing the data for each account securely in a database. Pet. 21–22 (citing Ex. 1003, Figs. 14-1, 14-2, 6:13–15, 6:21–23, 15:62–16:3; Ex. 1011 ¶¶ 86, 96–101). In particular, Petitioner asserts the first-level administrative privilege (limitation 1(d)) is taught by Fast because Fast’s wholesaler may create subscriber accounts. *Id.* at 22 (citing Ex. 1003, 38:46–54). Petitioner further asserts Fast also teaches a second-level administrative privilege (limitation 1(e)) because Fast’s subscriber has administrative privileges to create users (such as guardians) and “assign them access privileges to the one or more beacons (which may be assigned to dependents).” *Id.* at 24 (citing Ex. 1003, 20:42–62, 43:1–11).

Petitioner also argues an alternative mapping of Fast’s disclosure to the claimed administrative privileges, asserting that Fast’s subscriber may exercise a first-level administrative privilege by adding users and devices to the subscriber account. *See* Pet. 36 (citing Ex. 1003, 42:14–52 and Fig. 16, box 532). Under that mapping, Petitioner also asserts that an authorized user (such as a guardian) may exercise the claimed second-level administrative

privilege by creating and implementing scenarios to set zones, events, and alerts for an assigned group of beacons. *See id.*

Petitioner points to similar teachings in Phillips, in which access to location information may be “password protected” in a first level of administrative privilege (Pet 23 (citing Ex. 1007, 20:47–51, 20:54–56); *see also id.* at 26–27), and a “second level of administrative privilege” exists for select users to create geofences, which convey geofence alerts (*id.* at 25 (citing Ex. 1007, 9:15–27; Ex. 1011 ¶ 113); *see also id.* at 28–29, 31).

Petitioner also argues Zou discloses a server that “defines a first level administrative privilege through a user’s ability to add and edit fleets.” Pet. 58 (citing Ex. 1005 ¶ 192; Ex. 1011 ¶¶ 105–106). Petitioner also argues “Zou teaches ‘grouping’ of vehicles as fleets so that users can ‘view data by fleet, control data collection parameters by fleet, and compare performance between fleets.’” *Id.* (citing Ex. 1005 ¶¶ 190–192; Ex. 1011 ¶¶ 105–106). According to Petitioner, Zou’s users may also select other users to “view the fleet group” and are enabled “to set authority levels for the users who can view the fleet group.” *Id.* (citing Ex. 1005 ¶¶ 190–192). Petitioner asserts that “[t]hese privileges . . . protect the privacy of a fleet, i.e. a group of mobile telemetry devices, because not every user can view a fleet group, which protects the location information of the tracked vehicles.” *Id.* With regard to the second-level administrative privilege, Petitioner argues Zou discloses privileges for controlling the conveyance of information, such as through automatic alerts, wherein “[u]sers with appropriate permissions may create additional users and assign them to fleets, thus effectively using their permissions to ‘control conveyance of information’ regarding the customer’s fleets.” *Id.* at 58–59 (citing Ex. 1005 ¶¶ 79, 111–115, 189–195, and Figs.

18a, 18b, and 18e (e.g., the second user may have permissions to “view account configuration,” “edit account configuration,” “view users account permissions,” and “edit users account permissions”)).

Petitioner’s arguments regarding the teachings of Fast, Phillips, and Zou with regard to the “group” features of claim 1 are discussed in more detail below in connection with our analysis of the parties’ disputes.

Limitations 1(f) and 1(g): check first administrative privileges / user interface

With regard to limitations 1(f) and (g), Petitioner argues that “Fast discloses that the first administrative privileges are checked (*e.g.*, user name and password authentication) before adding a mobile device to a group (*e.g.*, assigning a beacon to a subscriber account, or assigning a beacon to an item in an item group).” Pet. 25. In particular, Fast discloses both wholesalers and subscribers must authenticate themselves to the system with a user ID and password before they can use their respective portals to add users or devices to “subscriber accounts (*e.g.*, groups).” *Id.* at 25–26; *see also* Ex. 1003, 38:26–54, 40:37–39, Fig. 14 (wholesaler); *id.* at 6:21–23, 20:42–62, 42:14–35, Figs. 11-1, 16-1, and 16-2 (subscriber); *id.* at 33:1–17 (assigning beacons). As we noted above, Petitioner argues the privilege to add devices in Fast is a “first level administrative privilege” as claimed. Pet. 21–22. Petitioner further argues that Fast’s wholesaler and subscriber portals are user interfaces for setting zones, events, and alerts for the group, as recited in limitation 1(g). *Id.* at 27 (citing Ex. 1003, 20:63–67, 21:5–7, 32:15–56, 28:10–13; Ex. 1011 ¶ 128).

Petitioner also argues Phillips teaches limitations 1(f) and 1(g) by disclosing “requiring a password to access the system such as a PIN or authentication code,” before a user may access the “user interface to add

phones to a geofence.” Pet. 26–27 (citing Ex. 1007, 2:25–27, 20:54–56 and Fig. 32; Ex. 1011 ¶¶ 123–124).

Petitioner similarly argues Zou teaches limitations 1(f) and 1(g) by teaching that a user must use a “User ID and password” to access the system, and also that each user has a “user profile” that is “checked prior to geofence functionality such as creating geofences for one or a group of vehicles, and assignment of a vehicle to a geofence.” Pet. 59 (citing Ex. 1005 ¶¶ 192–193, 205–206; Ex. 1011 ¶¶ 126–127). Petitioner further argues “Zou shows an example of a graphic user interface (GUI) for creating a zone, an event, and an alert at FIG. 20a for a fleet [of] multiple vehicles.” *Id.* at 59–60 (citing Ex. 1005 ¶¶ 91, 105, 203–211 and Fig. 15d (disable/Modify/Remove geofence), Figs. 20a and 20b).

As noted, Petitioner’s arguments regarding the teachings of Fast, Phillips, and Zou with regard to the “group” features of claim 1 are discussed in more detail below in connection with our analysis of the parties’ disputes.

Limitations 1(h)–(j): set zones, events, and alerts for the group

Petitioner argues that the combination of Fast, Phillips, and Zou discloses limitations 1(h)–1(j), which generally recite that the server receives a request to set a zone, an event, and an alert for the group. Pet. 60–61; *see also id.* at 30–35 (discussing combination of Fast and Phillips). With regard to Fast, Petitioner argues Fast discloses these limitations by describing a “Subscriber Administration Module” containing a “Zone Manager,” a “Notification Manager,” and a “Scenario Manager.” Pet. 27–28 (citing Ex. 1003, 20:63–67, 21:5–7, 42:14–16, 42:39–41, Fig. 16-2); *id.* at 30–35. Petitioner asserts Fast’s Zone Manager allows a subscriber to set zones for

one or more dependents, and the Notification Manager includes the functionality of creating and sending an alert to the group of mobile devices. *Id.* at 28. Petitioner also asserts Fast’s “Scenario Manager” allows a subscriber to create a software event monitoring system for a group of mobile devices. *Id.* at 24 (citing Ex. 1003, 32:15–56). For each scenario, a user may use a “notification scheme” to assign a list of “suitable entities” to be notified upon occurrence of an event. *Id.* (citing Ex. 1003, 35:47–51).

Further with regard to setting zones, Petitioner argues that, according to Fast, a subscriber may create zones, such as “allowed or disallowed zones,” to monitor the location of the tracked individual or object. Pet. 27–28 (citing Ex. 1003, 20:63–67); *see also id.* at 30–31. Petitioner additionally argues that Fast in combination with Phillips discloses a server (such as an application server) that may “receive a request to set a zone for the group,” wherein the boundary of the zone “is independent of where the group’s mobile devices are located” as recited in limitation 1(h). *Id.* at 30 (citing Ex. 1003, Fig. 2 and Ex. 1011 ¶¶ 133, 135, 138 (Fast); Ex. 1007, 9:53–63 (geofencing application on server), 14:22–27, 14:38–40 (geofence boundaries), 18:12–17 and Fig. 32 (boundaries with alerts applied to groups), and Ex. 1011 ¶¶ 140–141 (Phillips server receives requests)). Petitioner’s arguments regarding the teachings of Fast and Phillips with regard to setting zones “for the group,” which is a key point of contention between the parties, are discussed in more detail below.

Petitioner makes similar arguments regarding disclosure by Fast and Phillips of a server that receives requests for setting events. Pet. 32–35. In particular, Petitioner argues Fast discloses two ways to set an event: (1) threshold monitoring in tracking mode (Pet. 32 (citing Ex. 1011 ¶¶ 136–

138, 146, 147; Ex. 1003, 23:63–66, 29:60–66, 30:3–6)); and (2) a request through the Scenario Manager (*id.* at 33 (citing Ex. 1011 ¶ 146; Ex. 1003, 32:16–19, 32:51–56, 33:22–23 (Scenario Manager), 33:33–36 (setting geofence violations), 35:24–28 and Fig. 11 (trigger mechanism activating notification scheme), 33:3–6 (saving scenario to database))). Petitioner also argues Phillips discloses that an alert application in the application server allows an “event” to be “designated by the user as an alert-generating event,” and such events may be user-designated geofencing violations. *Id.* at 33–34 (citing Ex. 1007, 9:53–56, 14:27–30). As discussed previously, the application server in Phillips communicates with the user’s mobile device and, because the application server hosts the geofence and alert applications and the user “designates” the event, the server receives a request to set an event. *Id.* at 34 (citing Ex. 1011 ¶ 141). Petitioner also argues “Zou teaches an interface to receive a request to set an event for the group by creating and assigning geofences to vehicles or a fleet, such that an action (e.g., recording or alert) occurs upon interacting with the geofence.” Pet. 61 (citing Ex. 1005 ¶¶ 9, 95, 203–204, and Figs. 13, 17a, 20a, and 20b; Ex. 1011 ¶ 149). Petitioner’s arguments regarding the teachings of Fast, Phillips, and Zou with regard to setting events “for the group,” which is a key point of contention between the parties, are discussed in more detail below.

With regard to limitation 1(j), which recites a server receiving a request “to set an alert for the group, the request identifying a recipient of the alert,” Petitioner argues “[t]he combination of Fast and Phillips renders obvious that a server (*e.g.*, the GMMS or application server) receives a request to set an alert for the group (*e.g.*, through threshold monitoring or the scenario manager), wherein the request identifies a recipient of the alert (*i.e.*,

one or more users or entities).” Pet. 34 (citing Ex. 1003, 31:24–29, 27:38–44, 45:27–29 and Ex. 1011 ¶¶ 153–54 (Fast’s Beacon Manager and threshold monitoring); Ex. 1003, 21:5–7, 35:39–51, 36:1–3 and Ex. 1011 ¶¶ 150–151 (Fast’s notification scheme working with Fast’s Scenario Manager)). Petitioner also argues that Phillips similarly teaches that an alert application in an application server communicates with a user’s PEF, and allows an “event” to be “designated by the user as an alert-generating event,” and such events may be user-designated geofencing violations. Pet. 33–34 (citing Ex. 1007, 9:53–56, 14:27–30; Ex. 1011 ¶ 141).

As discussed in more detail below, although Petitioner argues Fast alone, or in combination with Phillips, teaches the “group” feature recited in claim 1, Petitioner also argues the “group” feature is taught by Fast and Phillips in combination with Zou. In particular, Petitioner argues Zou teaches “grouping” of vehicles as fleets so that users can “view data by fleet, control data collection parameters by fleet, and compare performance between fleets.” Pet. 58 (citing Ex. 1005 ¶¶ 190–192; Ex. 1011 ¶¶ 105–106). Petitioner further argues Zou discloses that users may also select other users to “view the fleet group” and are enabled to “to set authority levels for the users who can view the fleet group.” *Id.* (citing Ex. 1005 ¶¶ 190–192). In addition, according to Petitioner, Zou teaches an interface to receive a request to set an event for the group by creating and assigning geofences to vehicles or a fleet, such that an action (e.g., recording or alert) occurs upon interacting with the geofence, wherein the geofence alert is created for a fleet with identified recipients. Pet. 61 (citing Ex. 1005 ¶¶ 9, 91, 95, 203–210, Figs. 13, 17a, 18b, 20a, and 20b; Ex. 1011 ¶¶ 149, 156).

As noted, Petitioner’s arguments regarding the teachings of Fast, Phillips, and Zou with regard to the “group” features of claim 1 are discussed in more detail below in connection with our analysis of the parties’ disputes.

Limitation 1(k): check second-level administrative privileges

Limitation 1(k) requires the server to “check the second level administrative privileges before setting a zone, an event, or an alert for the group.” Petitioner argues that the combination of Fast and Phillips teaches that the server (e.g. an application server) checks the second-level administrative privileges (e.g., the user type) before permitting any user to set a zone, an event or an alert for the group (such as Fast’s Zone Manager, Scenario Manager, and Notification Manager). Pet. 35–36.

Petitioner argues two different mappings of the claimed second-level administrative privilege to Fast’s disclosure. In a first mapping, as noted above in connection with limitation 1(f), a wholesaler exercises a first-level administrative privilege to add users / devices to a subscriber’s account, and the subscriber is the user with the highest access privileges in the subscriber account. *Id.* at 35 (citing Ex. 1003, 42:32–35; Ex. 1011 ¶ 157). The subscriber may set zones, events, and alerts for the beacons in his account and, prior to his doing so, his privileges are checked by the GMMS servers. *Id.* (citing Ex. 1003, 32:15–36:40 (describing “scenarios”), 42:14–39 and Fig. 16 (describing and depicting authentication at login prior to being permitted to perform any action)). Under Petitioner’s alternative mapping discussed above—wherein the subscriber has the requisite “first level administrative privileges” and may create additional users and assign their access levels (Pet. 36 (citing Ex. 1003, 42:14–52; Fig. 16, box 532))—these

users (such as “guardians”) may be permitted to exercise the second-level administrative privilege to set zones, events, and alerts for their assigned group of beacons, and their privileges are likewise checked by the servers at login (*id.* (citing Ex. 1003, 42:14–52 and Fig. 16)).

Petitioner also argues that Phillips similarly teaches a process to authenticate users prior to setting zones, events, or alerts by disclosing that a user may be “granted partial or restricted access via a guest login.” Pet. 36 (citing Ex. 1007, 4:40–44; Ex. 1011 ¶ 158). In particular, Phillips stores information pertaining to the user’s level of access to determine a user’s privileges, which include privileges to create geofence alerts; those privileges are thus second-level administrative privileges, as claimed. *Id.* (citing Ex. 1007, 9:15–21).

Petitioner further argues Zou similarly teaches checking a user’s privileges in the user’s permission profile before a user can access functionality for, in particular, creating and editing geofences for a fleet, and viewing and editing an alert template. Pet. 61 (citing Ex. 1005 ¶¶ 203–206; Ex. 1011 ¶ 159).

As noted above, Petitioner’s arguments regarding the teachings of Fast, Phillips, and Zou with regard to the “group” features of claim 1 are discussed in more detail below in connection with our analysis of the parties’ disputes.

Limitation 1(l): store zones, events, and alerts in databases

Petitioner argues the combination of Fast, Phillips, and Zou discloses limitation 1(l), which recites that the server stores “the group’s zone, event, and alert in one or more databases.” In particular, Petitioner argues the combination of Fast and Phillips teaches that a server (e.g., an application server) stores the group’s zone, event and alert (e.g., the saved scenario) in one or more databases. Pet. 36. In Fast’s threshold monitoring embodiment, for example, the group’s zone, event, and alert are stored in a database associated with the threshold management system and the beacon manager. *Id.* at 36–37 (citing Ex. 1003, Figs. 4, 9 and 17:23–29; Ex. 1011 ¶¶ 162–165). In addition, a subscriber in Fast may send feature requests, including a zone request, to the Beacon Controller Interface, which can respond. *Id.* at 37 (citing Ex. 1003, Figs. 4 and 9). Thus, Fast teaches that the Beacon Controller Interface interacts with at least one database to store a user’s zone, event, and alert requests, which Petitioner argues may be a group of users’ zone, event, and alert settings. *Id.* (citing Ex. 1011 ¶¶ 164–165). Additionally, according to Petitioner, Fast teaches that a scenario, which includes the “trigger mechanism” of an event and may be based on a zone (Ex. 1003, Fig. 11-1, element 260), and the “notification scheme,” which “sends an alert associated with the event (*e.g.*, *id.*, 36:34–36), are [] saved and stored on a database in the GMMS so that the GMMS scheduling engine may operate the scenario.” *Id.* (citing Ex. 1003, 36:1–4; Ex. 1011 ¶¶ 160–161).

Petitioner also argues Phillips similarly teaches limitation 1(l) by disclosing an application server hosting a geospatial application, an alert application, and a geofencing application, wherein users connect through a

web server to a database server / application server to interface with those applications. Pet. 37 (citing Ex. 1007, 8:42–53, 9:37–43, 9:53–67). Further, according to Petitioner, Phillips discloses the database server or application server, or both, store zone, event, and alert information that a user “may define and/or manipulate a geofence via the Web browser,” wherein the geofence information itself would be not be stored on the browser but on a remote server. *Id.* (citing Ex. 1007, 14:38–40, 9:1–32). Petitioner argues that, given Phillips’ architecture, “a POSITA would understand that a user would access the application server which would access the database to retrieve stored zone, event, and alert information.” *Id.* at 38 (citing Ex. 1011 ¶ 166).

Petitioner makes similar arguments for Zou, arguing that Zou teaches that a user may create alerts from alert templates, “which a POSITA would understand would be stored in a database for use in the creation of other alerts” wherein the templates would include a group’s zone, event, and alert. Pet. 61–62 (citing Ex. 1005 ¶¶ 9, 105, 111–114, 201; Ex. 1011 ¶ 167). Petitioner also argues Zou’s disclosure of the Network Operations Center (“NOC”) includes “a server that maintains ‘user account information[,]’ which would include information about fleets, alerts, and templates, thereby satisfying this limitation.” *Id.* at 62 (citing Ex. 1005 ¶ 9).

*Limitation 1(m): receive IDs and location information
for multiple mobile devices in a group*

Petitioner argues that Fast, Phillips, and Zou all teach that a server receives IDs for the mobile devices in the group, as recited in limitation 1(m). Pet. 38–40 (Fast and Phillips); *id.* at 62 (Zou).

With regard to Fast, Petitioner argues that Fast’s beacon managers, which are software entities that reside on the GMMS servers, receive beacon

IDs and location information for the beacons in the subscriber's account. Pet. 38–39 (citing Ex. 1003, 25:40–47 (Beacon Manager), 27:1–9 (Beacon Controller Interface), 28:39–52 (Beacon Controller and Location Network Interface), 26:54–57 (tracking mode), 27:45–55 (Beacon Threshold Monitoring Feature), 31:24–29 (tracking mode), and 45:16–29 (threshold monitoring)). Petitioner also argues Phillips discloses that a server stores data from a mobile device (portable electronic facility (“PEF”) in a database, which includes geolocation information associated with that device. Pet. 39–40 (citing Ex. 1007, Fig. 4 and 6:33–34, 6:49–56). With regard to Zou, Petitioner argues that Zou's Network Operations Center is configured to receive serial number and location information from the telemetry devices, which Petitioner argues the ordinarily skilled artisan would understand to include an ID for the telemetry device “so that the server can determine where the message originated, and, in part, display information to a user about where particular telemetry devices are located for example in an alert report.” Pet. 62 (citing Ex. 1005 ¶¶ 9, 86, 105–106, 118, 121 and Figs. 4, 5, 21a; Ex. 1011 ¶¶ 80–81, 179).

As noted above, Petitioner's arguments regarding the teachings of Fast, Phillips, and Zou with regard to the “group” features of claim 1, including as recited in this limitation, are discussed in more detail below in connection with our analysis of the parties' disputes.

Limitation 1(n): determine whether to send an alert / send an alert

The final two limitations of claim 1, which Petitioner argues collectively as “limitation 1(n),” recite generally that the server is configured to compare the location information for the identified mobile devices with the group's zone (geofence) and event to determine whether to send the

group's alert, and is also configured to cause the group's alert to be sent. Limitation 1(n) is described by Patent Owner as requiring "server-based threshold monitoring" (PO Resp. 20), and it is a key point of contention between the parties that is addressed in more detail below in connection with our analysis of the parties' disputes.

In a nutshell, Petitioner argues the combination of Fast and Phillips renders this limitation obvious because Fast teaches embodiments where the comparison to determine whether to send the alert takes place in the server—specifically (1) threshold monitoring in tracking mode; and (2) the Scenario Manager. Pet. 40–43 (citing Ex. 1003, 27:38–42, 27:52–54, 23:56–62, 26:36–39, and 26:54–57 (threshold monitoring in tracking mode wherein Beacon Manager compares data harvested from beacons against zones); *id.* at 12:40–46; 21:5–7 (GMMS sends alerts when threshold met); Ex. 1011 ¶ 163 (beacon manager resides on server); Ex. 1003, 36:34–41 (processing the scenario involves executing the notification scheme); *id.* at 35:47–64 (notification scheme causes alert to be sent); *id.* at 36:19–41 (server causes alert to be sent according to notification scheme)). Petitioner also argues that, to the extent Fast's comparison does not take place in the server, Phillips makes up for that deficiency because Phillips discloses that its application server, which may include the geofencing and alert applications, "performs the comparison of IDs and location information with the zone and event to determine whether to send an alert, and cause[s] an alert to be sent." *Id.* at 43 (citing Ex. 1007, 9:37–42, 9:53–67 (application server may support geofencing)).

Petitioner argues the combination of Fast and Phillips also teaches that geofencing alerts "could be applied to multiple beacons or a group of

beacons.” Pet. 44 (citing Ex. 1011 ¶ 139). Petitioner additionally combines Zou with Fast and Phillips, arguing that Zou discloses determining “whether multiple telemetry device IDs apply to an alert” because, in Zou, “multiple vehicles can be tracked with respect to one geofence.” Pet. 63 (citing Ex. 1005 ¶ 204). Therefore, according to Petitioner, the combination of Fast, Phillips, and Zou teaches server-based threshold monitoring for a group because, once the system is triggered by a tracked mobile device relative to a geofence, the server will cause an alert to be sent for a group (fleet). *See id.*

As noted above, Petitioner’s arguments regarding the teachings of Fast, Phillips, and Zou with regard to the “group” features of claim 1, including as recited in this limitation, are discussed in more detail below in connection with our analysis of the parties’ disputes.

(b) Dependent Claims 2–7, 12–16, 20, and 22–26

Petitioner also provides analysis for claims 2–7, 12–16, 20, and 22–26, which all depend from claim 1, arguing that they also would have been unpatentable for obviousness over Fast, Phillips, and Zou. Pet. 44–54 (Fast and Phillips); *id.* at 63 (adding Zou). We briefly discuss Petitioner’s contentions for these claims, which focus on the teachings of Fast and Phillips. Petitioner argues that these claims would have been obvious over the combination of Zou with Fast and Phillips based on the reasons Petitioner provides with regard to claim 1 above and with regard to the dependent claims as noted below. *See* Pet. 63.

Petitioner argues that dependent claim 2, which, essentially, adds a second zone and event, is taught by the combination of Fast and Phillips because both teach that a user may set multiple zones and events. Pet. 44–45 (citing Ex. 1003, 32:45–46 (noting that multiple scenarios may be active

for a beacon); *id.* at 29:60–64); Ex. 1007, Figs. 32 and 36 (user interface could be used to create multiple zones, events, and alerts)).

Petitioner argues that dependent claims 3–5, which further define the interfaces of claim 1, are taught by Fast and Phillips because each reference discloses user interfaces to set zones, events, and alerts, and to add mobile devices. Pet. 45–47 (citing, *e.g.*, Ex. 1003, 4:57–58, 5:27–36, 18:52–54, 20:42–51, 20:63–21:7, 32:15–20, 32:58–35:67; Ex. 1007, Fig. 32; Ex. 1011 ¶¶ 128, 198, 202)).

Petitioner argues that dependent claims 6 and 7, which generally require that servers control access to the interfaces, are taught by Fast and Phillips because each reference discloses a server controlling access (such as through login credentialing) to one or more user interfaces (such as Fast’s portals) for adding mobile devices to the group (such as Fast’s adding beacons to an account or to a scenario). Pet. 47–49 (citing, *e.g.*, Ex. 1003, 5:28–36, 20:42–56, 24:56–62, 33:1–17, Figs. 11, 14-1, 16-1; Ex. 1007, 9:15–21, 9:63–67, 24:31–34, 24:39–40, Fig. 32; Ex. 1011 ¶¶ 204–205)).

Petitioner argues that dependent claims 12–15, which define the “alert” of claim 1 as an “email,” a “text message,” a “device notification,” or a “phone call,” respectively, are taught by Fast and Phillips because each reference discloses an alert in the form of an email, a text message, or a phone call, as well as a device notification such as an SMS text. Pet. 49–50 (citing Ex. 1003, 34:32–57, Fig. 11-2 (element 286); Ex. 1007, 4:16–22, 6:11–12, 16:26, Fig. 36; Ex. 1011 ¶¶ 210, 211, 213, 214, 216, 218, 219)).

Petitioner argues that dependent claim 16, which states that the location information for the mobile device in claim 1 is “determined by GPS,” is taught by Fast and Phillips because both references disclose

determining location information of a mobile device by GPS. Pet. 50 (citing Ex. 1003, 5:11–16; Ex. 1007, 11:48–51, 10:1–6; Ex. 1011 ¶¶ 220–221)).

Petitioner argues that dependent claim 20, which states that the “second level administrative privileges are defined for a customer account,” is taught by Fast because, as explained in connection with limitation 1(e), Fast teaches that the second-level administrative privileges are defined for a customer’s account, e.g., accessing the features of a subscriber’s account such as the scenario manager. Pet. 51 (citing analysis of 1(e) and Ex. 1011 ¶¶ 223–224). Petitioner further argues “[i]t would have been obvious to combine this teaching with Phillips.” *Id.* (citing Ex. 1011 ¶ 125).

Petitioner argues that dependent claim 22, which states that “the second level administrative privileges are checked at a log-in,” is taught by Fast because, as explained in connection with limitation 1(e), Fast teaches that “any access to a subscriber’s account in the system requires at least determination of the level of authorized access at login for second-level administrative users.” Pet. 51 (citing Ex. 1003, Fig. 16-1 (elements 505b, 505c, 512); Ex. 1011 ¶ 228). Petitioner further argues “Phillips describes that access may be granted at different access levels, and access may be granted via a ‘login,’” and the ordinarily skilled artisan “would understand these access levels are checked via a user login process.” *Id.* (citing Ex. 1007, 25:48–53; Ex. 1011 ¶ 229).

Dependent claims 23 and 24 generally state that the first / second level administrative privileges are checked “when” the specified function is performed (adding a mobile device to the group for the first level and setting a zone, event, or an alert for the second level). Petitioner’s arguments regarding claims 23 and 24 are discussed further below in our analysis of the

parties' contentions, as Patent Owner expressly challenges Petitioner's arguments regarding those claims. PO Resp. 26–29.

Dependent claim 25 states that “the one or more servers sends the alert.” Petitioner argues that this claim is taught by Fast because Fast teaches that the GMMS system includes application servers that send the alert. Pet. 53–54 (citing Ex. 1003, 36:12–18, 36:34–41 and Figs. 2, 12, 19; Ex. 1011 ¶ 237). Petitioner also argues Phillips teaches that the application server may host a geofencing application, which can send the alert for a PEF, and by extension for the group. *Id.* at 54 (citing Ex. 1007, 9:53–62, 14:27–30 (“In any case, the geofencing application may be the alert application and, therefore, may generate the alert when the [PEF] crosses the geofence.”); Ex. 1011 ¶ 238).

Dependent claim 26 states that “the one or more servers cause another server to send the alert.” Petitioner argues that this claim is taught by Fast because Fast discloses more than one server that can cause a server to send the alert. Pet 54. “For example the scenario manager located on the application server would cause another application server or the web server to send an alert.” *Id.* (citing Ex. 1003, 32:38–56 and Fig. 2; Ex. 1011 ¶ 242). Petitioner further argues the ordinarily skilled artisan would understand from Phillips “that an alert is generated by the application server (see analysis of Claim 25), and that the application server would cause the web server to relay the alert on to the PEF of the end user.” *Id.* (citing Ex. 1011 ¶ 243; Ex. 1007, 9:63–67 and Fig. 8). “In addition, as discussed above with respect to claim 12, Phillips discloses sending an email alert. . . . A POSITA would understand that an application server would cause another server (the web server) to send the email.” *Id.* (citing Ex. 1011 ¶ 243).

(2) Patent Owner's Contentions

Aside from arguing that Phillips is not prior art (which, as noted above, we do not find to be persuasive), Patent Owner raises two primary arguments against the combination of Fast, Phillips, and Zou for claim 1, challenging the prior art's disclosure of (1) the "group" features recited throughout claim 1; and (2) server-based threshold monitoring, as recited in limitation 1(n). PO Resp. 16–26 (Fast); *id.* at 30 (Phillips fails to disclose "group" limitations); *id.* at 31 (Zou does not overcome "server" or "group" deficiency in Fast). Patent Owner also argues "a person of ordinary skill would not be motivated to combine Fast and Zou" (*id.* at 31), and the secondary consideration of licensing "amply rebuts" Petitioner's obviousness case (*id.* at 32–34).

Patent Owner also expressly challenges Petitioner's arguments regarding Fast's disclosure of claims 23 and 24. *Id.* at 26–29. Patent Owner does not argue dependent claims 2–7, 12–16, 20, 22, 25 or 26 separately from claim 1.

We summarize each contention below, and we provide our analysis of these contentions along with our analysis of Petitioner's contentions in the subsequent section below.

(a) "Group" features

With regard to the "group" features recited throughout claim 1 (wherein, e.g., zones, events, and alerts are set and sent for a "group of mobile devices"), Patent Owner argues "Fast does not disclose assigning a *group* of beacons to a single scenario. Rather, every disclosure of scenarios in Fast states that only a single beacon is assigned to a given scenario." PO Resp. 7, 17–19. Patent Owner also argues "Phillips does nothing to

overcome the ‘group’ deficiency in Fast” because “Phillips (like Fast) tracks mobile devices on a device-by-device basis, not a group basis.” PO Resp.

30. Patent Owner similarly argues Zou “performs threshold monitoring on an individual device-by-device basis, not a group basis.” *Id.* at 31.

(b) Server-based threshold monitoring

With regard to the limitation 1(n), wherein the server compares “the IDs and location information with the group’s zone and event to determine whether to send the group’s alert,” Patent Owner argues Fast does not show “server-based threshold monitoring,” but discloses only the remote beacons or manual human personnel performing the task of comparing object location information with zone information. PO Resp. 2, 8–11, 20–25.

Patent Owner also argues “Zou does not overcome the ‘server’ deficiency in Fast, because Zou outsources threshold monitoring to remote telemetry devices instead of performing this task at servers.” *Id.* at 30 (citing Ex. 1005 ¶¶ 88, 91, 97). Patent Owner also argues “there is no dispute on this point: Petitioner’s own Petition stated that ‘Zou’s telemetry devices determine whether an event condition is met (instead of the server).’” *Id.* at 30–31 (citing Pet. 63).

(c) Claims 23 and 24: checking privileges “when” adding devices / setting a zone, event, or alert

Patent Owner argues Petitioner’s arguments are based on checking administrative privileges only at login, and Petitioner does not show that Fast discloses checking first or second administrative privileges “when” adding a mobile device (first level) or setting a zone, event, or alert (second level). PO Resp. 26–29. Patent Owner argues that checking these privileges *at login* is not the same as checking these privileges *when* performing the recited function, as required by these dependent claims. *Id.*

(3) Analysis and Reasoning

We have considered fully the evidence and arguments presented by Petitioner explaining how the combination of Fast, Phillips, and Zou teaches the limitations of claims 1–7, 12–16, 20, and 22–26. Pet. 19–54 (arguing claims over combination of Fast and Phillips); Pet. 56–63 (arguing claims over the combination of Fast, Phillips, and Zou, building on earlier arguments); Reply 1–8 (Fast), 14–18 (Fast, Phillips, Zou), 21–22 (claims 23–24); Ex. 1011 (Heppe Decl.). Except as expressly addressed below, we find Petitioner’s evidence and arguments persuasive and we adopt Petitioner’s analysis and reasoning as our own. Our reasons are as follows.

We find that Fast, Phillips, and Zou overlap broadly, with each reference generally disclosing location-tracking systems in which servers communicate with mobile devices (such as beacons, PEFs, or telemetry devices, respectively) that provide location information (such as through GPS). Ex. 1003, 9:10–16, 10:22–25 (Fast); Ex. 1007, 1:34–43, 10:47–50, 11:51–52 (Phillips); Ex. 1005 ¶¶ 9, 78–79, 95 (Zou). These systems all allow users to track the mobile devices relative to user-defined zones, and to create events wherein, for example, an alert will be sent if a tracked mobile device travels into or out of the zone. *E.g.*, Ex. 1003, 5:41–46, 32:15–56 (Fast); Ex. 1007, 9:53–56; 14:27–30 (Phillips); Ex. 1005 ¶¶ 1, 9, 95, 203–204, and Figs. 13, 17a, 20a, and 20b (Zou). Patent Owner concedes these general points. *See* PO Resp. 6, 7, 11, 12.

Although the references overlap substantially, we analyze claim 1, as do the parties, primarily with regard to the Fast reference. Fast discloses a location-tracking system using mobile devices (beacons) with, for example, GPS functionality to track locations of different items, such as individuals

(e.g., members of a family) or objects (e.g., vehicles). Ex. 1003, 3:19–22, 9:10–16, 10:22–25, 24:56–65, 33:1–17. Fast also discloses servers communicating with the mobile devices (*e.g.*, *id.* at 44:20–22), which each having IDs (*e.g.*, *id.* at 27:2–5). Thus Fast, alone, discloses limitations 1(a) and 1(b), and this much does not appear to be disputed by Patent Owner. See PO Resp. 6–7.

Fast also discloses multi-tiered administrative privileges as claimed. Fast’s disclosure of different administrative privileges is independent of, and distinct from, Fast’s hierarchies. For instance, Fast’s disclosure of *privilege levels* is directed to the *administrative abilities* of the users in the system (e.g., a first level to create/add users and devices, and a second level to build scenarios), whereas Fast’s disclosure of *hierarchical levels* is directed to the *relationships* between people using the system (e.g., wholesaler, subscriber, guardian). Fast’s multi-tiered system allows a “first level” of administrative *privilege* at both the wholesaler and the subscriber *hierarchy* levels because both hierarchical levels allow a privilege to configure information-sharing environments by creating/adding users. *E.g.*, Ex. 1003, 18:25–37, 38:46–54, 42:36–43:11, Fig. 22. Fast teaches a first-level administrative privilege at the wholesaler level because the wholesaler can configure subscriber accounts by, *inter alia*, adding, editing, and deleting subscribers and assigning beacons to a subscriber. *Id.* at 16:29–30, Fig. 22, Fig. 14-2 (box 432)). The wholesaler’s privilege is checked before the wholesaler may configure subscriber accounts (including adding/assigning beacons) because the wholesaler must login to the system (through its portal, which is a user interface) using a user ID and password. *Id.* at 16:9–11, 38:31–32, Fig. 14-1 (box 404) (wholesaler portal).

Fast's subscriber uses a second-level administrative privilege (which is different from the first-level privilege to, *inter alia*, add devices (beacons)), by creating and managing scenarios using the Scenario Manager through the subscriber's portal (which is a user interface), in which specific beacons are monitored and specified people may be notified upon occurrence of events. Ex. 1003 at Figs. 16-1, 16-2, 6:21–23, 32:51–56, 42:14–41. The subscriber's privilege is checked before the subscriber may perform these functions because the subscriber must login to the system (through its portal / user interface) using a user ID and password. *Id.* at Fig. 16-1 (box 504) and 42:19–20 (subscriber portal).

Fast's subscriber may also act as an administrator of its own account and use a first-level administrative privilege, through the subscriber portal, to add, delete, and manage other users, including guardians, and to manage beacons. *Id.* at 42:35–67 and Figs. 16-1, 16-2 (boxes 522, 523). As part of this administrative function, the subscriber may authorize a guardian, such as a babysitter, to track the location of a child. *Id.* at 4:61–62, 20:42–45, 43:1–11, Fig. 16-2 (box 527, “Assign Guardians to Dependents/Assets”). The guardian may carry out this tracking responsibility by using the Scenario Manager in the same manner as the subscriber described above—wherein the system will convey at least location information (such as information about the location of the tracked child relative to a designated zone), to “specified people.” *See id.* at 4:61–62, 43:1–11, 32:51–56, 35:7–36:11, Figs. 16-1, 16-2, 11-1, and 11-2. Fast thus discloses a subscriber uses a first-level administrative privilege, as claimed, because the subscriber may use its portal to, *inter alia*, add devices (manage beacons), and Fast's guardian exercises a second-level administrative privilege, as claimed,

because the guardian may also use the subscriber portal (using an authorized login) to specify event conditions by configuring scenarios. Because login is required before accessing the portal to perform these functions, Fast discloses that these administrative privileges are checked before the functions are performed, as claimed.

Fast also discloses user interfaces (portals) for setting a zone, an event, and an alert by describing the Subscriber Administration Module, which provides functionality that may be accessed through the subscriber's portal. Ex. 1003, at Figs. 16-1, 16-2 (subscriber portal) 20:32–21:12, 42:14–43:11. As part of that functionality, which includes a “Zone Manager,” Fast allows zones to be created, such as “allowed or disallowed zones,” to enable monitoring of tracked items in particular areas, which may be activated or deactivated according to a schedule. *Id.* at 20:63–67. These zones are independent of where the mobile devices are located, as recited in claim 1, because they “can be defined as any geographic shape or combinations of shape on a map.” *Id.* at 33:34–36. Subscribers may also use a Scenario Manager, also accessed through the subscriber's portal, to set up the GMMS software to automatically notify them (send an alert, such as a message) upon certain event conditions, such as a beacon reaching a specified location. *Id.* at 12:40–44, 32:14–56. Thus, Fast discloses a server within the GMMS system receiving requests through a user interface to set a zone, an event, and an alert, as claimed. Fast also discloses one or more databases for storing zone, event, and alert information because it discloses that once a trigger mechanism (zone/event), a schedule (event), and a notification scheme (alert) have been defined for a scenario, all of this information is saved in a database. *E.g., id.* at 36:1–6.

We provide further analysis in the context of the parties' disputes, which center on the server-based threshold monitoring limitation of claim 1 and the "group" features recited throughout claim 1.

(a) Server-based threshold monitoring (Limitation 1(n))

As noted above, Patent Owner argues neither Fast nor Zou disclose limitation 1(n), which, generally stated, requires the server to perform the comparison of the location of the mobile device with the group's zone and event to determine whether to send an alert. PO Resp. 30–31. Patent Owner contends that Fast and Zou, unlike the claimed invention, perform this comparison in the *mobile devices* themselves, and *not at the server*. *Id.*

We are not persuaded by Patent Owner's arguments because they are based on inaccurate characterizations of the prior art. For the "server" portion of this limitation, as Petitioner points out, Fast's threshold monitoring functionality teaches the claimed server-side comparison and alert determination. *See* Pet. 41. In particular, Fast discloses that a beacon can perform only one task at a time, so if a beacon is in "tracking" mode (such as tracking a lost dog, Ex. 1003, 26:44–54), it cannot perform threshold monitoring itself. In that situation, the Beacon Manager will take over threshold monitoring using "locate points," *e.g.*, location information, sent by the beacon:

When the BM [Beacon Manager] receives the request to go into a threshold monitoring state, the BM checks to determine if the beacon is currently in a tracking state. If so *the system simply uses the data harvested from the beacon* while in a tracking session *to compare* against the parameters of the threshold settings.

Ex. 1003, 27:49–54 (emphases added); *see also id.* at 31:24–29. Fast's Beacon Manager, which is software running on a server, thus performs

“threshold monitoring while the Beacon itself is in the tracking mode.” *Id.* at 30:67–31:3. Fast explains that “the Beacon Manager has been designed to provide multiple features simultaneously even if the Beacon itself can only operate in one mode at a time.” *Id.* at 30:65–67. In performing threshold monitoring, “the [Beacon Manager] inspects each point to manually determine if the beacon is still within the prescribed zone or not.” *Id.* at 26:54–57. We find Fast teaches that the server-side Beacon Manager software module, in a “threshold monitoring” mode, harvests “tracking points” from an identified beacon and compares those points with the “prescribed zone.” Therefore, we find Fast teaches that a server in Fast may perform the comparison of mobile device IDs and location information with the user-defined zone.

Patent Owner argues Fast’s disclosure of harvesting tracking points from beacons that are in “tracking” mode does not refer to “server activity” but instead, by describing the harvesting as being done “manually,” discloses “human activity.” PO Resp. 20–21. As support, Patent Owner relies on deposition testimony from both parties’ designated experts, who acknowledged that they were not aware of use of the term “manually” to describe software activity. *Id.* at 20–21 (citing Ex. 2002 (Heppe Dep.) at 156:14–20, 160:20–161:7; Ex. 2010 (Schonfeld Decl.) ¶ 25). Patent Owner additionally argues that reference in a particular passage of Fast to the “system” using location data harvested from a beacon does not necessarily reference server activity, because Fast teaches that “human operators” are part of the Fast “system.” PO Resp. 23 (citing Ex. 1003, 27:49–54); *id.* at 21–22 (citing Ex. 1003, 30:64–66, 4:50–52).

We are not persuaded by Patent Owner’s arguments. Although it may be unusual to use the term “manually” to refer to actions performed by software, we find persuasive the credible deposition testimony of Petitioner’s expert, Dr. Heppe, on this point and afford it substantial weight. In particular, Dr. Heppe opines that the use of the term “manually” in the referenced passage of Fast logically distinguishes the Beacon Manager performing a point-by-point inspection of location data received from the beacon, as opposed to the situation in which the beacon itself performs threshold monitoring. *See* Ex. 2002, 155:16–156:5; *see also* Pet. Reply 6. Dr. Heppe’s opinion is supported by Fast’s consistent description of the Beacon Manager as a server-side “software entity” that is “assigned to each Beacon in the GMMS system.” Ex. 1003, 25:41–47. Fast also states that the Beacon Manager is accessible through many software-based administration modules within the “GMMS Software Architecture,” which is based on a software application framework called the “Guardian Agile Mobile Monitoring Architecture.” *Id.* at 18:5–7, 18:60–67, 19:29–31, 19:41–45, 19:50–51, 20:42–45, 22:26–35. Fast also repeatedly refers to the GMMS as running on a server network. *Id.* at 6:66–7:2, 7:43–45, 8:38–40.

In addition, Fast consistently states that the software-based “Beacon Manager”—not a human operator—performs threshold monitoring if the beacon is not able to do so (e.g., if the beacon is in tracking mode). This is clear not only from the passages we cite above, but also from the flow charts in Figures 6–8 of Fast, which depict the operation of the Beacon Manager as a software entity managing the beacons. Figure 8 in particular illustrates how the Beacon Manger provides threshold monitoring while the Beacon is in tracking mode. Ex. 1003, Fig. 8, block 187. The related passage of Fast’s

written description, describing the flow chart of Figure 8, also states that the Beacon Manager performs this function:

If the determination made at **183** that the Beacon is already in the tracking state, **185**, the Beacon Manager begins real-time inspection **187** of all incoming data from the Beacon. *Inspecting this data and comparing it to the threshold allows the Beacon Manager to provide threshold monitoring while the Beacon is in tracking mode.*

Id. at 31:24–29 (emphasis added).

Ignoring those portions of Fast, Patent Owner cites Fast’s disclosure of a particular example called a “Multi-User Locate Request,” in which a customer seeks real-time tracking of an object for which the beacon is already in tracking mode. *See* PO Resp. 10 (citing Ex. 1003, 26:34–39). Fast explains that, in this situation, Fast’s Beacon Manager does not send a “second, redundant command” to the beacon to perform tracking, but will harvest the locate points “to both the monitoring station application as well as the subscriber application.” Ex. 1003, 26:37–39. Although we agree, as Patent Owner contends, that this passage describes Fast’s Beacon Manager sending location information to a monitoring station, where it may be viewed by a human operator (PO Resp. 10), we disagree that this passage supports Patent Owner’s argument against Fast’s disclosure of server-side threshold monitoring or requires a different view of the portions of Fast we have relied upon above. Simply put, these portions of Fast describe different functionality. The example highlighted by Patent Owner describes a specific example of how Fast’s Beacon Manager may respond to a real-time *tracking request* that is redundant of ongoing tracking by a particular beacon (e.g., reporting current location of a stolen car) (Ex. 1003 at 26:29–39), whereas the portions of Fast we have relied upon above describe situations in which

the Beacon Manager performs *threshold monitoring* (e.g., comparing beacon location to a pre-set zone boundary) over and above ongoing tracking by a beacon (*id.* at 23:62–67, 27:46–48)). *See also* Pet. Reply 6–7.

Patent Owner also emphasizes another isolated passage of Fast (cited in our Institution Decision), which refers to the “system” taking steps that constitute threshold monitoring. PO Resp. 23 (citing Inst. Dec. 27 and Ex. 1003, 27:49–54). Focusing on that specific reference to “the system,” Patent Owner argues that it represents a “change of phrasing,” which suggests that Fast must be disclosing that “some system component *other than the BM* is performing the threshold monitoring.” *Id.* at 25 (emphasis added). Patent Owner then argues that because Fast’s “system” includes human operators, Fast’s reference to the “system” performing threshold monitoring means that *humans* perform that function instead of software running on a server. *Id.* at 23–24. We disagree. As we note above, Fast refers in several places to the “Beacon Manager” in particular—not merely “the system”—as performing “threshold monitoring.” *E.g.*, Ex. 1003, 30:67–31:3, 31:24–29; *see also* Reply 7–8. Moreover, although we agree Fast discloses that human operators within the system may “watch for incoming alarm signals” (*id.* at 4:50–52), we do not agree that Fast’s disclosure teaches that humans, instead of software modules running on servers, generate the alarm signals *themselves* by harvesting beacon location points and comparing them to zones when the beacons are in tracking mode.

In sum, we find Petitioner’s reasoning and analysis—that Fast discloses server-side threshold monitoring when beacons are in tracking mode—to be persuasive and supported by the cited portions of Fast and, as such, we adopt them as our own along with our additional analysis above.

On the other hand, Patent Owner's arguments, which rely principally on portions of Fast in isolation, do not show ambiguity in Fast's disclosure (*cf.* PO Resp. 25) and are not persuasive to rebut Petitioner's showing.

Similarly, because Patent Owner's expert relies on the same analysis of Fast's disclosure as advanced by Patent Owner (which, as noted above, we find ignores critical portions of the record evidence), we afford little weight to his testimony. *See* Ex. 2010 ¶¶ 21–25.

We also find persuasive Petitioner's arguments based on the combination of Fast with Phillips, which Patent Owner does not address. For that combination, Petitioner notes that Fast also discloses a server-side determination of whether to send alerts through Fast's "Scenario Manager," in which an event is triggered and sent out as an alert in response to a zone violation. *See* Pet. 42–44; Ex. 1003, 8:59–63, 26:7–12. In particular, Fast discloses that servers receive location-tracking information from beacons and share that information with specified users according to specified scenarios. For example, Fast's Scenario Manager, running on a server, includes a scenario monitor that "listens for incoming trigger reports from all Beacons." *Id.* at Figs. 2, 3-1, 3-2, 12 (depicting server environment and Scenario Manager module of subscriber portal), 36:14–15. Fast further discloses "[p]rocessing the scenario involves executing the notification scheme associated with the trigger from the associated Beacon," which "specifies what messages are sent to what entities using what notification methods." *Id.* at 36:34–38. Even if Fast does not disclose in that situation that the comparison of beacon IDs and location information is made at the server, Phillips discloses that its application server, which may include geofencing and alert applications, performs the comparison of PEF IDs and

location information with a user-defined zone and event to determine whether to send an alert, and cause an alert to be sent. *See* Ex. 1007, 9:37–42, 9:53–67, 14:27–34, and Fig. 32.

We find that the ordinarily skilled artisan, in light of the combined disclosures of Fast and Phillips, would understand that Fast’s server could receive location information from the beacons and perform threshold monitoring itself as part of its determination whether to send alerts. As Petitioner’s expert explains, and we find credible, this is consistent with a trend at the time of the invention in which software vendors were moving from selling software that operated on a client’s device to software operating on a server. Ex. 1011 ¶¶ 57–64. Thus, the ordinarily skilled artisan would have had reason to combine the teachings of Fast and Phillips to employ threshold monitoring at a server, instead of at a mobile device, to allow vendors to update software and features of their system for all of their clients at once, and also to free up client devices to perform other tasks.

In sum, we find Fast, alone, discloses the server-side threshold monitoring, as recited in limitation 1(n), by disclosing the Beacon Manager performing threshold monitoring, and we are not persuaded by Patent Owner’s contrary arguments and expert testimony, which we find ignore critical portions of the record. We also find the combination of Fast and Phillips teaches this portion of limitation 1(n), and note that neither Patent Owner nor Patent Owner’s expert address this combination relative to that limitation. We further address the “group” feature, recited throughout claim 1 including limitation 1(n), below.

(b) “Group” Limitations

Group limitations—Fast alone.

Patent Owner argues that limitations 1(g)–1(j)—which, stated generally, require the server be configured to receive, through an interface, requests to set a zone, an event, and an alert “for the group”—are not satisfied by a system that provides only tracking on a per-beacon basis, but instead require “a unified zone, event, and alert scenario [assigned] to a *group* of tracked [devices].” PO Resp. 16. Therefore, according to Patent Owner, Fast does not disclose these limitations because “Fast does not disclose applying a monitoring scenario to a group of tracked beacons”; rather, “every example of applying a scenario to a beacon in Fast indicates that only a single beacon (not a group of beacons) is assigned to that scenario.” *Id.* at 17 (citing Ex. 1003, 35:9–38, 25:50–26:64, Fig. 11-1).

Petitioner, on the other hand, argues that Fast teaches the “group” feature because a subscriber in Fast may have “multiple beacons” (Pet. Reply 2 (citing Ex. 1003, 24:56–65) and a scenario, once created, may be applied to more than one beacon (*id.* (citing Ex. 1003, 36:1–6, 35:16–22; Fig. 11-1, boxes 255, 261 and 294)). Petitioner further argues that Fast discloses group monitoring by disclosing that a “zone” may be assigned to “one or more dependents” (*id.* (citing Ex. 1003, 20:65); *see also* Pet. 26), that a scenario monitor may listen for incoming trigger reports for multiple beacons (Pet. Reply 2 (citing 36:12–16)), and that notifications (alerts) of events based on zones may be sent to multiple entities (Pet. 24 (citing Ex. 1003, 35:47–51); *see also* Ex. 1003, 36:34–41 (notifications sent to “entities”)).

The parties' dispute centers on whether Fast discloses the "group" features of claim 1 by disclosing that the same zones, events, and alerts in Fast may be individually applied to multiple beacons considered, at some level, to be part of group, such as beacons assigned to a subscriber's family. *See* Pet. 26; PO Resp. 17; Pet. Reply 2; Tr. 84:3–17 (Patent Owner); *id.* at 41:10–43:4 and 139:9–16 (Petitioner). In that regard, the parties do not appear to dispute that Fast's user interface does not allow a user to select a "group" of devices, recognized as such in the interface, and thereby set a zone, device, and alert for that group in one transaction.

Petitioner disputes, however, that the '931 patent claims require assigning a zone, event, and alert to a group in "one transaction." Tr. 140:6–9. Petitioner argues, in particular, that it is unclear from the claims "whether certain actions in relation to the 'group,' such as setting a zone, event, and alert for the group requires that the action specify a group name or group identification rather than taking the action individually for each device within the group." Pet. 10. Petitioner also argues that "it is unclear whether the action needs to apply to every device within the group, or whether the claim requires only that the action relates to at least one member of the group." *Id.* Petitioner takes the position that the '931 patent describes a "group" as, for example, coextensive with members of a family or users in an "information-sharing environment." *Id.* Based on that view, according to Petitioner, Fast's "group" would be understood by the ordinarily skilled artisan "to be a group of dependents or beacons under or within a subscriber's account, the beacons assigned to certain groups of items, or the group of beacons under the purview of a guardian." Pet. 26 (citing Ex. 1011 ¶ 87).

Having considered fully the arguments of the parties, we are not persuaded that Fast's disclosure falls within the claimed "group" features of claim 1. As an initial matter, we note that Petitioner's references to a "group" appear to include a subjective consideration. In essence, under Petitioner's view, the claimed "group" features may be satisfied by a logical construct and mapped to Fast's disclosure wherein, for example, a subscriber subjectively considers individually tracked dependents to be a "group," such as where they are, at some point, assigned to a common guardian. *See* Tr. 141:6–15, 142:6–14. We disagree with Petitioner's argument. We conclude that claim 1, read as a whole, requires the server be configured to provide an interface that allows setting a zone, an event, and an alert for tracking "multiple mobile devices" *as a group*, which does not include repeating settings, seriatim, for individual devices that may be subjectively considered by the subscriber to be a "group."

Our reading of the "group" features of claim 1 is not premised on a particular reading of the term "group," which we conclude is subject to its plain and ordinary meaning of "two or more," but instead on the entirety of claim 1. The "group" features are argued by the parties principally with regard to limitation 1(g), which requires the server be configured to provide "one or more interfaces for setting a zone, an event, and an alert *for the group*." The "group" features are also recited throughout claim 1, wherein limitations 1(h)–1(j), generally, require the server be configured to receive a request to set a zone, an event, and an alert "for the group." Indeed, virtually every limitation in claim 1 refers to "the group." In terms of what devices are part of "the group," the term "group of multiple mobile devices" is introduced in limitation 1(c), and builds on limitation 1(b), which recites that

the “mobile devices” each have an ID as well as a “location information source.” The requirement of a “location information source” in each mobile device indicates that “the group” in claim 1 refers to a *group of devices that may be tracked*, which is not satisfied by a “group” comprising one mobile device being tracked and one mobile device doing the tracking. Thus, we do not agree with Petitioner’s view that, in claim 1, the “group of mobile devices” includes devices being tracked as well as the devices receiving tracking information, which would allow (according to Petitioner) the ability to set a zone, an event, and an alert for one device to be tracked to satisfy the “group” limitation because the mobile device to be tracked would be logically “grouped” with a device doing the tracking. *See* Pet. 10.

We also conclude that claim 1’s requirement of a particular configuration of an interface for setting a zone, event, and an alert on a “group” basis also answers negatively the question, posed by Petitioner, as to whether claim 1 encompasses an interface in which those actions are taken only on a device-by-device basis. *See* Pet. 10. If applying a scenario to a single dependent beacon does not create “group” tracking, as Petitioner appears to concede (Tr. 139:9–140:1), the ability of Fast’s subscriber simply to access the same interface at some later point and repeat the same scenario for another dependent beacon cannot change that result without making the determination of whether these two beacons are a “group” turn on the subscriber’s subjective point of view. In other words, if a “group of mobile devices” may be read on a logical construct as mentally applied by a subscriber—such as the subscriber subjectively considering two dependent beacons assigned to the same guardian as a “group”—then whether a system falls within the scope of claim 1 would turn on the subjective intent of the

user. Such a view of the scope of claim 1 is unreasonable as it would render the claim indeterminate. *Cf. Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1350-55 (Fed. Cir. 2005) (“The scope of claim language cannot depend solely on the unrestrained, subjective opinion of a particular individual purportedly practicing the invention.”) (*abrogated on other grounds by Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120 (2014)).

We conclude that independent claim 1 of the '931 patent, by requiring, *inter alia*, a server configured to provide an interface for setting a zone, an event, and an alert “for the group,” does not encompass a system, as we find Fast discloses, in which a zone, an event, and an alert are set on a device-by-device basis—even if the same zone, event, and alert may be repeated for more than one device. Thus, we are not persuaded that Fast’s disclosure reads on the “group” features of the '931 patent claims.

Group limitations—Fast combined with Phillips.

Petitioner also argues the “group” feature of claim 1 is obvious in light of Fast combined with Phillips. Pet. 27–30; Pet. Reply 15–17. In particular, Petitioner argues Phillips discloses tracking “locations of users in a defined group” (Pet. Reply 15 (citing Ex. 1007, 4:65–67 and 6:1–2)), and also discloses a user interface for assigning a geofence to a group (*id.* (citing Ex. 1007, Fig. 32); *see also* Pet. 29). Referring to Figure 32 of Phillips (shown below), Petitioner argues that Phillips discloses phones assigned to “Alan” and “Frank” that are both assigned to the same geofence, and further illustrates that another phone assigned to “Geoff” may also be assigned to the same geofence, thus disclosing the claimed “group” feature. Pet. Reply 15.

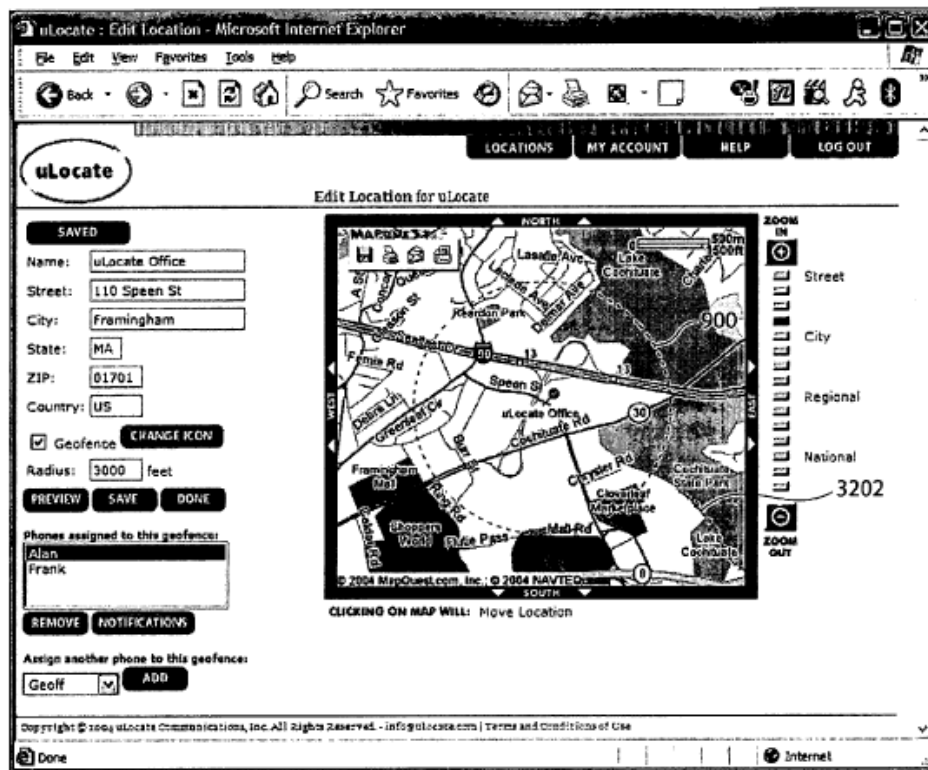


Fig. 32

Figure 32 of Phillips, reproduced above, purports to be a screenshot of a user interface that “shows a geofence.” Ex. 1007, 6:6.

Patent Owner argues, however, that “Phillips (like Fast), tracks mobile devices on a device-by-device basis, not a group basis.” PO Resp. 30.

Patent Owner argues Figure 32 does not depict group tracking because “each phone is linked to a *separate* event with a *separate* list of alert recipients.”

Id. at 14. According to Patent Owner, “Phillips makes this clear at Figure 36,” wherein “[e]ach phone is associated with different events even though Alan’s events and Geoff’s event are both defined in relation to the geofence zone “uLocate Office.” *Id.* at 14–15. Patent Owner further notes

“[t]ellingly, Fig. 36 does not have any row containing more than one tracked phone. This confirms that events and alerts are constructed and managed on an individual device-by-device basis in Phillips, not a group basis as

required by claim 1 of the '931 Patent.” *Id.* at 15. Figure 36 of the Phillips reference (Ex. 1007) is reproduced below.

3602

Alert for uLocate test

Location	Phone	Event	Alert Contacts	
uLocate Office	Alan	<=>	SMS: Alan Email: Jeremy email	Edit Delete
uLocate Office	Geoff	<=>	Email: Nina	Edit Delete
uLocate Office	Alan	<=>	SMS: Alan Email: Alan's email Email: Frank's email Email: Alan's work email	Edit Delete
Frank's Home	MAD	<=>	Email: Frank's email	Edit Delete
Frank's Home	Frank	<=>	Email: Frank's email	Edit Delete
uLocate Office	Stefan uWAM	<=>	SMS: Stefan's SMS Email: Alan's email Email: Frank's email	Edit Delete

Create New Alert

Fig. 36

Figure 36 of the Phillips reference, reproduced above, purports to depict “a graphical user interface that may be used to define alerts using the system.” Ex. 1007, 6:11–12.

Petitioner disagrees with Patent Owner’s view of these figures, and asserts that Figures 32 and 36 of Phillips “are independently illustrative rather than limiting each other.” Pet. Reply 17. Petitioner further argues Phillips “shows a ‘notifications’ button underneath the group of phones assigned to the geofence” as illustrated in Figure 32, and notes that Petitioner’s expert, Dr. Heppe, opines that Figure 32 shows that the locations of the phones in the group are intended to be compared to the defined geofence in order to generate an alert. *Id.* (citing Ex. 1011 ¶ 186). According to Petitioner, Dr. Heppe’s opinion is supported by Phillips’ references to handling “locations of all the users *in a defined group.*” *Id.* (citing Ex. 1007, 4:65–67, 6:1–2) (emphasis added).

For reasons similar to those stated above with regard to Fast's disclosure, we are not persuaded that a preponderance of the evidence shows that the combination of Fast with Phillips discloses the "group" features of claim 1. Nor do we lend much weight to Petitioner's expert declaration on this issue, as it does not address relevant record evidence. In particular, we find that Phillips, like Fast, discloses setting alerts and events on an *individual* basis, even though more than one individual may be tracked according to the same geofence zone. Although Petitioner and its expert point to statements in Phillips discussing "locations of all the users in a defined group" (Pet. Reply 17 (citing Ex. 1011)), those references are only with regard to displaying current locations of users in the group, such as on a graphical interface. See Ex. 1007, 4:65–67, 6:1–2; *see also* Figs. 28 and 29 and 5:66–6:2. Visually displaying the *current locations* for all users in a "defined group," as depicted in Phillips' Figures 28 and 29 (the group being "all" users), does not, however, disclose an interface for setting a zone (geofence) for a group, as claimed. For one thing, displaying current locations of users does not necessarily pertain to a geofence; current locations may be displayed without regard to a geofence, and Figures 28 and 29 of Phillips do not purport to depict geofences. Moreover, even if Phillips did disclose a visual interface depicting geofences relative to multiple users, such disclosure would not necessarily teach or suggest that the geofence was originally set *for a group comprising those multiple users*.

Nor does Petitioner point to teachings in Phillips of setting an event or an alert on a group basis. Rather, as noted above with regard to Figure 36, Phillips' disclosure of event and alert settings suggests that they are made on a device-by-device basis. And, as we find above in connection with Fast, an

interface that sets a zone, an event, and an alert on an individual device basis (as we find is disclosed by Phillips as well as Fast) does not fall within the scope of the '931 patent claims, even if the user may use that interface, seriatim, to repeat the same settings for multiple mobile devices that the individual subjectively considers to be part of a “group” and wishes to track using the same settings.

Group limitations—Fast combined with Phillips and Zou.

Petitioner also argues that combining Zou, which teaches fleet tracking, with Fast and Phillips satisfies the “group” features of claim 1. We are persuaded by these arguments.

As we discuss above, Zou’s disclosure overlaps substantially with that of Fast and Phillips, as all three references disclose location-tracking systems. Zou, in particular, discloses implementation of mobile-tracking devices “for vehicle fleet management.” *See, e.g.*, Ex. 1005 ¶ 78. Zou also provides for various levels of authority within the system and describes more detailed user interfaces in the context of implementing geofencing in fleet management. *See, e.g., id.*, Figs. 15g, 17a, 18b, 18c. Petitioner’s expert, Dr. Heppe, also opines that Zou “shows how to tailor a tracking and monitoring system for managing fleets.” *See* Ex. 1011 ¶¶ 68, 105–106. We find that testimony credible and afford it substantial weight.

As part of its disclosure of fleet management, Zou teaches “grouping” of vehicles as fleets so that users can “view data by fleet, control data collection parameters by fleet, and compare performance between fleets.” Ex. 1005 ¶¶ 190–192. Users may also select other users to “view the fleet group” and are enabled to “to set authority levels for the users who can view the fleet group.” *Id.*

Zou also discloses a graphic user interface (“GUI”) for creating a zone, an event, and an alert for a fleet with multiple vehicles. *See, e.g.*, Ex. 1005 ¶¶ 91, 203–211, Figs. 15d, 15i (geofence), 20a and 20b (“Manage Alerts”). According to Zou, the vehicles in a fleet may be tracked with the use of “telemetry devices,” which may be attached to the vehicle and which may include “GPS hardware.” *Id.* ¶¶ 80, 83, 95, 205. For example, Figure 18a of Zou, reproduced below, depicts a GUI with a menu “displayed to enable a user to assign vehicles to fleets.” *Id.* ¶ 191. As depicted, a fleet may be named and may comprise several different vehicles.

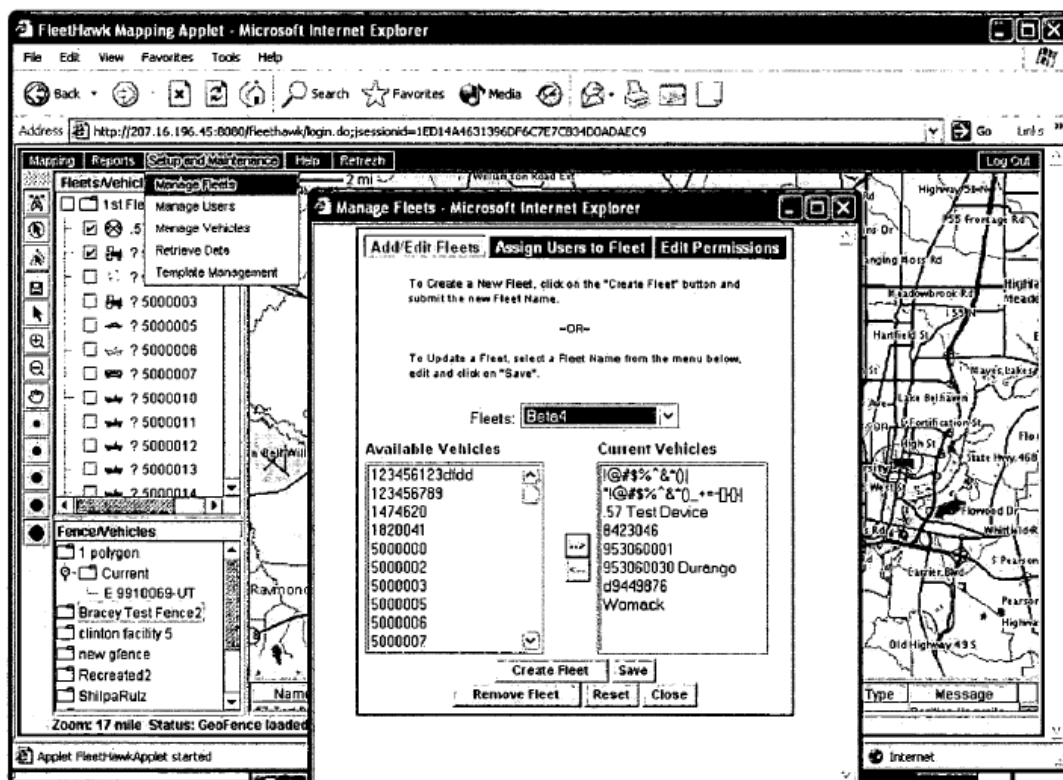


Figure 18a of Zou, reproduced above, “is a graphical screen depiction of a form displayed to enable a user to assign vehicles to fleets.” Ex. 1005 ¶ 58.

Zou also discloses a GUI for creating a “GeoFence” (zone) for a group of mobile devices (vehicles) having a boundary that is independent of where the group’s mobile devices are located. Ex. 1005 ¶¶ 204–211 (describing creation of “GeoFences”); *see also id.* at Fig. 13 (depicting user interface to set geofences). According to Zou, a user (depending on the user profile—that is, the user’s “permissions” as noted above) “may be able to create GeoFences for one or a *group of vehicles*.” *Id.* ¶ 206 (emphasis added). Figure 15i of Zou, reproduced in part below, depicts a GUI showing multiple “Fleets/Vehicles” with selection boxes (in which a grouping of two devices within “1st Fleet” is depicted with check marks) as well creation of a geofence:

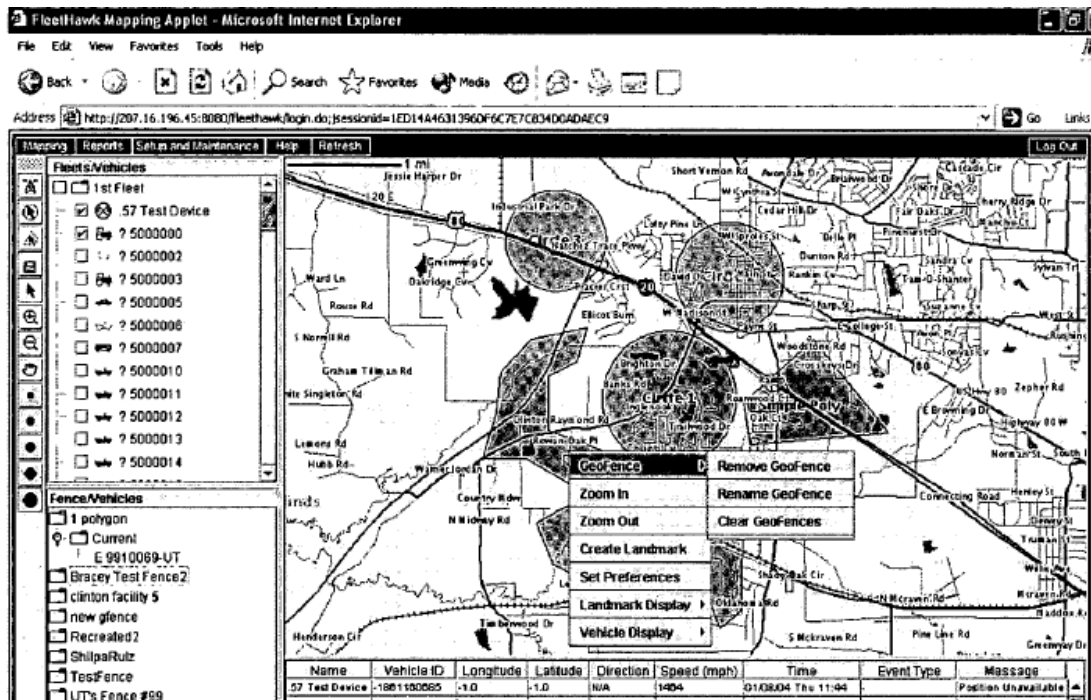


Figure 15i of Zou, reproduced in part above, is a “graphical screen depiction showing a pop up menu available upon a mouse right click on a GeoFence object on the map.” Ex. 1005 ¶ 47.

Zou also discloses setting alerts and events for a fleet. For example,

in Figure 20a reproduced below, Zou depicts a GUI for setting an alert for vehicles within a fleet as well as identifying a recipient of the alert:

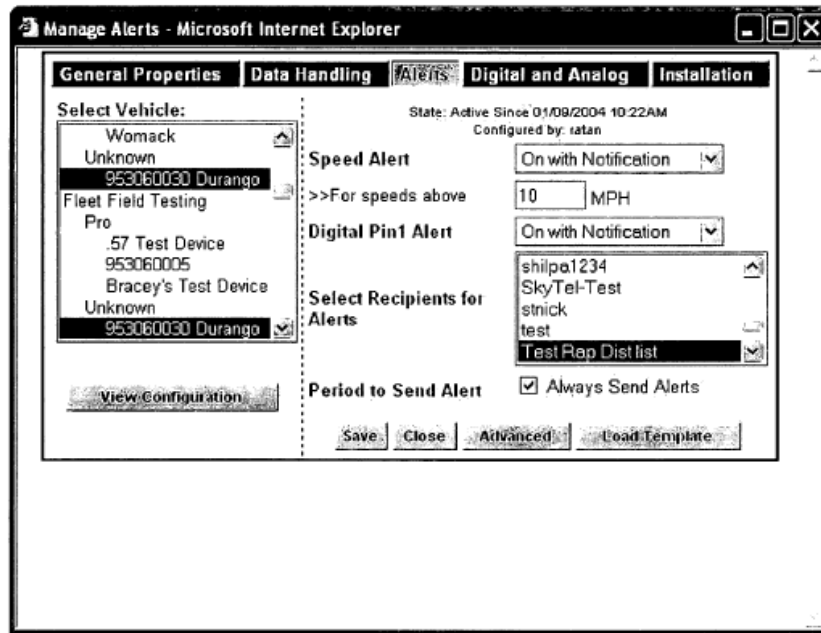


Figure 20a of Zou, reproduced above, “is a graphical screen depiction of a form displayed to collect information indicating a user preference for information to be collected regarding alerts.” Ex. 1005 ¶ 66.

Although the alert depicted in Zou’s Figure 20a is for speed, we find the ordinarily skilled artisan would understand that a similar GUI would be used to set a zone, event, and an alert for the group because this functionality is described in the specification. *See, e.g.*, Ex. 1005, Fig. 20a, ¶¶ 204–211. In that regard, we find credible the declaration statements by Petitioner’s expert on this topic, Ex. 1011 ¶¶ 132, 149, and we award them substantial weight. In addition, although Figure 20a shows only a single vehicle highlighted, Zou discloses that, per its user interfaces, multiple vehicles may be selected by “hold[ing] down the ‘Ctrl’ key on the keyboard while clicking each vehicle one at a time.” Ex. 1005 ¶ 172. Zou also discloses setting events by setting geofences, noting that “[u]sing GeoFences, the exemplary

system will record each time the vehicle(s) enters or exits the boundaries of the GeoFence. These ‘events’ can also, e.g., trigger the system to send alerts to provider pagers or email.” *Id.* ¶ 204. Zou’s interface as depicted in Figure 20a also allows selecting recipients for the alerts.

As noted above, we find the combination of Fast and Phillips teaches the limitations of independent claim 1, except, as we discuss above, for the “group” limitations. We find, however, that Zou makes up for this deficiency in the disclosures of Fast and Phillips by teaching a location-tracking system for tracking vehicles (such as a fleet of vehicles) on a “group” basis—including a user interface for setting a zone, an event, and an alert “for the group,” as recited in claim 1. We also find combining Zou’s disclosure of group-based monitoring and tracking with the disclosures of Fast and Zou would extend to encompass all of the “group” features as recited in claim 1. In that regard, we find persuasive the analysis and reasoning provided by Petitioner, and we adopt them as our own. Pet. 56–63.

Patent Owner argues, however, that Zou “performs threshold monitoring at remote telemetry devices only,” and this means that “Zou cannot perform threshold monitoring on a group basis, as required by Limitation 1[n].” PO Resp. 31. According to Patent Owner, in Zou “[e]ach remote telemetry device is attached to a single tracked vehicle, meaning that it can only perform threshold monitoring for that single vehicle — not a group of vehicles. Zou thus performs threshold monitoring on an individual device-by-device basis, not a group basis.” *Id.*

Patent Owner’s argument is not persuasive to rebut Petitioner’s arguments and evidence because it fails to address the combination relied

upon by Petitioner. As Petitioner notes, “Petitioner relies on Fast and Phillips (not Zou) for server-[side] threshold monitoring.” Pet. Reply 18. In addition, even if each of Zou’s telemetry devices monitors only a single vehicle, that does not detract from Zou’s teaching of group monitoring and tracking via Zou’s Network Operations Center (“NOC”), which “interacts with the telemetry devices **103** to exchange information for supporting fleet and asset management.” Ex. 1005 ¶ 103.

(c) Claims 23 and 24: checking privileges “when” adding devices / setting a zone, event, or alert

As addressed above, independent claim 1 requires checking first and second administrative privileges “before” taking the recited actions. Dependent claims 23 and 24 further require these privileges to be checked “when” taking the recited actions. The parties’ dispute over these claims is not over whether the claimed privileges are checked in the prior art, but rather whether they are checked “when” the recited actions are taken.

Petitioner argues Fast discloses these claims because Fast discloses that the administrative privileges “are checked at every login when the user communicates with the GMMS,” and also because “a user must login to add a beacon mobile device” as well as “for the purpose of setting a zone, an event, or an alert for the group.” Pet. 52–53 (citing Ex. 1003, 5:28–30 (portals access GMMS), Figs. 16-1 (subscriber account status checked, as well as other credentialing) 16-2, elements 523, 518)). Thus, according to Petitioner, Fast discloses checking the claimed privileges “when” performing the recited function in the situation in which the user logs in for the purpose of performing that recited function. We find this analysis and reasoning to be persuasive and we adopt it as our own. We also find credible the supporting testimony of Petitioner’s expert, Dr. Heppe, who

opines that logging in and setting a zone, an event, or an alert may happen within the same session (Ex. 1011 ¶ 233), and we afford that testimony substantial weight.

Petitioner also argues that, in addition to the same-session situation disclosed by Fast, it would have been obvious in light of the combination of Fast, Phillips, and Zou to perform the privilege checks at the time the function is implemented (e.g., adding a mobile device, setting a zone/event/alert) by setting a flag in software (such as at login) and rechecking the flag at the time of implementing the action. Pet. 52–53; Pet. Reply 21–22. As support, Petitioner relies on the testimony of Dr. Heppe, who explains that “[t]he privileges must be checked at one time or the other, and it does not matter which approach is used.” Ex. 1011 ¶¶ 229, 234. Thus, the ordinarily skilled artisan would consider it obvious to check the second-level administrative privileges when setting a zone, an event, or an alert for the group by relying on a flag or parameter set at login. *Id.* We find Dr. Heppe’s testimony to be credible and we afford it substantial weight. Dr. Heppe’s opinions are also consistent, for example, with Zou’s teaching that a user’s profile will indicate whether a user is allowed to take certain actions, thus suggesting that user profiles (and hence the users’ privileges) are checked “when” taking an action. See Ex. 1005 ¶¶ 205–206, 211.

Combining Phillips with Fast, Petitioner also argues “it would be obvious to add to the ‘access levels’ security functionality of Phillips to Fast’s system.” *Id.* (citing Ex. 1007, 9:7–14, 4:38–40, 25:48–50). We find this analysis and reasoning set forth by the Petitioner in support of this argument to be persuasive, and we adopt it as our own. We also find

credible the supporting testimony of Dr. Heppe, who opines that the ordinarily skilled artisan would have had reason to combine the teachings of Fast with Phillips to improve on Phillips's access privilege functionalities for implementation in an enterprise (Ex. 1011 ¶¶ 234–235), and we afford this testimony substantial weight.

We have reviewed Patent Owner's arguments with regard to claims 23 and 24, but we do not find them persuasive to rebut Petitioner's arguments and evidence. Patent Owner argues that checking user privileges when logging in "is a much simpler, one-size-fits-all process than checking administrative privileges when specific actions are taken," and thus disclosure of checking privileges *at login*, as Patent Owner contends is disclosed by the prior art, does not disclose the subject matter of claims 23 and 24. PO Resp. 28–29. As support, Patent Owner relies on the declaration of Dr. Schonfeld, who states that "it would not have been obvious to alter Fast's procedure of checking privileges at login only to the more complex computational system of checking privileges whenever specific actions are taken." *Id.* at 29 (citing Ex. 2010 ¶ 28). Dr. Schonfeld's opinion, however, lacks any analysis and is unsupported by the record, including any evidence indicating, for example, the relative complexity of checking privileges at login versus checking privileges at various points in the process. We, therefore, afford Dr. Schonfeld's testimony little weight. We further note that neither Patent Owner nor Dr. Schonfeld address Dr. Heppe's explanation of allowing privileges to be checked "when" performing an action by simply checking a flag that was set earlier, which is consistent with (for example) Zou's teaching of restrictive user profiles (*e.g.*,

Ex. 1005 ¶¶ 205–206, 211), and which does not suggest an increase in computational complexity. *See* Ex. 2011 ¶¶ 229, 233–236.

Patent Owner does not argue dependent claims 2–7, 12–16, 20, 22, 25, or 26 separately from independent claim 1.

(4) Conclusion Regarding Teaching/Suggestions of Prior Art

For the foregoing reasons, considering the evidence and arguments before us, we find that Petitioner has established that the combination of Fast, Phillips, and Zou teaches or suggests each element of the challenged claims. We now turn to the issue of whether Petitioner has established sufficient reasons for combining these references in the manner proposed.

c. Rationale To Combine

Petitioner’s expert, Dr. Heppe, provides rationales for combining Fast, Phillips, and Zou that we find credible, and we adopt that reasoning and analysis as our own. *See* Ex. 1011 ¶¶ 54–68. In particular, the ordinarily skilled artisan seeking to apply Fast’s and Phillips’ systems in the context of fleet management would have had reason to incorporate the functionality of Zou because Zou shows how to tailor a tracking and monitoring system in particular for managing fleets, as we find above. In addition, Fast’s hierarchical approach of wholesalers and subscribers maps to a Network Operations Center (“NOC”), as disclosed in Zou, that provides fleet management servers to various customers (acting as subscribers to the service). Similarly to how Zou’s NOC allows different companies to track their own fleets, Ex. 1005 ¶¶ 9, 111–113, and Fig. 3, a wholesaler in Fast creates subscriber accounts so that subscribers can independently track their own dependents/employees. *E.g.*, Ex. 1003 at 16:29–30, 24:56–65, 33:1–17, and Fig. 22.

Patent Owner does not dispute Petitioner’s showing of a rationale to combine with regard to Fast and Phillips, but argues that “a person of ordinary skill would not have been motivated to combine Fast and Zou.” PO Resp. 31. We have reviewed Patent Owner’s arguments with respect to the combination of Fast and Zou but we do not find them to be persuasive. In particular, Patent Owner argues “Fast teaches a hierarchical structure of predefined user types, including ‘subscribers,’ ‘wholesalers,’ ‘guardians’, etc. arranged in hierarchical fashion,” whereas “[b]y contrast, ‘[t]here are no predefined user hierarchies in Zou.’” *Id.* (citing Ex. 2010 (Schonfeld Decl.) ¶ 29). Patent Owner’s argument fails to acknowledge Fast’s express disclosure that a subscriber has the flexibility to add, delete, and update users, such as guardians, and assign them different levels of access to the various functions and information in the subscriber’s portal. *See, e.g.*, Ex. 1003, 42:14–52, Fig. 16. In that regard, we find credible the testimony of Dr. Heppe (Ex. 1011 ¶ 28) and we afford it substantial weight. Fast’s disclosures support a user-defined capability for Fast’s location-monitoring system, even though some other aspects of the system may be pre-defined. Similarly, because Patent Owner’s expert (Dr. Schonfeld) focuses solely on the pre-defined aspects of Fast’s system to the exclusion of the user-defined aspects—in particular, the capability of the subscriber to define levels of access of other users—we afford little weight to his testimony, as it ignores critical portions of the record evidence, as we discuss above.

In addition, to the extent Patent Owner asserts the references must be physically combinable to provide the requisite rationale to combine, such contention is legally erroneous. “It is well-established that a determination of obviousness based on teachings from multiple references does not require

an actual, physical substitution of elements.” *In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012); *see also In re Etter*, 756 F.2d 852, 859 (Fed. Cir. 1985) (en banc) (“Etter’s assertions that Azure cannot be incorporated in Ambrosio are basically irrelevant, the criterion being not whether the references could be physically combined but whether the claimed inventions are rendered obvious by the teachings of the prior art as a whole.”).

Accordingly, Patent Owner does not persuade us that Fast and Zou cannot be combined in the manner asserted. Rather, we credit the testimony of Petitioner’s expert that a skilled artisan would have had sufficient reason to incorporate Zou’s group-tracking features into Fast’s and Phillips’ similar location-tracking systems (Ex. 1011 ¶¶ 54–68), and we, therefore, find the Petition and supporting testimony of Petitioner’s expert witness provide a sufficient rationale to combine the teachings of Fast, Phillips, and Zou in a manner demonstrating the obviousness of the challenged claims. *See* Pet. 15–18 (Fast and Phillips), 56–57 (Fast and Zou); Ex. 1011 ¶¶ 54–68.

d. Secondary Considerations

Prior to making our ultimate conclusion regarding obviousness, we must consider Patent Owner’s proffered evidence of secondary considerations—specifically, evidence of licensing of the ’931 patent, which Patent Owner contends “amply rebuts the obviousness case.” PO Resp. 32. In particular, Patent Owner states the following companies “in the fleet-tracking industry” have taken licenses to the ’931 patent: Industrack LLC, Geotab Inc., Fleetronix, Navman Wireless, Teletrac, Inc., Telogis, Inc., TV Management d/b/a GPS North America, GPS Logic, Inc., Forward Thinking Systems LLC, LiveViewGPS, Inc., and thingtech LLC. *Id.* at 33. As Patent Owner notes, “this roster of licensees” includes “*all* of the companies who

brought this IPR proceeding.” *Id.* (emphasis added). Patent Owner argues that these companies “have shown that [the ’931 patent] is a valuable invention worth licensing.” *Id.*

To establish a secondary consideration, a patent owner must show a nexus “between the evidence and the merits of the claimed invention.” *Novartis AG v. Torrent Pharms.*, 853 F.3d 1316, 1330 (Fed. Cir. 2017) (quoting *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1246 (Fed. Cir. 2010)).

The only evidence submitted by Patent Owner in support of this argument is the Declaration of Patent Owner’s counsel, who attests that the ’931 patent along with “other patents in the same family” have been licensed to the companies identified above. Ex. 2011 ¶¶ 3, 4. As Petitioner notes, however, Patent Owner does not provide copies of any of the license agreements, despite Petitioner’s objection and request for copies of the agreements. Pet. Reply 24.

We find that Patent Owner’s mere identification of the existence of license agreements to a family of patents—whose terms have been withheld from Petitioner and not provided to the Board—provides little relevant evidence of non-obviousness of the invention claimed in the ’931 patent. Moreover, as Petitioner notes, all of the licensees identified by Patent Owner had been sued by Patent Owner for infringement of multiple patents, including the ’931 patent. Pet. Reply 22; Ex. 1027. As the Federal Circuit has observed, licenses intended to resolve litigation disputes are not strong evidence of non-obviousness because “it is often cheaper to take licenses than to defend infringement suits.” *In re Cree, Inc.*, 818 F.3d 694, 703 (Fed. Cir. 2016) (internal quotes omitted). And where, as here, “the licenses themselves are not even part of the record,” it is difficult to determine if “the

licensing program was successful either because of the merits of the claimed invention or because they were entered into as business decisions to avoid litigation, because of prior business relationships, or for other economic reasons.” *In re Antor Media Corp.*, 689 F.3d 1282, 1293–94 (Fed. Cir. 2012). The *Antor* case is particularly instructive, as it involved a situation very similar to the present proceedings:

Antor, beyond alleging the existence of a number of licenses, has not asserted any nexus between the merits of the invention and the licenses themselves. *See In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995). Antor merely lists the licensees and their respective sales revenue. The licenses themselves are not even part of the record. Antor provides no evidence showing that the licensing program was successful either because of the merits of the claimed invention or because they were entered into as business decisions to avoid litigation, because of prior business relationships, or for other economic reasons. The Board was thus correct in holding that the existence of those licenses is, on its own, insufficient to overcome the prima facie case of obviousness.

Id.

Similarly, here, because Patent Owner has neither made the licenses part of the record nor connected sufficiently the licenses to the merits of the claimed invention (as opposed merely to a business decision to avoid litigation), we find Patent Owner’s licensing evidence falls far short of the objective criteria necessary for weighing evidence of non-obviousness. *See Merck Sharp & Dohme Corp. v. Hospira, Inc.*, 874 F.3d 724, 730–32 (Fed. Cir. 2017) (holding that commercial success is a “fact-specific inquiry” in which “all the evidence” must be considered and weighed in an obviousness analysis).

e. Obviousness Conclusion

After considering all of the evidence of record, we determine that Petitioner has shown, by a preponderance of the evidence, that the subject matter of claims 1–7, 12–16, 20, and 22–26 of the '931 patent would have been obvious to a person of ordinary skill in the art at the time of invention in view of the combination of Fast, Phillips, and Zou.

D. Ground # 2: Anticipation of Claims 1–7, 12–16, 20, and 22–26 by Fast

Petitioner also asserts Fast, alone, anticipates the challenged claims, citing its analysis of Fast that we have addressed above. *See* Pet. 55–56. We do not find Petitioner's arguments persuasive because, as we note above in connection with Ground 3 (obviousness over Fast, Phillips, and Zou), we find that Petitioner has not proved by a preponderance of the evidence that Fast, alone, discloses the “group” features of claim 1, including as recited in limitations 1(g)–1(j) of claim 1. By extension, Petitioner has not shown that all elements of dependent claims 2–7, 12–16, 20, and 22–26 are disclosed by Fast. We, therefore, conclude that Petitioner has not proved that Fast anticipates claims 1–7, 12–16, 20, and 22–26.

E. Ground #1: Obviousness of Claims 1–7, 12–16, 20, and 22–26 in Light of Fast and Phillips

Petitioner also asserts that the combination of Fast and Phillips would have rendered obvious claims 1–7, 12–16, 20, and 22–26 of the '931 patent. Pet. 11–54.

With regard to Ground 2, Patent Owner argues that even if Phillips were prior art, “the combination of Fast and Phillips could not be used to invalidate the '931 claims because Phillips (like Fast) fails to disclose the “group” limitations of '931 claim 1.” PO Resp. 30. As noted above, Patent Owner further argues “Phillips (like Fast) tracks mobile devices on a device-

by-device basis, not a group basis. Thus, Phillips does nothing to overcome the ‘group’ deficiency in Fast.” *Id.* (citation omitted).

We do not find Petitioner’s arguments on this ground persuasive because, as we note above in connection with Ground 3 (obviousness over Fast, Phillips, and Zou), we find that Petitioner has not proved, by a preponderance of the evidence, that Fast, alone or combined with Phillips, teaches the “group” features of claim 1, including as recited in limitations 1(g)–1(j) of claim 1. By extension, Petitioner has not shown that all elements of dependent claims 2–7, 12–16, 20, and 22–26 are taught by the combination of Fast and Phillips. We, therefore, conclude that Petitioner has not proved that claims 1–7, 12–16, 20, and 22–26 are unpatentable for obviousness over the combination Fast and Phillips.

III. CONCLUSION

After considering the evidence and arguments presented, we determine that Petitioner has demonstrated by a preponderance of the evidence that challenged claims 1–7, 12–16, 20, and 22–26 of the ’931 patent are unpatentable for obviousness over Fast, Phillips, and Zou.

IV. ORDER

Accordingly, it is hereby:

ORDERED that claims 1–7, 12–16, 20, and 22–26 of the '931 patent are unpatentable;

FURTHER ORDERED that, because this is a Final Written Decision, any party to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

Case IPR2016-01278

Patent 9,071,931 B2

PETITIONER:

Vivek Ganti

Steven G. Hill

HILL, KERTSCHER & WHARTON, LLP

vg@hkw-law.com

sgh@hkw-law.com

perdiemIPR@hkw-law.com

PATENT OWNER:

Alan Whitehurst

Marissa R. Ducca

QUINN EMANUEL URQUHART & SULLIVAN, LLP

alanwhitehurst@quinnemanuel.com

marissaducca@quinnemanuel.com

PERDIEM-IPR@quinnemanuel.com

Robert Babayi

VECTOR IP LAW GROUP

robert@vectoriplaw.com