

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 IPR2016-01064
Patent 9,003,499 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. 9,003,499 B2 (Ex. 1001, “the ’499 patent”). TV Management, Inc., d/b/a GPS North America (“Petitioner”)¹ requested an *inter partes* review of claims 1, 3–6, 8, 11, 12, and 16–20 of the ’499 patent. Paper 5 (“Pet.”). We instituted *inter partes* review of all of the challenged claims (Paper 20, “Inst. Dec.”) because Petitioner 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 28, “PO Resp.”), and Petitioner followed with a Reply (Paper 37, “Reply”). 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 48 (“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, 3–6, 8, 11, 12, and 16–20 of the ’499 patent is unpatentable. See 35 U.S.C. § 316(e). We issue this Final Written Decision pursuant to 35 U.S.C. § 318(a).

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 11. The Board granted that motion on August 24, 2016. Paper 13. 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 26.

² An oral hearing in related Cases IPR2016-01061 and IPR2016-01278 occurred on the same day, with similar issues presented and argued.

II. BACKGROUND

A. Related Matters

The '499 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; 9,071,931; 9,119,033; 9,319,471; 9,485,314; 9,621,661; and 9,680,941.

In addition to *inter partes* review of the '499 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. IPR2016-01278 (the '931 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 '499 patent, along with the '207, '012, '166, and '931 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 '499 patent, along with the '012, '931, '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. The district court case is currently stayed pending resolution of this IPR proceeding and the related IPR proceedings.

B. The '499 Patent (Ex. 1001)

The '499 patent describes a system that conveys information related to an object to one or more users in “information-sharing environments.” Ex. 1001, 1:61–62, 5:27–38. According to the '499 patent, various technologies (such as Global Positioning Systems (“GPS”)) may be used to track the location of objects. *Id.* at 6:9–11. The objects tracked may be people (such as a child), vehicles (such as a semi-truck or a car), or other objects or animals (such as a crate or a dog). *Id.* at 6:24–27; *see also id.* at Fig. 1. The objects may be tracked relative to “user-defined zones.” *Id.* at

1:62–2:8, 5:10–14. The system also monitors “event[s],” which are, for example, instances when a tracked object enters or exits a zone. *Id.* at 1:64–2:3.

An “information-sharing environment,” as described in the ’499 patent, may include a family or group of friends or it may be larger (e.g., a company). *Id.* at 5:27–38. Multiple information-sharing environments may co-exist within a larger information-sharing environment. *Id.* at 5:33–35. 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. An administrator with privileges may configure an information-sharing environment by specifying authorized users and giving these authorized users their own privileges. *Id.* at 5:39–42. Various levels of administrator privileges may exist. *Id.* at 5:51–54.

Each information-sharing environment may be administered to manage conveyance of information among computing devices based on “user identification codes” and/or “group codes.” *Id.* at 5:65–67, 7:45–50. Such codes “may be managed by a control station or may be established based on user unique user identification,” and can be associated with “one or more groups, and one or more information access privilege classifications, etc.” *Id.* at 7:2–7. Based on these codes, conveyance of specified object location information may be limited to specified users. *Id.* at 7:45–67. Each user may be associated with a level of access, thereby limiting who may receive the location information. *Id.* at 2:45–3:3, 6:64–7:60.

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, i.e., an access privilege, with each user’s identification code. *Id.* at 10:30–54.

C. Challenged Claims

Petitioner challenges claims 1, 3–6, 8, 11, 12, and 16–20, of which claims 1 and 19 are independent. Challenged claim 1 is exemplary and is reproduced below.³

1. [a] A system for conveying a plurality of event information associated with a corresponding plurality of events that occur based on satisfactions of a corresponding plurality of specified event conditions related to locations of a corresponding plurality of mobile objects having a corresponding plurality of mobile object identification codes, [b] wherein each mobile object is associated with at least one location information source that provides a corresponding location information over a wireless network, said system comprising:
 - [c] one or more computer servers configured to create a plurality of information-sharing environments, [d] said plurality of information-sharing environments providing user interfaces for a plurality of authorized users over a network of computing devices, [e] said plurality of authorized users being associated with a corresponding plurality of authorized user identification codes, [f] wherein said plurality of information-sharing environments are configurable based on varying levels of administrator privileges, said varying levels

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

of administrator privilege comprising a first level of administrator privilege associated with a network administrator and a second level of administrator privileges associated with said plurality of authorized users, [g] said first level of administrator privilege being used in a first information-sharing environment to allow for configuring a plurality of event information-sharing environments within said first information-sharing environment independent of one another, [h] wherein said plurality of event information-sharing environments are configurable based on said second levels of administrator privileges for specifying the plurality of specified event conditions;

- [i] one or more access control systems that are configured to communicates [sic] with said one or more computer servers to control access to the plurality of information sharing environments, [j] wherein access control to the plurality of information sharing environments is based on access control codes requiring multiple levels of access control comprising a first level of access control and a second levels [sic] of access control, [k] wherein access to said first information sharing environment is controlled under the first level of access control based on access control codes associated with the plurality of authorized user identification codes, [l] wherein access to said event information sharing environments is controlled under the second level of access control to access the plurality of specified event conditions independent of each other based on a corresponding plurality of event information access codes that are associated with the plurality of authorized user identification codes; and
- [m] an administrator system in communication with said one or more computer servers adapted to configure a corresponding plurality of access privileges for the plurality of authorized users that specify the specified event conditions based on the plurality of event information access codes, wherein conveyance of the plurality of event information is managed based on the plurality of access privileges.

D. Instituted Grounds

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

- (1) Fast et al., U.S. Patent No. 7,327,258 B2, filed January 31, 2005, and issued February 5, 2008 (“Fast”) (Ex. 1003); and
- (2) Zou et al., 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
Fast	§ 102	1, 3–6, 8, 11, 12, and 16–20
Fast and Zou	§ 103	1, 3–6, 11, 12, and 16–20

Inst. Dec. 40.

III. 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 an *inter partes* review, we give claim terms in an unexpired patent their broadest reasonable interpretation in light of the specification of the patent in which they appear. *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (concluding the broadest reasonable construction regulation “represents a reasonable exercise of the rulemaking authority that

Congress delegated to the Patent Office”); 37 C.F.R. § 42.100(b). Under that standard, claim terms are presumed to have their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art in the context of the specification. *See In re Translogic Tech. Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). That presumption may be rebutted by a term defined in the patent specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). In the absence of such a definition, limitations are not to be read from the specification into the claims. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

1. “information access code” / “event information access code”

In the Institution Decision, we considered the construction of a generic “information access code” (as proposed by Petitioners), or the specific type “event information access code” (as proposed by Patent Owner). Inst. Dec. 8–9. As we noted therein, the construction of these terms raises the broader question of the nature of “access codes” as described and claimed in the ’499 patent. As a precursor to describing the specific types of “information access codes,” the ’499 patent specification describes generic “access codes” and how they may be associated with, and used to manage conveyance of, information in accordance with the claimed invention:

[A]ccess codes can be associated with information to manage the conveyance of the information to computing devices. Specifically, an object location information access code can be associated with object location information. A user-defined zone information access code can be associated with user-defined zone information and/or an object location event information access code can be associated with object location event information. These access codes can be used in various ways. In

one arrangement, *an access code specifies the individual users and/or groups of users having access to the information to which the access code is associated.* Such an access code would typically *include specific user identification codes and/or group codes.* For example, by a user logging into a computing device, a given user identification code is associated with the computing device. The user identification code may also be associated with one or more groups having corresponding group identification codes. *The user identification code and group identification code(s) are compared to those included in the access code whereby a match would indicate the user is authorized to receive the information.* As such, *the 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 (emphases added).

Although the '499 patent specification describes embodiments in which an “access code” is similar to a password in that it must be entered by a user into the user’s computing device “in order to be granted access to the information,” Ex. 1001, 7:61–8:3, the specification also describes embodiments in which “a user may be granted access to the [information] based on the [access code] *without having knowledge of the access code.*” *Id.* at 11:10–13 (emphasis added). With regard to an event information access code, for example, the specification states that “a user that defines an object location event can also associate an object location event information access code . . . and can thereby manage the conveying of the object location event information to one or more users.” *Id.* at 16:54–59. The specification further explains that an “object location event information access code determines which user(s) are conveyed the object location event information” because the user setting up the access code “specif[ies] individual users or groups allowed access to” that information. *Id.* at 16:59–62.

Thus, the specification describes an “information access code” as having different embodiments—not limited to a password, but also including an “access code” that may be associated with specific information and may be used to control access to that information by specifying which users have access to that information. In this context, the “access code” functions as an identifier that links specific information with one or more user identification codes for users that are authorized to receive the information. *See* Ex. 1001, 7:54–57: “The user identification code . . . [is] compared to those *included in the access code* whereby a match would indicate the user is authorized to receive the information” (emphasis added).

In light of the foregoing, we preliminarily construed the terms “information access code” / “event information access code” in our Institution Decision as encompassing

an identifier in the form of a name, number, or other series of letters, numbers, symbols, or the like, that is associated with specific information (such as “object location event information” in the case of an “event information access code”) and may be used to manage conveyance of that information by specifying which users are authorized to receive that information.

Inst. Dec. 11. Neither party disputed this preliminary construction during trial, or provided any further argument or evidence regarding the proper construction of these terms. We maintain our earlier construction of these terms.

2. “*authorized user*”

Prior to institution, the parties also disputed construction of the term “authorized user,” which appears in all of the independent claims of the ’499 patent. *See* Inst. Dec. 12. The specification describes users being “authorized” to receive information—for example, if their “user identification codes” are designated as being authorized to access that information:

In one arrangement, an access code specifies the individual users and/or groups of users having access to the information to which the access code is associated. . . . The user identification code and group identification code(s) are compared to those included in the access code whereby *a match would indicate the user is authorized to receive the information*. As such, the 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, 7:45–48, 7:54–60 (emphasis added). The specification further states, in one embodiment, “users may be granted access to the object location information based on the access code without having knowledge of the access code.” *Id.* at 10:62–65. The specification also states “an Internet service based on the present invention can be provided and administered such that anyone having access to the Internet can purchase the service and be an authorized user.” *Id.* at 5:54–57.

In light of the foregoing, we preliminarily construed “authorized user” in our Institution Decision as “a user who is given permission to access information.” Inst. Dec. 12. Neither party disputed this preliminary construction during trial, or provided any further argument or evidence regarding the proper construction of this term. We maintain our earlier construction of this term.

We do not need to further construe the claims to resolve the parties' present disputes. Thus, we decline to adopt further express constructions of the claim terms. *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 Prior Art

Petitioner asserts that the subject matter of one or more of claims 1, 3–6, 8, 11, 12, and 16–20 is anticipated by Fast and/or that the subject matter of one or more of claims 1, 3–6, 11, 12, and 16–20 would have been obvious under 35 U.S.C. § 103(a) over the combination of Fast and Zou.⁴ Pet. 6. 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.

⁴ Of note, with regard to claim 8, Petitioner asserts only anticipation by Fast and does not assert obviousness over the combination of Fast and Zou. Pet. 6.

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:

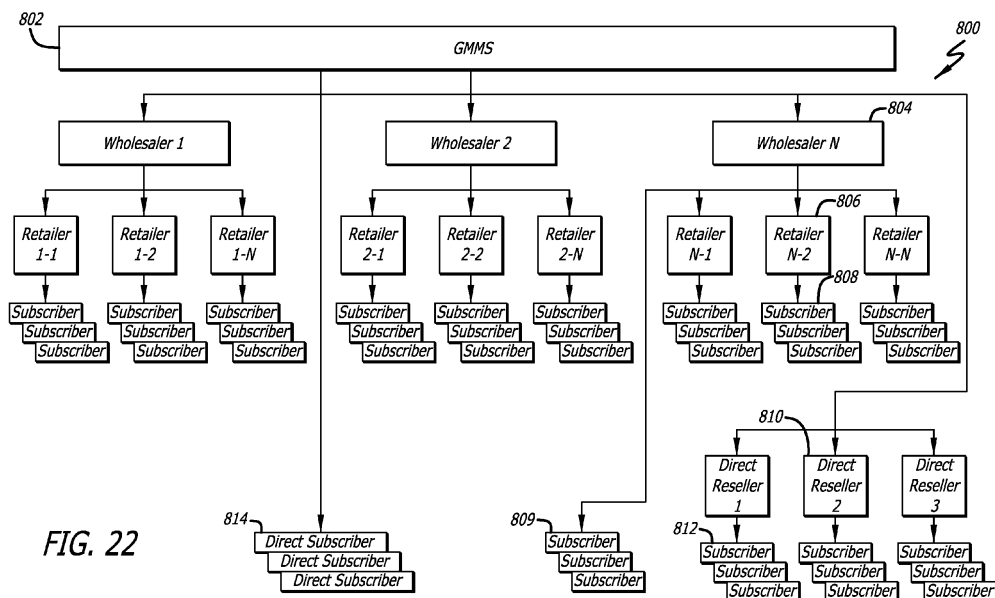


Figure 22 of Fast, reproduced above, is a schematic diagram showing the interrelationship between the GMMS, individual wholesalers, individual retailers, and individual subscribers in monitoring mobile items. Ex. 1003, 2:58–62. The GMMS refers to the overall system, within which wholesalers work with 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

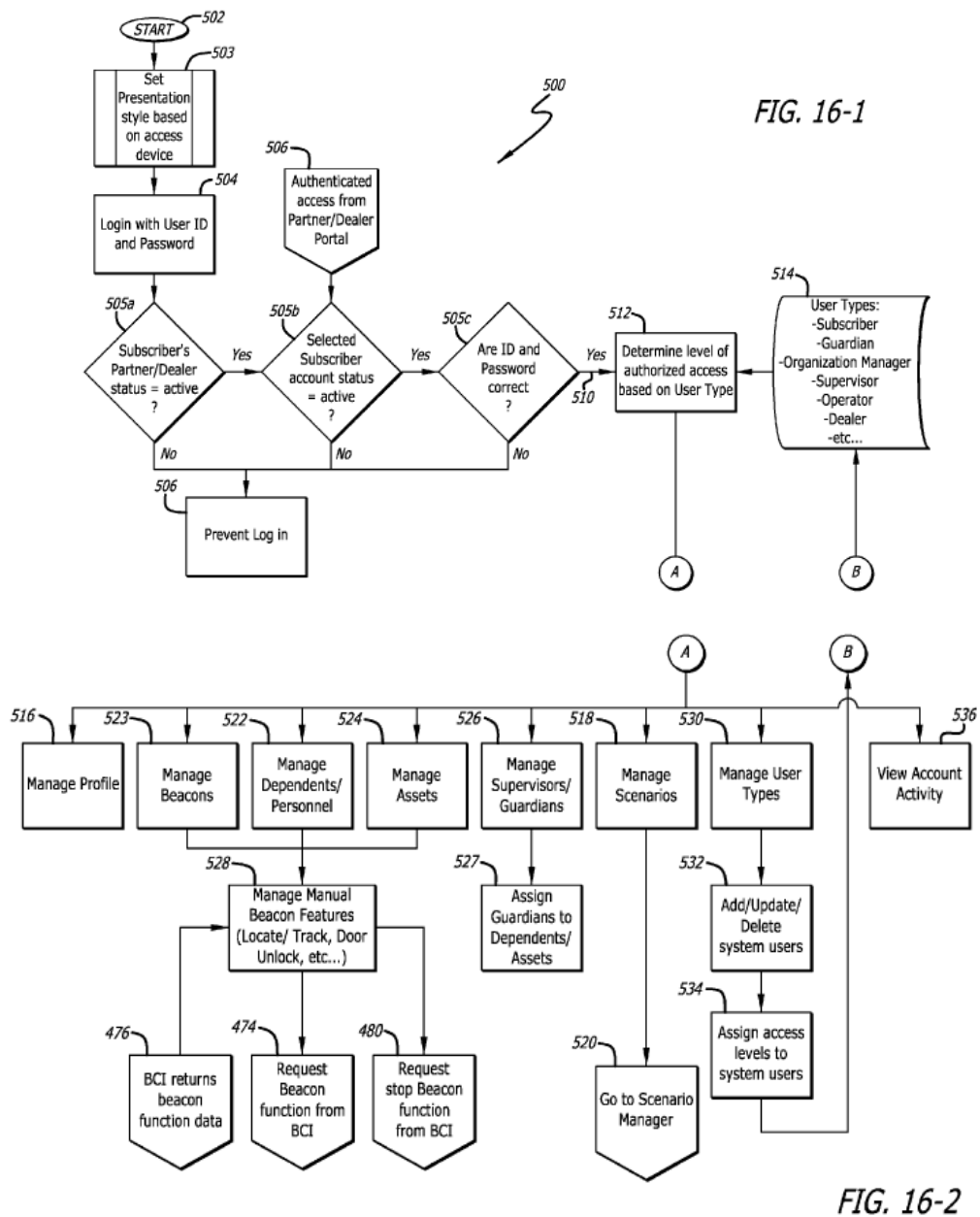
(e.g., vehicles). Ex. 1003, 24:56–65, 33:1–17. The subscriber may create zones, such as “allowed or disallowed zones,” to allow monitoring of the tracked items in particular areas, which may be activated or deactivated according to a schedule. *Id.* at 20:63–67. Subscribers may set up the GMMS software 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 administrators. *Id.* at 16:5–11, 37:44–38:54, Figs. 14-1 and 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, 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.

Figures 16-1 and 16-2 of Fast (reproduced below) depict the functionality available through the subscriber portal.



Figures 16-1 and 16-2 from Fast, reproduced above, “represent[] the functionality of the residential and commercial subscriber’s portal.”

Ex. 1003, 42:14–15.

As shown in block 504 of Figure 16-1, access to the subscriber portal is granted through login with the user’s “User ID and Password.” Block 512 of Figure 16-1 states that the “level of authorized access” is determined “based on User Type.” These “User Types,” which are listed in Block 514 of Figure 16-1, include “Subscriber” and “Guardian.” Viewed in light of the written description, Figure 16-2, which is a continuation through “A” and “B” of Figure 16-1, depicts that, *unless restricted*, a user has access to *all* of the functionality of the subscriber portal, including access to the “Scenario Manager” through blocks 518 and 520. *See* Ex. 1010 ¶ 48.

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. Zou

Petitioner contends that Zou is prior art under 35 U.S.C. § 102(e) and is a printed publication under 35 U.S.C. § 102(a). Pet. 5. 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.* at ¶ 12, communicating with a Network Operations Center (NOC), *id.* at ¶ 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.* at ¶ 113, Fig. 3. The presentation server provides functions including fleet and asset tracking and “general purpose I/O monitoring and control.” *Id.* at ¶ 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.* at ¶ 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.* at ¶ 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.* at ¶¶ 191–193, 202, 203, Figs. 18a, 18e.

C. Anticipation by Fast

Petitioner challenges claims 1, 3–6, 8, 11, 12, and 16–20 of the ’499 patent as anticipated by Fast. Pet. 15–40. 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 Fast anticipates the challenged claims. *Id.*; Reply 3–14; Ex. 1010.

1. Independent Claim 1

Patent Owner argues that independent claim 1 of the ’499 patent describes a “system for tracking the location of objects and determining whether certain events have occurred,” while protecting users’ privacy by using “tiered privileges and access codes,” which allow the claimed system to “protect the event information, while allowing authorized users more

freedom to configure the system to their specific needs.” PO Resp. 3–4. Patent Owner argues Fast does not anticipate the invention recited in claim 1 (which Patent Owner argues collectively with independent claim 19) because Fast’s system “conveys information according to a predetermined hierarchical structure, **not** a flexible user-defined structure.” *Id.* at 13. Focusing its arguments on limitations 1(k), 1(l), and 1(m), Patent Owner argues that Fast does not disclose those limitations because, collectively, they “require two levels of access control—an ‘authorized user identification code’ (AUIC) and an ‘event information access code[]’ (EIAC).” *Id.* at 2 and 18–22. As discussed more fully below, Patent Owner argues that Fast does not disclose these two levels of access control because Fast does not disclose any such access codes; instead, according to Patent Owner, the level of authorized access in Fast is “determined by predefined user type.” *Id.* at 18.

We discuss Patent Owner’s contentions more specifically in connection with limitations 1(k)-1(m) below. We also address the remaining limitations of claim 1, in order, for completeness and context.

Limitation 1(a) (preamble): “A system for conveying a plurality of event information associated with a corresponding plurality of events that occur based on satisfactions of a corresponding plurality of specified event conditions related to locations of a corresponding plurality of mobile objects having a corresponding plurality of mobile object identification codes,”

In essence, the preamble of claim 1 describes a system for conveying information associated with user-specified “events,” which are based on the locations of mobile objects satisfying certain conditions. *E.g.*, Ex. 1001, 1:62–2:8. Petitioner asserts Fast meets limitation 1(a) because:

Fast discloses a wireless network and system for using Beacons to convey a plurality of event information (*e.g.*, zone violation

notifications) associated with a corresponding plurality of events (*e.g.*, zone violations) that occur based on satisfactions of a corresponding plurality of specified event conditions (*e.g.*, a trigger mechanism and zone parameters defined in a scenario) related to locations of a corresponding plurality of mobile objects (*e.g.*, Beacons carried by dependents) having a corresponding plurality of mobile object identification codes (*e.g.*, Beacons IDs, dependent's names).

Pet. 21–22.

We find Petitioner's assertions are supported by Fast's disclosure. *E.g.*, Ex. 1003, Abstract, 4:9–11, 12:40–44, 26:5–23, 32:51–56. In particular, Fast discloses using 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, 24:56–65, 33:1–17. Users may be notified upon certain event conditions, such as a beacon reaching a specified location or entering or leaving a user-defined zone. *E.g.*, *id.* at 12:40–44, 32:51–56. As such, we find persuasive Petitioner's analysis of this element of claim 1, and we adopt Petitioner's reasoning as our own.

Patent Owner does not address limitation 1(a) in its Patent Owner Response.

Limitation 1(b) (preamble): “wherein each mobile object is associated with at least one location information source that provides a corresponding location information over a wireless network, said system comprising[]”

The preamble of claim 1 also requires, in essence, that each mobile object has a location information source that provides data over a wireless network. Petitioner asserts: “Fast discloses that each mobile object is associated with a location information source (*e.g.*, the Beacon/Beacon's GPS receiver) wirelessly transmitting its location information over a

network. A beacon typically contains a wireless location-determining module and a wireless communications module. The location determining module may be a GPS receiver.” Pet. 23 (citing Ex. 1003, 9:10–15). Patent Owner does not address limitation 1(b).

We find Petitioner’s assertions are supported by the cited disclosures of Fast. In particular, the beacons in Fast’s GMMS transmit location information (based, for example, on GPS information) over a wireless network. *E.g.*, Ex. 1003, 3:19–22, 9:10–15. As such, we find persuasive Petitioner’s analysis of this element of claim 1, and we adopt Petitioner’s reasoning as our own.

Limitation 1(c): “one or more computer servers configured to create a plurality of information-sharing environments,”

This limitation introduces the concept central to claim 1 of “information-sharing environments” (“ISE’s”) in which, for example, location and/or monitoring information regarding the mobile objects is shared.

Petitioner asserts Fast discloses limitation 1(c) because “Fast discloses one or more servers (*e.g.*, web server and application servers) configured to create a plurality of ISEs (*e.g.*, a wholesaler’s network, a subscriber’s network),” including “a web server farm to interface with client devices and an application server cluster to carry out the framework of the GMMS.” Pet. 23 (citing Ex. 1003, 14:37–50, Fig. 2, items 25 and 26). Petitioner also asserts:

Fast provides portals for users to access the functionality of GMMS. (*Id.*, p.34, 5:28-31). Fast describes that the Guardian Administration Portal in the GMMS is used to create and enable wholesalers. (*Id.* 37:44-38:4). An unlimited number of wholesalers can be enabled and each one is provided with its own

wholesaler portal to user as an interface for configuring ISEs. (*Id.*, p.18, FIG. 14-2 and p.39, 16:7-9). The Wholesaler may have numerous users, each with a different level of access privilege. (*See, e.g., Id.* 38:37-45).

Once a Subscriber Account has been created, a subscriber who has been authorized may log into his Subscriber Account through the subscriber portal using his user identification code. (*Id.*, p.52, 42:20-25). An authorized subscriber may track the location of any of his “dependents (family members) and personnel (organization members).” (*Id.*, p.52, 42:53-60). The subscriber can create an unlimited number of users for its Subscriber Account and assign an access level to the other users by restricting access to some functions of the subscriber portal for these other users. (*Id.*, p.52, 42:26-35; 42:47-52). These portals allow wholesalers, subscribers and other users to configure ISEs.

Pet. 23–24. We find persuasive Petitioner’s analysis and reasoning, which we agree are supported by the cited teachings of Fast, and, as such, we adopt them as our own.

In particular, Fast discloses that servers create information-sharing environments by, for example, setting up subscriber portals through which specific beacons may be assigned to track specific objects and report location information to servers, which in turn may automatically share certain information with specified individuals. Ex. 1003, 5:50–52 (servers), 44:16–24 (portals connected to servers), 42:14–52 (subscriber portal), 32:15–56 (information sharing). A subscriber portal disclosed by Fast is an “information-sharing environment,” as recited in claim 1, because that portal is an environment (including one or more users and one or more assigned location-tracking beacons) through which information may be shared.

Second, Fast also discloses that servers determine occurrence of events. 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" Ex. 1003, 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. Thus, we find that Fast discloses limitation 1(c).

Patent Owner does not expressly address this limitation in its Patent Owner Response.

Limitation 1(d): "said plurality of information-sharing environments providing user interfaces for a plurality of authorized users over a network of computing devices,"

Claim 1 also requires, in essence, that authorized users are able to access the information-sharing environments through user interfaces.

Petitioner asserts Fast discloses limitation 1(d) because:

Fast uses "portals" which are "privately accessible interface[s] to the GMMS for a particular subscriber, user, or user type. Portals are normally accessed using a web browser." (Ex. 1003, p.35, 5:28-30). Subscribers are authorized users who make up the ISEs. (*Id.*, p.39, 16:9-11; Ex. 1010, ¶¶ 75, 86-88).

Pet. 24.

We find Petitioner's assertions are supported by the cited disclosures of Fast and are persuasive, and we adopt Petitioner's analysis and reasoning as our own. We further find that the portals in Fast (such as the wholesaler portal and the subscriber portal), which are part of information-sharing

environments as we find above, provide user interfaces through which authorized users (e.g., wholesalers / subscribers) may perform various functions for their particular information-sharing environment. Ex. 1003, 38:26–54 (wholesaler portal), 42:14–43:11 (subscriber portal). Thus, Fast discloses limitation 1(d).

Patent Owner does not expressly address this limitation in its Patent Owner Response.

Limitation 1(e): “said plurality of authorized users being associated with a corresponding plurality of authorized user identification codes,”

Claim 1 also requires that authorized users are associated with “authorized user identification codes.” Petitioner asserts Fast discloses this limitation in the form of user IDs for the authorized users of the GMMS. Pet. 25. We agree. In particular, Fast discloses that portals (such as a wholesaler portal and a subscriber portal) are accessible via the Internet to authorized users who log in with a “User ID and Password.” Ex. 1003, Fig. 14-1 box 404, 16:9–11, 38:31–32 (wholesaler portal); *id.* Fig. 16-1 box 504 and 42:19–20 (subscriber portal). We find the user IDs for the authorized users in Fast are “authorized user identification codes,” as claimed.

Patent Owner does not address limitation 1(e), and, in particular, does not dispute that Fast’s user IDs are “authorized user identification codes.”

Limitation 1(f): “wherein said plurality of information-sharing environments are configurable based on varying levels of administrator privileges, said varying levels of administrator privilege comprising a first level of administrator privilege associated with a network administrator and a second level of administrator privileges associated with said plurality of authorized users,”

Limitation 1(f) describes the information-sharing environments as having two levels of administrative privilege—a “first level” associated with

a “network administrator” and a “second level” associated with “authorized users.”

Petitioner argues Fast discloses a “first level of administrator privilege associated with a network administrator,” as recited in claim 1, in two alternative ways: (1) “the wholesaler privilege to create users and manage subscribers”; and (2) “the subscriber’s privilege to define parents and guardians within a subscriber account OR add/update subscriber accounts.” Pet. 25–26. With regard to the claimed “second level of administrator privileges,” Petitioner argues Fast discloses “[a]t the subscriber level . . . the privilege to build scenarios . . . associated with said plurality of authorized users (*e.g.*, subscribers, guardians).” *Id.*; *see also* Reply 13. We agree with Petitioner’s analysis and reasoning and adopt it as our own.

As argued by Petitioner, 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 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; *see also* Pet. 25–26, Reply 4–7. Further analysis of Fast’s disclosure of different levels of administrative privilege, and the exercise of those privilege levels, is provided below in connection with limitations 1(k)–1(m).

Patent Owner argues claim 1 requires “[t]he network administrator is assigned a **first level** administrator privilege, and the authorized users are assigned **second level** administrator privileges.” PO Resp. 10. Patent Owner further argues “[t]he network administrator is **not** an authorized user.” *Id.* Patent Owner does not expressly challenge Fast’s disclosure of limitation 1(f), but raises this argument as a precursor to arguing, in connection with limitations 1(k)–1(l), that Fast discloses a system with user types that are predefined by an administrator, such that authorized users in Fast cannot exercise a second level of administrator privilege to specify event conditions. See PO Resp. 10–11, 15, 18–19. This argument is discussed below in connection with limitation 1(k)–1(l).

Limitations 1(g) and 1(h): “[g] said first level of administrator privilege being used in a first information-sharing environment to allow for configuring a plurality of event information-sharing environments within said first information-sharing environment independent of one another, [h] wherein said plurality of event information-sharing environments are configurable based on said second levels of administrator privileges for specifying the plurality of specified event conditions”

Claim 1 further requires, stated generally, that the first level of administrative privilege allows for creating independent event-information sharing environments, and the second level of administrative privilege allows for specifying event conditions within those environments.

As noted above, Petitioner argues Fast discloses “a first level of administrative privilege” at both the wholesaler and subscriber hierarchical levels. Petitioner’s arguments present two different configurations for the “first information-sharing environment”: a wholesaler-level information-sharing environment, which we refer to herein as “configuration 1,” and a

subscriber-level information-sharing environment, which we refer to herein as “configuration 2.” Pet. 26–28; Reply 4–6.

With regard to configuration 1, Petitioner argues that a wholesaler may exercise a first level of administrator privilege, in a first information-sharing environment (using a wholesaler portal), to create subscriber accounts, which are event information-sharing environments, and can add, update and delete subscribers. Pet. 26 (citing Ex. 1003, 38:26–39 (describing wholesaler login), 38:50–54 (describing a wholesaler managing subscriber accounts)); *see also* Reply 6. Petitioner also asserts the subscriber accounts are independently configurable in that the wholesaler may create separate subscriber accounts, and each subscriber may further configure its own account independently of other subscribers. Pet. 26–27; *see* Ex. 1003, 38:50–54 (wholesaler management of subscriber accounts), 42:47–52, 42:31–35, 43:1–11 (subscriber account configuration); *see also* Reply 6.

We agree that the first configuration argued by Petitioner (Fast’s disclosure of a wholesaler configuring subscriber accounts) teaches a first level of administrative privilege being used in an information-sharing environment to configure event information-sharing environments, as recited in limitation 1(g). An “information-sharing environment” disclosed by Fast includes a wholesaler portal, which is an environment in which a wholesaler may provide location monitoring services to multiple subscriber accounts. Ex. 1003, 16:29–30, Fig. 22. Fast’s subscriber portal, in turn, is an “event information-sharing environment” because it is an environment in which location information may be shared based on occurrence of events. *Id.* at Figs. 16-1, 16-2, 32:51–56, 42:36–41. Fast’s subscriber is authorized to

configure that event information-sharing environment, using a second-level administrative privilege (which is different from the first-level privilege to create and add users), by creating and managing scenarios using the Scenario Manager, in which specific beacons are monitored and specified people may be notified upon occurrence of events—if, for example, “the specified vehicle is outside of the specified zone, at the specified time.” *Id.*

Petitioner also relies on a second configuration (which we call “configuration 2”), in which Fast discloses that a subscriber may exercise a first level of administrator privilege through the subscriber portal by assigning guardians to create and manage scenarios, wherein the scenarios are event information-sharing environments. Pet. 31–32; Reply 4–6. We agree that Petitioner’s assertions are supported by Fast’s disclosure. For example, in Fast, a subscriber, acting as an administrator, may use the subscriber portal to add, delete, and manage other users, including guardians. Ex. 1003, 42:45–52. 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 (block 527, “Assign Guardians to Dependents/Assets”). Unless the subscriber restricts the guardian’s access to this functionality, 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,” which include the guardian as well the subscriber and/or another user. *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 of administrative privilege, in a first information-sharing environment (e.g., the subscriber portal), to allow for configuring event-sharing information environments because the subscriber may assign guardians to track dependents by using the Scenario Manager. A subscriber's assigning a particular guardian to track a particular dependent, for example, allows for configuring an event information-sharing environment at least because the subscriber is providing the guardian with the ability to create scenarios in the Scenario Manager. *See id.* And the scenarios are "event information-sharing environments" because they create event conditions by defining the parameters of what information will be gathered to be shared, with which users, and under what circumstances. *See id.* The guardian may configure the scenarios by exercising a second-level administrative privilege to specify event conditions, which is different from the first-level administrative privilege as noted above.

Patent Owner does not challenge Fast's disclosure of limitations 1(g) and 1(h), but argues, in connection with limitations 1(k)–1(l), that Fast discloses a system in which user types are predefined by an administrator, such that authorized users in Fast cannot exercise a second level of administrator privilege to specify event conditions. *See* PO Resp. 10–11, 15, 18–19. This argument is discussed below in connection with limitations 1(k)–1(l).

Limitation 1(i): "one or more access control systems that are configured to communicates [sic] with said one or more computer servers to control access to the plurality of information sharing environments,"

Claim 1 also requires "access control systems" to control access to the information-sharing environments. Petitioner argues limitation 1(i) is

satisfied by Fast’s disclosure of password-protected portals that communicate with servers:

Fast discloses one or more access control systems (*e.g.*, password protected portals) that are configured to communicate with said one or more computer servers to control access to the plurality of ISEs. According to Fast, a “portal is accessible via the Internet and is restricted, using password protection, to users that are authorized by the system administrators.” (Ex. 1003, p.39, 16:9-11). Users login using their user IDs. (*Id.*, p.50, 38:31-32). A POSITA would understand that Fast’s password protected portals allow users to communicate with web servers and applications servers to help create the ISEs. (Ex. 1010, ¶¶ 111-114; *see also*, Ex. 1003, p.34, 5:28-31, and 5:50-59).

Pet. 28–29. Patent Owner does not address limitation 1(i).

We find Petitioner’s assertions are supported by the cited disclosures of Fast. In particular, the information-sharing environments in Fast (*e.g.*, the wholesaler portal and the subscriber portal) communicate with the GMMS servers, and include access restrictions that require login with a user ID and password. Ex. 1003, 16:5–11, 37:44–38:54, Figs. 14-1 and 14-2 (wholesaler portal); *id.* at 6:21–23, 42:14–35, Figs. 16-1 and 16-2 (subscriber portal); *id.* at 5:50–51, 44:16–24, Fig. 1 (portals access GMMS servers through the Internet). We agree Fast’s disclosure of portals accessing GMMS servers through the Internet and including secure access restrictions discloses the required “access control systems” as recited in limitation 1(i) because these portals communicate with servers to limit (control) access to information-sharing environments to only those users having authorized login information.

Limitation 1(j): “wherein access control to the plurality of information sharing environments is based on access control codes requiring multiple levels of access control comprising a first level of access control and a second levels [sic] of access control,”

Limitation 1(j) recites “multiple levels of access control,” and introduces a “first level of access control” and a “second level[] of access control” that are further defined in limitations 1(k) and 1(l), respectively. As recited in limitation 1(k), the “first level of access control” is used to control “access to said first information sharing environment,” and, as recited in limitation 1(l), the “second level[] of access control” is used to control “access [to] the plurality of specified event conditions.” The parties’ arguments regarding the first and second levels of access control are addressed below in connection with limitations 1(k) and 1(l).

Limitation 1(k): “wherein access to said first information sharing environment is controlled under the first level of access control based on access control codes associated with the plurality of authorized user identification codes,”

As noted above, Petitioner relies on Fast’s multi-tiered architecture and asserts Fast discloses limitation 1(k) in at least two configurations: (1) configuration 1, wherein the wholesaler environment is a first information-sharing environment, in which the wholesaler serves as administrator, and the subscriber environment is a second information-sharing environment with subscribers as authorized users (Pet. 17–18; Reply 6–7); and (2) configuration 2, wherein the subscriber environment is the first information-sharing environment, in which the subscriber serves as administrator, and user-created scenarios, which may be created by guardians as authorized users, are second information-sharing environments (Pet. 18–21, 24–27; Reply 4–6).

With regard to configuration 1, Petitioner argues “Fast teaches that access to the first-ISE (*e.g.*, wholesaler environment) is controlled under the first level of access control (*e.g.*, the wholesaler’s user type) based on access control codes (*e.g.*, the IDs or password associated with the wholesaler user type).” Reply 6; Pet. 30; Ex. 1003, Fig. 14-1. Petitioner further argues “Fast also teaches that the wholesaler’s access control codes are associated with the plurality of [authorized user identification codes], such as subscriber ID codes.” Reply 7 (citing Ex. 1010 ¶ 126). In particular, Petitioner argues “the wholesaler’s user ID/password and the subscriber’s ID are associated when wholesalers log into their own portal (Fig. 14) to then manage subscribers using their subscriber IDs.” Reply 8; *see also, e.g.*, Ex. 1003, 38:26–54 (describing wholesaler portal and management of subscriber accounts).

With regard to configuration 2, Petitioner argues “Fast discloses that access to said first ISE (*e.g.*, subscriber’s environment) is controlled under the first level of access control (*e.g.*, the subscriber’s user type) based on access control codes (*e.g.*, the subscriber’s ID or password) associated with the plurality of authorized user identification codes (*e.g.*, Guardian IDs).” Reply 5. Petitioner further argues “[i]n Fast, the subscriber’s login User ID/password is associated with the authorized Guardian’s ID because a subscriber must log into the subscriber portal using his User ID/password (Ex. 1003, FIG. 16-1, item 504) before the subscriber can manage and assign guardians (*id.*, FIG. 16-2, items 526 and 527).” *Id.* In particular, according to Petitioner, “Fast uses a ‘guardian manager’ to allow a subscriber to create ‘an unlimited number of guardians’ and assign them user IDs such as phone

numbers, email addresses Thus, a subscriber ID/password is associated with Guardian IDs of the guardians created by the subscriber.” *Id.*

Patent Owner, however, argues “there is no ‘authorized user identification code’ in Fast.” PO Resp. 18. According to Patent Owner: “As its name confirms, the claimed [authorized user identification code (“AUIC”)] is a code that identifies an ‘authorized user’ (as opposed to the network administrator).” *Id.* Patent Owner appears to interpret Petitioner’s argument as equating the “authorized user identification code” in the wholesaler-level information-sharing environment with the *wholesaler’s* user ID or password. *Id.* Patent Owner then argues that this mapping would be incorrect because Fast’s wholesaler is the administrator, not the authorized user. *Id.* at 19. Patent Owner’s interpretation of Petitioner’s argument is incorrect. As Petitioner notes, with regard to the wholesaler-level information-sharing environment (configuration 1), “Petitioner equates access control codes to a wholesaler’s user ID/password and equates the AUIC to the *subscriber’s* ID.” Reply 8 (emphasis added); *see also* Pet. 30–31. With regard to the subscriber-level information-sharing environment (configuration 2, which Patent Owner does not expressly address in its Response), Petitioner equates access control codes with the subscriber’s user ID/password and equates the AUIC to a guardian’s ID. Reply 5.

We find, in both configurations argued by Petitioner, that Fast discloses a first information-sharing environment that has an administrator as well as one or more authorized users, wherein the first level of access control is the user type/user ID of the administrator (wholesaler for configuration 1 and subscriber for configuration 2) and the authorized user identification codes are IDs or passwords for authorized users (subscriber for

configuration 1, and guardian for configuration 2). In particular, we have discussed above how Fast's multi-tiered system has an administrator at both the wholesaler and the subscriber levels who may configure those information-sharing environments by, *inter alia*, creating/adding users, and allow for configuring event information-sharing environments. See Ex. 1003, 18:25–37 and Fig. 22 (multi-tiered system), 38:26–54 (wholesaler portal and management of subscriber accounts), *id.* at 20:57–62 (Guardian Manager), 34:22–28 (subscriber assignment of guardians), 42:15–52 (subscriber portal), Figs. 16-1, 16-2 (subscriber portal flow chart). Because these wholesaler and subscriber portals may be used to share location information and to control how, when, and with whom that information may be shared, they are each “first information-sharing environment[s]” as recited in claim 1. See *id.* Access to those portals is restricted in Fast to those with the proper user ID and password. *Id.* at Fig. 14-1 box 404, 16:9–11, 38:31–32 (wholesaler portal); *id.* Fig. 16-1 box 504 and 42:19–20 (subscriber portal). This restricted access to each portal is a “first level of access control” as claimed because it controls access to a “first information sharing environment.” This restricted access, requiring user IDs, is also “based on access control codes” because these user IDs are used to control access—that is, access to the portals is granted only to those submitting a proper user ID. *Id.*

Fast also discloses “access control codes associated with the plurality of authorized user identification codes.” First, with regard to what we have termed “configuration 1” (wherein the wholesaler acts as administrator and subscribers are authorized users), Fast discloses that the wholesaler's access control codes are associated with the plurality of authorized user

identification codes, such as subscriber IDs. In particular, Fast discloses this association by disclosing that each subscriber corresponds to a respective wholesaler. Ex. 1003, Fig. 22. The wholesaler may update a subscriber, who has a user ID/password, by using the wholesaler's own user ID/password (access control code) to log into the wholesaler portal. *Id.* at 38:46–54. This shows an association between the wholesaler's ID/password and the subscriber's ID. Similarly, considering “configuration 2” (wherein the subscriber acts as administrator and guardians are authorized users), Fast discloses the subscriber's login User ID/password is associated with the authorized guardian's ID because a subscriber must log into the subscriber portal using his User ID/password before the subscriber can manage and assign guardians. *Id.* at Fig. 16-1, item 504, and Fig. 16-2, items 526 and 527. Fast also discloses a “Guardian Manager” that allows a subscriber to create “an unlimited number of guardians” and assign them user IDs such as phone numbers and/or email addresses. *Id.* at 20:57–62. Thus, a subscriber ID/password is “associated with” the IDs of the guardians created by the subscriber.

Patent Owner argues that Fast fails to disclose “authorized user identification codes” as claimed because, according to Patent Owner, Fast discloses that the level of authorized access “is determined by a predefined user type.” PO Resp. 18. In other words, according to Patent Owner, “[a]ll of the subscribers in Fast are *treated the same based on the user type*. Therefore, it is not possible to authorize certain subscribers based on an AUIC.” PO Resp. 19 (emphasis added). Patent Owner's reading of Fast is untenable. As Petitioner notes:

Patent Owner confuses “user types” with specific users. Using the portal of FIG. 14, a wholesaler can create any number of

subscribers under the wholesaler's account. (Ex. 1003, FIG. 22, FIG. 14-2, item 416; *id.*, 38:46-54). Even though all subscribers have the same "user type," each subscriber will be assigned different levels of access such that each subscriber can access his own account but not the account of other subscribers. (See Ex. 1010 ¶¶45-47; Ex. 1003, 18:25-37). *Because each subscriber has access to only his own account, each subscriber is uniquely defined and protected.*

Reply 8 (emphasis added). Petitioner's analysis is persuasive and we adopt it as our own. Indeed, the purpose of individual subscriber accounts in Fast—each having password-protected access to its own portal—would be defeated if, as Patent Owner contends, all subscribers were treated "the same based on the user type." Under Patent Owner's interpretation of Fast, every user of the same type could see the same information for everyone else of that same user type—thus, one "subscriber" could see the locations of all other mobile objects (such as dependents) being tracked by other subscribers. That interpretation is unreasonable, and is contradicted by Fast as noted above.

In addition, as noted, Patent Owner's argument does not address the subscriber-level information-sharing environment (configuration 2), in which the subscriber acts as an administrator and authorized users include guardians, each having a user ID and password. See Reply 4–6, 9–10. In that regard, Fast discloses customization of users associated with a particular subscriber's account through the subscriber's portal, which allows "managing the different User types," such that "[f]or each User, the subscriber can assign an access level 534 indicating what functionality they will be restricted from using." Ex. 1003, 42:41–44, 48–52. Thus, as Petitioner's expert witness opines, an ordinarily skilled artisan would understand Fast as disclosing that a subscriber may, for example, allow one

guardian to access the Scenario Manager in that subscriber's portal, while restricting access by another guardian; the subscriber may also assign different dependents to different guardians and limit each guardian's access to location information regarding each dependent. See Ex. 1010 ¶¶ 48, 94, 98, 101. We agree with that analysis and adopt it as our own.

Limitation 1(l): "wherein access to said event information sharing environments is controlled under the second level of access control to access the plurality of specified event conditions independent of each other based on a corresponding plurality of event information access codes that are associated with the plurality of authorized user identification codes"

Limitation 1(l) describes, in essence, a second level of access control, which controls access to "event information sharing environments" by using "event information access codes" to access the "specified event conditions."

Petitioner asserts Fast discloses limitation 1(l) by disclosing that subscribers (or guardians authorized by the subscriber) build "scenarios" and select "notification schemes" to notify suitable entities when a scenario is triggered. See Pet. 31–32. In particular, Petitioner asserts:

Part of building a scenario involves selecting a notification scheme name that references the desired recipients. (*Id.*, p.13, FIG. 11-1, R. 276 and 278). By selecting a notification scheme, the system knows which users are to be given access to notifications generated as a result of the scenario being triggered. (*Id.*, p.49, 35:46-51; see also 36:34-41). Thus, a POSITA would understand Fast's notification scheme name to be an event information access code when it is used to build an event-triggered scenario. (Ex. 1010, ¶ 135).

Id. at 32.

Patent Owner argues that Fast's "notification scheme name" cannot be an event information access code ("EIAC"), as claimed, because Fast's "notification scheme name is merely a shorthand for the event itself. It has

nothing to do with whether the event has occurred, and it certainly is not used to control whether a subscriber can access this information.” PO Resp. 21. We disagree, and note that Patent Owner’s argument is inconsistent with our construction of “information access code” as stated in our Institution Decision at 10–11 and also discussed above. In particular, we construe “information access code” to encompass a series of letters, numbers, or symbols, or other identifier, that is associated with specific information (such as “object location event information” in the case of an “event information access code”) and may be used to manage conveyance of that information by specifying which users are authorized to receive that information. Similarly, we construe an “event information access code,” as recited in claim 1, as encompassing an identifier associated with event information that may be used to manage conveyance of that information to specified users.

We find Fast’s disclosure falls within this construction. In particular, a “notification scheme name” is an identifier associated with the user-specified event information, and it is used to specify which users will receive notifications triggered by the specified event. Ex. 1003, 35:46–51, 36:34–41; *see also* Pet. 31–32. When building a scenario in Fast, the user selects a notification scheme to be part of the scenario. *Id.* at Fig. 11-1, item 278 (“select a notification scheme”). The notification scheme number is not, as Patent Owner argues, a “shorthand for the event” (PO Resp. 21), but is rather a shorthand for those entities who will be notified in response to the occurrence of an event. Ex. 1003, 36:36–38 (stating “[t]he notification scheme **276** (see also **276** in FIG. 11) specifies what messages are sent to what entities using what notification methods”). Thus, by identifying the

subscriber as a recipient (*id.* at 35:49–50), the notification scheme number is used to control whether a subscriber can access location information.

Patent Owner also argues:

[T]he claims specify that the authorized user has second level administrator privileges, *see* limitation 1(f), and these second level administrator privileges are used to configure the [event information-sharing environments (“E-ISEs”)] and specify event conditions, *see* limitation 1(h). Therefore, the authorized user has to be someone with the capability to access and configure the E-ISE, not merely the recipients of a notification scheme.

PO Resp. 20. Patent Owner’s argument assumes, incorrectly, that Petitioner reads “authorized user” on just a recipient of a notification scheme. In fact, Petitioner reads “authorized user” on entities that *configure* the event information-sharing environment by building scenarios and selecting notification scheme names. In particular, Petitioner argues that “when the administrator is a wholesaler,” as in the wholesaler information-sharing environment (configuration (1)), “the authorized user is a subscriber.”

Reply 10. And “when the administrator is a subscriber,” as in the subscriber-level information-sharing environment (configuration (2)), “the authorized user is a guardian.” *Id.* In both configurations, the authorized user (a subscriber or guardian) may configure the event information-sharing environment by building a scenario and selecting a notification scheme. *See* Ex. 1003, Fig. 16-1 (subscriber portal), Figs. 11-1 and 11-2 (Scenario Manager), 32:15–56, 34:36–37, 35:8–36:41; *see also* Pet. 31–32.

Patent Owner also argues there is no “event information access code” in Fast because that code must be “specified by the authorized user when it configures the EISE,” and Fast has only “predefined user type[s]” such that “it is not possible to use the subscriber user type to limit the other

subscribers' access to the event information.” PO Resp. 20–21. This argument appears to be premised on the incorrect assumption that Petitioner reads the claimed “event information access code” on Fast’s “user type.” To the contrary, as noted above, Petitioner equates Fast’s “notification scheme name” with the claimed “event information access code.” See Pet. 31; Reply 12. As noted above, we find that Petitioner’s assertion is supported by Fast’s disclosure and our claim construction, and we have adopted that analysis as our own.

Limitation 1(m): “an administrator system in communication with said one or more computer servers adapted to configure a corresponding plurality of access privileges for the plurality of authorized users that specify the specified event conditions based on the plurality of event information access codes, wherein conveyance of the plurality of event information is managed based on the plurality of access privileges”

The final limitation of claim 1 describes, in essence, an “administrator system,” in which conveyance of event information is managed based on authorized users’ “access privileges.”

Petitioner asserts Fast discloses limitation 1(m) because:

Fast discloses an administrator system (*e.g.*, a computing device employing the subscriber portal) in communication with said one or more computer servers (*e.g.*, web servers and application servers of FIG. 2) adapted to configure a corresponding plurality of access privileges for the plurality of authorized users (*e.g.*, subscribers and subscribers who add guardians, and operators) that specify the specified event conditions based on the plurality of event information access codes, wherein conveyance of the plurality of event information (*e.g.*, notifications generated from a scenario being triggered) is managed based on the plurality of access privileges.

Pet. 32. In particular, Petitioner asserts Fast discloses “[t]he subscriber portal allows subscribers to configure access privileges specified for other

authorized users such as guardians.” Pet. 33 (citing Ex. 1003, 42:47–52, 43:1–11, Fig. 16). Petitioner further asserts Fast discloses “[a]ccess to the subscriber’s portal allows access to the scenario manager,” and thus Fast discloses “configuring access privileges for the plurality of authorized users that specify the specified event conditions based on the plurality of event information access codes.” Pet. 33 (citing Ex. 1003, Fig. 19; Ex. 1010 ¶¶ 143–149). Petitioner further asserts Fast’s guardians may be authorized users who may manage scenarios:

The subscriber portal is accessible to both wholesalers (See Ex. 1003, FIG. 14-1, item 418 “access subscriber portal”), as well the subscriber/subscriber’s guardians (*id.*, FIGS. 16-1 and 16-2). Fast discloses “authorized users” by describing the creation, control, and management of “guardians.” (See Petition, p.19; Ex. 1003, 42:48-52, FIG. 16-2, item 534; Ex. 1010, ¶¶48, 98). Fast also teaches a Guardian Manager. A subscriber can make a guardian an authorized user who may manage the subscriber’s scenarios (Ex. 1003, 43:1-11; *see also id.*, FIG. 16-1, items 512 and 514 showing a guardian user type having access to the scenario manager in FIG. 16-2, item 518; Ex. 1010, ¶149).

Reply 13.

Patent Owner argues Fast does not disclose limitation 1(m), which Patent Owner characterizes as allowing “an authorized user to configure the E-ISE if they have the necessary access privileges based on the EIAC,” because Fast’s “level of authorized access” is “determined by a predefined user type.” PO Resp. 21. In particular, with regard to Petitioner’s assertion that subscribers are “authorized users,” Patent Owner argues “in Fast, all of the subscribers are *treated the same based on the user type*. Therefore, it is not possible to authorize a subset of the subscribers.” *Id.* at 21–22 (emphasis added). Patent Owner also argues Fast does not disclose limitation 1(m)

because Fast fails to disclose an “event information access code,” as Patent Owner argues in connection with limitation 1(l). *Id.* at 21.

As noted above, we find Patent Owner’s reading of Fast—treating all subscribers “the same based on the user type”—to be untenable. At a minimum, as Petitioner notes, “each subscriber has unique privileges to manage only his own account, where such privileges are defined when a Wholesaler creates a subscriber.” Reply 14. We agree with Petitioner’s analysis and adopt it as our own. We find, for example, that the ordinarily skilled artisan reading Fast would understand that a subscriber in Fast’s system would have access privileges to create scenarios with notification schemes to track beacons associated with that subscriber’s *own* account, but would not have access privileges to track beacons associated with a *different* subscriber’s account. *See* Ex. 1003, 20:42–45 (noting that the Beacon Manager “provides the subscriber with a view of all of the beacons *associated with their account*”), 47:8–29 (noting that access to a subscriber’s portal is restricted “to maintain the *security and privacy of the subscriber*,” while allowing for operator overrides “in case of emergency”) (emphases added); *see also* Ex. 1010 ¶¶ 98, 101 (describing independence and privacy of Fast’s individual subscriber accounts). Thus, contrary to Patent Owner’s assertion, Fast does not treat all subscribers “the same” because, *inter alia*, different subscribers may be authorized to track different beacons.

In addition, as we have found above in connection with limitation 1(k) and “configuration 2,” Fast’s multi-tiered architecture supports viewing a subscriber as an administrator and guardians assigned to that subscriber’s account as authorized users. Ex. 1003 at 20:57–62 (Guardian Manager), 34:22–28 (subscriber assignment of guardians), 42:15–52 (subscriber

portal), Figs. 16-1, 16-2 (subscriber portal flow chart); *see also* Reply 4–6. In that subscriber-level information-sharing environment (configuration 2), the subscriber may, for example, assign one guardian to track one dependent, while assigning a different guardian to track a different dependent. *See* Ex. 1010 ¶¶ 46–47. As Petitioner’s expert witness, Dr. Heppe, explains, “If different guardians are chosen and assigned, then the guardians’ access may be limited only to those children with beacons who are assigned to them.” *Id.* at ¶ 47. Patent Owner does not address this configuration other than generally arguing that Fast allows only pre-defined user types such that all user types are treated “the same.” *E.g.*, PO Resp. 15–17, 19, 21. As noted, we find that reading of Fast to be untenable and incorrect.

For the foregoing reasons, we find by a preponderance of the evidence that Fast discloses all limitations of claim 1, and, thus, anticipates claim 1.

2. Claims 3–5

We have considered fully the evidence and arguments presented by Petitioner explaining how claims 3–5 are also anticipated by Fast. Pet. 33–36. Patent Owner does not address claims 3–5.

We find Petitioner’s evidence and arguments persuasive, and we adopt Petitioner’s reasoning as our own. Accordingly, we determine that the preponderance of the evidence weighs in favor of Petitioner’s proof that, like claim 1 above, claims 3–5 also are unpatentable as anticipated by Fast.

3. Claims 6 and 11

Claims 6 depends from claim 1 and claim 11 depends from claim 6. Ex. 1001, 24:1–46, 24:64–65. Claims 6 and 11 recite “group identification codes” and “grouping configurations.” *Id.* We have considered fully the

evidence and arguments presented by Petitioner explaining how dependent claims 6 and 11 are also anticipated by Fast. Pet. 36–38.

As Petitioner asserts, Fast’s user-defined “scenario names” correspond to the claimed “user group identification codes”:

Fast discloses a system wherein said plurality of identification codes are associated with a plurality of user group identification codes (saved scenario names) in the one or more data bases under a plurality of grouping configurations (*e.g.*, associating users with particular scenarios) associated with said plurality of specified event configurations (*e.g.*, the parameters of the scenario) for the plurality of mobile objects (*e.g.*, tracked dependents having beacons). Fast explains that scenarios are named and saved in a database. (Ex. 1003, p.49, 36:1-6). Each named scenario is a group ID code. (Ex. 1010, ¶ 162). A scenario associates a mobile device ID code of the dependent being tracked (*id.*, p.13, FIG. 11-1, boxes 254, 256) with one or more selected recipients for the notification (*id.*, p.14, FIG. 11-2, box 284; *see also* p.49, 35:46-51).

Pet. 36–37. Patent Owner does not address claims 6 and 11.

We find Petitioner’s evidence and arguments persuasive, and we adopt Petitioner’s analysis and reasoning as our own. Accordingly, we determine that the preponderance of the evidence weighs in favor of Petitioner’s proof that, like claim 1 above, claims 6 and 11 also are unpatentable as anticipated by Fast.

4. Claim 8

Claim 8 depends from claim 1, and recites: “further comprising one or more computing devices remote from the plurality of mobile objects adapted to determine occurrence of events based on the plurality of specified event conditions.” Ex. 1001, 24:47–50.

We have considered fully the evidence and arguments presented by Petitioner explaining how Fast discloses each of the elements of claim 8. In

particular, Petitioner asserts Fast discloses “one or more computing devices” in the form of an “application cluster”—that is, applications running on servers. Pet. 37; *see also* Ex. 1003, Fig. 2 (depicting “application server cluster”). As Petitioner asserts, “Fast explains that an applications server cluster, which may be implemented on a J2EE platform, provides the GMMS functionality.” Pet. 38 (citing Ex. 1003, 14:44–56). Petitioner further asserts:

Fast describes the threshold monitoring may occur within the Beacon Manager, which is a software entity that processes on the central servers (remote from the objects). (Ex. 1010, ¶ 43). Fast also explains that a Scenario Monitor is responsible for listening to trigger reports received from beacons. (Ex. 1003, p.49, 36:12-18). The trigger report passes certain parameters relating to the trigger mechanism. (*Id.*). Upon receiving a trigger report, Fast explains that the parameters in the trigger report are compared to an active schedule of an active scenario. (*Id.*, p.49, 36:26-29).

Pet. 37. Petitioner also asserts: “The fact that the processing may occur in the Beacon Manager, and that reports are received away from beacons[,] shows remote processing away from the tracked mobile devices.” Pet. 38. We have considered fully the evidence and arguments presented by Petitioner. We find Petitioner’s evidence and arguments persuasive, and adopt Petitioner’s analysis and reasoning as our own. Patent Owner does not address claim 8 in its Patent Owner Response.

Accordingly, we determine that the preponderance of the evidence weighs in favor of Petitioner’s proof that claim 8 is also unpatentable as anticipated by Fast.

5. *Claim 12*

Claim 12 depends from claim 11, which in turn depends from claim 6. Ex. 1001, 24:66–67. We have considered fully Petitioner’s arguments and evidence regarding anticipation of claim 12 by Fast. Pet. 38–39. We find Petitioner’s evidence and arguments persuasive, and adopt Petitioner’s analysis and reasoning as our own. Patent Owner does not address claim 12.

Accordingly, we determine that the preponderance of the evidence weighs in favor of Petitioner’s proof that claim 12 is also unpatentable as anticipated by Fast.

6. *Claims 16–18*

Claims 16 and 17 depend, directly or indirectly, from claim 6 (Ex. 1001, 25:9–14), and claim 18 depends from claim 1 (*id.* at 25:15–18). We have considered fully Petitioner’s evidence and arguments regarding anticipation of claims 16–18 by Fast. Pet. 39–40. We find Petitioner’s evidence and arguments persuasive, and adopt Petitioner’s analysis and reasoning as our own. Patent Owner does not address claims 16–18.

Accordingly, we determine that the preponderance of the evidence weighs in favor of Petitioner’s proof that claims 16–18 also are unpatentable as anticipated by Fast.

7. *Claims 19 and 20*

Claim 19 is independent and claim 20 depends from claim 19. Ex. 1001, 25:19–26:39. We have considered fully Petitioner’s arguments and evidence regarding anticipation of claims 19 and 20 by Fast, which incorporate Petitioner’s arguments for claims 1 and 6. Pet. 40. For the reasons set forth above regarding claim 1, we find Petitioner’s evidence and

arguments persuasive, and we adopt Petitioner's analysis and reasoning as our own.

Patent Owner does not raise separate arguments for claim 19 but argues that claim collectively with claim 1. PO Resp. 13–22. For the reasons noted above regarding claim 1, we do not find Patent Owner's arguments persuasive. Patent Owner does not address claim 20 in its Patent Owner Response.

Accordingly, we determine that the preponderance of the evidence weighs in favor of Petitioner's proof that, like claim 1 above, claims 19 and 20 also are unpatentable as anticipated by Fast.

8. Conclusion Regarding Anticipation by Fast

Based on the full record, including the Petition, Patent Owner's Response, Petitioner's Reply, and all other supporting evidence, we find that Petitioner has shown by a preponderance of the evidence that claims 1, 3–6, 8, 11, 12, and 16–20 (all challenged claims) of the '499 patent are anticipated by Fast.

D. Obviousness of Claims 1, 3–6, 11, 12, and 16–20 in View of Fast and Zou

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).

Petitioner contends that claims 1, 3–6, 11, 12, and 16–20 are unpatentable for obviousness over Fast combined with Zou. Pet. 41–59. Patent Owner raises several points of contention with Petitioner’s combination of Fast and Zou: first, that Petitioner’s combination fails to teach two levels of access control in terms of both “authorized user identification codes” (“AUICs”) and “event information access codes” (“EIACs”) (PO Resp. 22–24); second, that a skilled artisan would not be motivated to combine the references as argued by Petitioner (PO Resp. 24–25); and third, that “the secondary consideration of licensing amply rebuts the obviousness case” (PO Resp. 25–27).

1. 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. 1010 ¶ 10. 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. 2011 ¶ 17.

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.

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

Petitioner relies, in part, on Fast as disclosing the elements of the challenged claims and refers back to its anticipation analysis in support thereof. Pet. 43–44. In combining Zou with Fast, Petitioner notes Zou “shows how to use Fast's location tracking system for [vehicle] fleet management applications.” *Id.* at 43. Petitioner further asserts Zou teaches “specific types of [] user interfaces, permissions, and other features that Fast would include when used specifically for fleet management.” *Id.* For example, Zou teaches information-sharing environments as fleets, within which users may be granted “fleet permissions” to have access to location information regarding vehicles in a fleet. Pet. 50 (citing Ex. 1005 ¶¶ 66, 91, 118, 192, and Figs. 18e, 20b). Petitioner additionally provides a detailed analysis regarding the combined teachings of Fast and Zou with regard to each limitation of independent claim 1 (Pet. 44–55), and further addresses

the combination of Fast and Zou as applied to each of claims 3–6, 11, 12, and 16–20 (Pet. 55–59).

Patent Owner focuses its arguments on independent claim 1, which it argues collectively with claim 19. PO Resp. 22–27. Patent Owner argues that Petitioner’s combination fails to teach two levels of access control in terms of both “authorized user identification codes” (“AUICs”) and “event information access codes” (“EIACs”). PO Resp. 22–24.

a. Independent Claim 1

We address Patent Owner’s contentions in the context of claim 1. Patent Owner argues Zou fails to overcome the deficiencies of Fast because, “[j]ust like Fast, Zou fails to teach two levels of access control in limitations 1(k), 1(l), 1(m).” PO Resp. 22. Petitioner responds by noting that “Zou describes creating a first ISE (*e.g.*, location sharing of multiple fleets) to configure a plurality of event ISEs (*e.g.*, geofence alerts for a specific fleets/vehicles).” Reply 15; *see also* Pet. 48. Petitioner further asserts:

Zou describes a flexible hierarchy of users having different privileges to:

- “Add/edit Fleets” which adds new fleets (expanding the first ISE)[;]
- “Add users to Fleets” which authorizes new users for one or more fleets[; and]
- “Edit Permissions” which allows a user to set authority levels for the users who can view the fleet group[.]

Reply 15 (citing Ex. 1005 ¶ 192). We find Petitioner’s assertions are persuasive and supported by the cited teachings of Zou. As such, we adopt Petitioner’s analysis and reasoning as our own.

Patent Owner further argues, in Zou “there is **no** mention of an AUIC.” PO Resp. 23. As Petitioner correctly notes, however, Patent Owner

appears to confuse the authorized user identification code (“AUIC”) with an “access code.” *Id.* at 23. Petitioner cites to Zou’s *user ID* (Ex. 1005, Fig. 18b), not Zou’s *permissions*, as the claimed authorized user identification code (AUIC). *See* Reply 16. Patent Owner’s expert, Dr. Schonfeld, also opines that “there is no teaching or suggestion in Zou of an authorized user identification code” because “it appears that any ‘permissions’ in Zou are pre-defined, and not user-specific.” Ex. 2011 ¶ 25. We do not credit his testimony because Dr. Schonfeld’s opinion ignores Zou’s teachings that a user can “edit permission profiles for existing users.” Ex. 1005 ¶ 192; *see also* Reply 16. We find Zou’s teaching of a user ID teaches or suggests the claimed “authorized user identification code.”

With regard to the recited “access control codes,” Zou’s user ID is associated with, but different from, the authority levels stored in a user’s permission profile. In particular, Zou explains that a user’s permissions are encoded into a user profile. Ex. 1005 ¶ 152 (explaining how a user profile may not allow the user access to a particular feature); *see also id.* ¶ 211. Petitioner’s expert witness, Dr. Heppe, explains that the data stored in Zou’s profiles equates to “access control codes” because this data “itemizes which permissions” the user may access. Ex. 1010 ¶ 123 (citing Ex. 1005 ¶¶ 151, 192, 211). We credit Dr. Heppe’s testimony, and we find Zou’s teaching of “fleet permissions” and “authority levels” that “are stored in a user’s permission profile” corresponds to “access control codes,” as recited in the ’499 patent claims, because this data specifies which permissions the user may access. Moreover, we find these access control codes are “associated with the plurality of authorized user identification codes” because each user profile in Zou is associated with the user’s ID. Ex. 1005 ¶ 193.

Patent Owner also argues that “Petitioner makes another leap that a user’s ability to create or edit geofences is somehow an EIAC.” PO Resp. 24. Patent Owner further argues “as explained above, the EIAC is specified by the authorized user when it configures the E-ISE, and there is no such code in Zou.” *Id.* Petitioner responds by noting that “Patent Owner misconstrues Petitioner’s invalidity argument by conflating the second level of administrator privilege with access to geofence functionality.” Reply 17. Petitioner further asserts:

Zou teaches at least two levels of administrator privileges: those users who can edit other users (*e.g.*, creating users or editing their profiles) and those users who cannot. (See Ex. 1005, ¶0192). As discussed in the Petition, Zou describes a fleet manager (first level) who creates and sets privileges for other users (second level). (Petition, p.47). Some of these created users have access to geofence functionality, while others do not. (Ex. 1005, ¶0205 stating “The exemplary telemetry system allows the user to create and view current GeoFences; however, the user’s user profile may not allow the user to create GeoFences.”). In this respect, Zou’s disclosure of how some users at the second level are given access to geofence functionality teaches the EIAC claimed in limitations [l] and [m]. This teaching is additive to Zou’s disclosure of a Fleet Manager who also creates users (*e.g.*, a flexible hierarchical structure).

Id.; see also Pet. 52–53; Ex. 1005 ¶¶ 206–211.

We find Petitioner’s assertions to be persuasive and supported by Zou’s disclosure, and we adopt Petitioner’s analysis and reasoning as our own. We also find our construction of “information access code” (which includes the related term “event information access code”), *supra*, encompasses Zou’s teachings. In particular, we find Zou’s teaching of “geofence crossings” corresponds to “specified event conditions” because

Zou discloses that geofence crossings (that is, when a device enters or exits an area bounded by a geofence) may trigger an alert (Ex. 1005 ¶¶ 91, 204), and that the alert associated with a geofence can be configured to transmit date, time, position, speed, and analog or digital status indications. *Id.*; *see also* ¶ 171. Thus, we find Zou’s teaching of data stored in a user’s profile indicating that user’s ability to create or edit geofences teaches or suggests an identifier (name, number, or other series of letters, numbers, symbols, or the like) associated with specific information (geofence crossings) that may be used to manage conveyance of that information by specifying which users are authorized to receive that information. Accordingly, Zou teaches or suggests the claimed “event information access code.”

b. Dependent Claims 3–6, 11, 12, 16–18, and 20

Petitioner argues that dependent claims 3–6, 11, 12, 16–18, and 20 also would have been unpatentable for obviousness over Fast and Zou. Pet. 55–59. Patent Owner does not expressly dispute Petitioner’s evidence of obviousness with respect to these claims, other than as addressed with regard to independent claims 1 and 19.

We have considered fully the evidence and arguments presented by Petitioner explaining how Fast, either alone or as modified by Zou, teaches the limitations of all these claims. *See* Pet. 55–59. We find Petitioner’s evidence and arguments persuasive, and adopt Petitioner’s reasoning as our own.

3. Rationale To Combine

Patent Owner also argues the combination of Fast and Zou does not render the '499 claims obvious because “a person of ordinary skill in the art would not be motivated to combine Fast with Zou.” PO Resp. 24. In particular, Patent Owner argues:

Fast teaches a predefined hierarchical structure that is administrator-specified. Fast also touts the benefits of having a rigid system that cannot be modified. *See* Ex. 1003 at 6:12-19, 48-65. By contrast, Zou teaches a more flexible user-defined structure where users can change permissions. *See* Ex. 1005 at ¶ [192]. Thus, Fast and Zou teach fundamentally different and incompatible ways of setting privileges and access rights.

Id. at 24–25. Patent Owner cites, as support, the declaration of its expert witness, Dr. Schonfeld, who opines that a “person of ordinary skill in the art would likely not have even been *able* to combine these systems, due to their fundamentally different ways of arranging and conveying information in incompatible data structures, and instead would need to redevelop the system’s software from scratch.” PO Resp. 25 (citing Ex. 2011 ¶ 24).

We are not persuaded by Patent Owner’s arguments, which contradict the intrinsic record. As we have found, Fast does not treat all users within a type “the same,” as Patent Owner contends. Rather, we find Fast discloses a flexible system in which a subscriber, through its own secure portal, may create different users, such as guardians, having different levels of access to functionality and information in the subscriber’s portal. Ex. 1003, 42:14–52, Figs. 16–1, 16–2; *see also* Ex. 1010 ¶¶ 30, 45–47, 101.

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.”).

We find the Petition and supporting testimony of Petitioner’s expert witness, Dr. Heppe, provide a sufficient rationale to combine the teachings of Fast and Zou in a manner demonstrating the obviousness of the challenged claims. *See* Pet. 41–43; Ex. 1010 ¶¶ 55–58.

4. Secondary Considerations

Patent Owner argues that secondary considerations—specifically, evidence of licensing of the ’499 patent—“amply rebuts the obviousness case.” PO Resp. 25. In particular, Patent Owner states the following companies “in the fleet-tracking industry” have taken licenses to the ’499 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 26. As Patent Owner notes, “this roster of licensees” includes “*all* of the companies who brought this IPR proceeding.” *Id.* Patent Owner argues that these companies “have shown that [the ’499 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 Pharm.*, 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 '499 patent, along with "other patents in the same family," have been licensed to the companies identified above. Ex. 2012 ¶¶ 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. Reply 22–23.

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 '499 patent. Moreover, as Petitioner notes, all of the licenses identified by Patent Owner involved the settlement of suits by Patent Owner for infringement of multiple patents, including the '499 patent. Reply 20; Ex. 1015. 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, Patent Owner has not made any license part of the record, has not shown any reason why any of the identified licensees took a license other than as part of a business decision to avoid litigation, and has not identified a nexus between the merits of the invention reflected in any claim of the '499 patent (as opposed to any of the other patents licensed in the same settlement agreements) and the licenses themselves. We, therefore, find Patent Owner has made an insufficient showing of nexus between the asserted license agreements and the claims at issue here to demonstrate evidence tending to show non-obviousness.

5. Obviousness Conclusion

We determine that Petitioner has shown, by a preponderance of the evidence, that claims 1, 3–6, 11, 12, and 16–20 of the '499 patent would have been obvious to a person of ordinary skill in the art in view of Fast in combination with Zou.

IV. CONCLUSION

After considering the evidence and arguments presented in the Petition, Patent Owner's Response, and the Reply, we determine that Petitioner has demonstrated by a preponderance of the evidence that challenged claims 1, 3–6, 8, 11, 12, and 16–20 of the '499 patent are unpatentable as anticipated by Fast, and claims 1, 3–6, 11, 12, and 16–20 are unpatentable for obviousness over Fast and Zou.

V. ORDER

Accordingly, it is hereby:

ORDERED that claims 1, 3–6, 8, 11, 12, and 16–20 of the '499 patent are unpatentable;

FURTHER ORDERED that, because this is a Final Written Decision, the parties 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 IPR2016-01064

Patent 9,003,499 B2

PETITIONER:

Vivek Ganti

HILL, KERTSCHER & WHARTON, LLP

vg@hkw-law.com

PATENT OWNER:

Alan Whitehurst

Marissa R. Ducca

QUINN EMANUEL URQUHART & SULLIVAN, LLP

alanwhitehurst@quinnemanuel.com

marissaducca@quinnemanuel.com

Robert S. Babayi

VECTOR IP LAW GROUP

robert@vectoriplaw.com