

Petition for *Inter Partes* Review of U.S. Patent No. 11,468,757

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

RAVE WIRELESS, INC. AND MOTOROLA SOLUTIONS, INC.,
Petitioners

v.

SAMSCLOUD, LLC,
Patent Owner

IPR2027-00009

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 11,468,757**

CONTENTS

EXHIBIT LIST.....	vi
MANDATORY NOTICES UNDER 37 C.F.R. 42.8(A)(1).....	ix
I. Real Party-in-Interest under 37 C.F.R. 42.8(b)(1)	ix
II. Related Matters under 37 C.F.R. 42.8(b)(2)	ix
III. Lead and Back-Up Counsel under 37 C.F.R. 42.8(b)(3)	x
IV. Service Information under 37 C.F.R. 42.8(b)(4).....	x
V. Claims Listing.....	xi
A. Claim 1.....	xi
B. Claim 2.....	xii
C. Claim 3.....	xii
D. Claim 4.....	xiii
E. Claim 5.....	xiii
F. Claim 6.....	xiii
G. Claim 7.....	xiii
H. Claim 8.....	xiv
I. Claim 9.....	xiv
J. Claim 10.....	xiv
K. Claim 11.....	xvi
L. Claim 12.....	xvi
M. Claim 13.....	xvii
N. Claim 14.....	xvii
O. Claim 15.....	xvii
P. Claim 16.....	xvii
Q. Claim 17.....	xviii
R. Claim 18.....	xviii
PETITION.....	1
I. Introduction.....	1
II. Requirements Under 37 C.F.R. 42.104.....	1

A.	Grounds for Standing.....	1
B.	Identification of Challenge and Statement of Precise Relief Requested	1
III.	The '757 Patent and Prosecution History	2
IV.	Priority Date and Level of Ordinary Skill in the Art	5
V.	Claim Construction	5
VI.	Summary of Prior Art	6
A.	Staton (EX[1007]).....	6
B.	Noland (EX[1008]).....	7
C.	Rauner (EX[1009])	7
D.	Azmoodeh (EX[1010])	7
VII.	Grounds of Unpatentability.....	8
A.	Ground 1: Obviousness of Claims 1-4, 6, 8, 10-13, 15, and 17 In View of Staton (EX[1007]) + Knowledge of a POSITA	8
1.	Claim 1.....	8
2.	Claim 2.....	29
3.	Claim 3.....	32
4.	Claim 4.....	34
5.	Claim 6.....	35
6.	Claim 8.....	37
7.	Claim 10.....	38
8.	Claim 11.....	40
9.	Claim 12.....	40
10.	Claim 13.....	40
11.	Claim 15.....	40
12.	Claim 17.....	40
B.	Ground 2: Obviousness of Claims 5, 7, 9, 14, 16, and 18 in view of Staton (EX[1007]) + Noland (EX[1008]) + Knowledge of a POSITA	41
1.	A POSITA Would Have Combined Staton with Noland	41
2.	Claim 5.....	43

3.	Claim 7.....	44
4.	Claim 9.....	47
5.	Claim 14.....	49
6.	Claim 16.....	49
7.	Claim 18.....	49
C.	Ground 3: Obviousness of Claims 1-4, 6-8, 10-13, and 15-17 in view of Rauner (EX[1009]) + Azmoodeh (EX[1010]) + Knowledge of a POSITA	50
1.	A POSITA Would Have Combined Rauner With Azmoodeh	50
2.	Claim 1.....	53
3.	Claim 2.....	65
4.	Claim 3.....	67
5.	Claim 4.....	69
6.	Claim 6.....	70
7.	Claim 7.....	72
8.	Claim 8.....	73
9.	Claim 10.....	74
10.	Claim 11.....	75
11.	Claim 12.....	75
12.	Claim 13.....	75
13.	Claim 15.....	75
14.	Claim 16.....	76
15.	Claim 17.....	76
D.	Ground 4: Obviousness of Claims 5, 9, 14, 18 in view of Rauner (EX[1009]) + Azmoodeh (EX[1010]) in further view of Noland (EX[1008]) + Knowledge of a POSITA	76
1.	A POSITA Would Have Been Motivated to Combine the Rauner and Azmoodeh System with Noland	76
2.	Claim 5.....	78
3.	Claim 9.....	80
4.	Claim 14.....	81
5.	Claim 18.....	81

VIII. Secondary Considerations.....	81
IX. Conclusion	82

EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent No. 11,468,757 (“’757 Patent”)
1002	File History for ’757 Patent
1003	U.S. Patent No. 12,154,421 (“’421 Patent”)
1004	File History for ’421 Patent
1005	Declaration of David H. Williams
1006	Curriculum Vitae of David H. Williams
1007	U.S. Patent No. 7,317,927 (“Staton”)
1008	U.S. Patent App. Pub. No. 2018/0158305 (“Noland”)
1009	U.S. Patent App. Pub. No. 2019/0166480 (“Rauner”)
1010	U.S. Patent App. Pub. No. 2017/0287006 (“Azmoodeh”)
1011	U.S. Patent 10,085,117 (“Smith”)
1012	File History for Reissue Application No. 18/648,671
1013	U.S. Patent No. 7,881,733 (“Staton ’733”)
1014	U.S. Patent App. Pub. No. 2014/0155094 A1 (“Zises”)
1015	U.S. Patent App. Pub. No. 2016/0358432 A1 (“Branscomb”)
1016	U.S. Patent App. Pub. No. 2018/0075108 A1 (“Park”)
1017	U.S. Patent No. 6,714,791 (“Friedman”)
1018	U.S. Patent No. 6,353,390 (“Berl”)
1019	U.S. Patent No. 6,721,652 (“Sanquetti”)
1020	Nat’l Emergency No. Ass’n, <i>A Public Safety Answering Point Managers' Guide to Geographic Information Technology</i> (Oct.

	2002), https://cdn.ymaws.com/www.nena.org/resource/collection/2BEE3832-DD9B-4CD6-AB89-979F2CA8F789/57-001A_GIS_Guide.pdf .
1021	U.S. Patent No. 7,133,685 (“Hose”)
1022	U.S. Patent No. 7,164,986 (“Humphries”)
1023	U.S. Patent No. 10,257,644 (“Samsung SDS”)
1024	U.S. Patent No. 9,747,380 (“IBM”)
1025	U.S. Patent No. 5,839,088 (“Hancock ’088”)
1026	U.S. Patent No. 6,339,744 (“Hancock ’744”)
1027	U.S. Patent No. 6,618,593 (“Drutman”)
1028	U.S. Patent No. 8,103,729 (“Tornabene”)
1029	Clery Center, The Jeanne Clery Act, https://www.clerycenter.org/the-clery-act#:~:text=The%20Clery%20Act%20requires%20colleges,place%20to%20improve%20campus%20safety .
1030	Stephen Lawson, <i>Worker Tracking Service Coming to Nextel Phones</i> , Network World (Mar. 4, 2003), https://www.networkworld.com/article/895404/uc-voip-worker-tracking-service-coming-to-nextel-phones.html .
1031	Gary Krakow, <i>Two New Cellular Phones Built for Abuse</i> , NBC News (Feb. 20, 2004, 3:51 PM EST), https://www.nbcnews.com/id/wbna4324939 .
1032	CIO Staff, <i>Sprint Launches GPS-Based Child-Locator Service</i> , CIO (Apr. 13, 2006), https://www.cio.com/article/257110/mobile-sprint-launches-gps-based-child-locator-service.html .
1033	U.S. Patent No. 9,510,141 (“Matamala”)

1034	Ecma Int'l, ECMA-340, <i>Near Field Communication — Interface and Protocol (NFCIP-1)</i> (3d ed. June 2013).
-------------	--

MANDATORY NOTICES UNDER 37 C.F.R. 42.8(A)(1)

I. REAL PARTY-IN-INTEREST UNDER 37 C.F.R. 42.8(B)(1)

Rave Wireless, Inc., is a Delaware corporation (“Rave”) and wholly-owned subsidiary of Motorola Solutions, Inc. (“MSI”), which is a Delaware corporation and publicly traded company. Rave and MSI are the Petitioners.

No other parties exercised or could have exercised control over this Petition; no other parties funded or directed this Petition. *See* Office Patent Trial Practice Guide, 77 FED. REG. 48759, 48759-60.

II. RELATED MATTERS UNDER 37 C.F.R. 42.8(B)(2)

Patent Owner (“PO”) asserted the ’757 Patent against Rave in a complaint filed on July 23, 2026. *Samscloud, LLC v. Rave Wireless, Inc., d/b/a Rave Mobile Safety*, Case No. 1-26-cv-00900 (D. Del.). On the same day, PO also asserted the ’757 Patent against Raptor Technologies, LLC in *Samscloud, LLC v. Raptor Technologies, LLC*, Case No. 1-26-cv-00899 (D. Del.) and Genetec Inc. in *Samscloud, LLC v. Genetec Inc.*, 1-26-cv-00901 (D. Del.).

PO filed a reissue proceeding on the ’757 Patent on April 29, 2024 to correct alleged errors in dependent claims 9 and 18. *See* EX[1012], 57-60, 138-146. During the reissue proceeding, the Examiner rejected all claims 1-18 of the original patent on June 4, 2026. *Id.* 6, 23-35. Applicant then expressly abandoned the reissue on September 23, 2026. *Id.* 7-8.

III. LEAD AND BACK-UP COUNSEL UNDER 37 C.F.R. 42.8(B)(3)

Petitioners designate the following:

LEAD COUNSEL	BACK-UP COUNSEL
Eliot D. Williams (Reg. No. 50,822) eliot.williams@bakerbotts.com Tel: 202-639-1334 BAKER BOTTS L.L.P. 700 K Street, N.W Washington, D.C. 20001-5692	Katharine Burke (<i>pro hac vice</i> application forthcoming) katharine.burke@bakerbotts.com Tel: 202-639-7720 BAKER BOTTS L.L.P. 700 K Street, N.W Washington, D.C. 20001-5692 Sam Kassa (<i>pro hac vice</i> application forthcoming) sam.kassa@bakerbotts.com Tel: 202-639-7794 BAKER BOTTS L.L.P. 700 K Street, N.W Washington, D.C. 20001-5692 Matthew Thompson (Reg. No. 80,905) matthew.thompson@bakerbotts.com Tel: 212-408-2580 BAKER BOTTS L.L.P. 30 Rockefeller Plaza New York, NY 10112-4498

A Power of Attorney is filed concurrently herewith under 37 C.F.R. 42.10(b).

IV. SERVICE INFORMATION UNDER 37 C.F.R. 42.8(B)(4)

Correspondence to lead and back-up counsel can be provided at the postal and electronic addresses above. Petitioners consent to service by electronic mail at: eliot.williams@bakerbotts.com; katharine.burke@bakerbotts.com; sam.kassa@bakerbotts.com; and matthew.thompson@bakerbotts.com.

V. CLAIMS LISTING

A. Claim 1

1[pre]	A method for facilitating supervision of individuals based on geofencing, the method comprising:
1[a]	receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor;
1[b]	receiving, using the communication device, a geographical location from the at least one supervisor device;
1[c]	analyzing, using a processing device, the geographical location based on the at least one security parameter;
1[d]	generating, using the processing device, a geofence corresponding to a geographical area based on the analyzing;
1[e]	receiving, using the communication device, at least one supervisee data associated with a supervisee from at least one supervisee device;
1[f]	analyzing, using the processing device, the at least one supervisee data based on the geofence;
1[g]	generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data;
1[h]	transmitting, using the communication device, the supervision notification to the at least one supervisor device; and
1[i]	storing, using a storage device, the at least one supervisee data and the supervision notification, wherein:
1[j]	the geofence is characterized by a geofence area corresponding to the geographical area, wherein the geofence comprises a plurality of geofence grid boxes associated with the geofence area, wherein each geofence grid box is characterized by a grid box geofence area of the geofence area, wherein the method comprises:
1[j][1]	receiving, using the communication device, at least one grid parameter

	from the at least one supervisor device, wherein the processing device is further configured for:
1[j][2]	analyzing, using the processing device, the at least one grid parameter;
1[j][3]	determining, using the processing device, the grid box geofence area based on the analyzing of the at least one grid parameter; and
1[j][4]	generating, using the processing device, a number of geofence grid boxes based on the determining.

B. Claim 2

2[a]	The method of claim 1 further comprising: receiving, using the communication device, at least one location indication associated with the geographical area from the at least one supervisor device;
2[b]	identifying, using the processing device, at least one location corresponding to the at least one location indication;
2[c]	analyzing, using the processing device, the at least one supervisee data based on the at least one location; and
2[d]	determining, using the processing device, a location anomaly based on the analyzing of the at least one supervisee data based on the at least one location, wherein the generating of the supervision notification is based on the determining.

C. Claim 3

3[a]	The method of claim 1, wherein the supervision notification comprises at least one supervisee event, wherein the at least one supervisee event is associated with at least one action, wherein the method comprises:
3[b]	determining, using the processing device, the at least one action based on the supervision notification; and
3[c]	performing, using the processing device, the at least one action based on the determining, wherein the at least one action comprises an establishment of a communication session between the at least one supervisor device and the at least one supervisee device.

D. Claim 4

4[a]	The method of claim 1 further comprising: identifying, using the processing device, the supervisee based on the analyzing of the at least one supervisee data; and
4[b]	retrieving, using the storage device, supervisee profile data associated with the supervisee based on the identifying, wherein the generating of the supervision notification is based on the retrieving.

E. Claim 5

5[a]	The method of claim 1 further comprising: identifying, using the processing device, at least one object associated with the supervisee based on the analyzing of the at least one supervisee data; and
5[b]	determining, using the processing device, a lethality of the at least one object based on the identifying, wherein the generating of the supervision notification is based on the determining.

F. Claim 6

6[a]	The method of claim 1 further comprising: receiving, using the communication device, at least one environment data associated the geographical area corresponding to the geofence;
6[b]	analyzing, using the processing device, the at least one environment data; and determining, using the processing device, at least one threat based on the analyzing of the at least one environment data, wherein the generating of the supervisor notification is based on the determining.

G. Claim 7

7[a]	The method of claim 1 further comprising: retrieving, using the storage device, a blueprint associated with the geographical area corresponding to the geofence;
-------------	--

7[b]	analyzing, using the processing device, the blueprint and the at least one supervisee data; and
7[c]	determining, using the processing device, a location of the supervisee on the blueprint based on the analyzing of the blueprint and the at least one supervisee data, wherein the generating of the supervision data is based on the determining.

H. Claim 8

8[a]	The method of claim 1, wherein the at least one supervisee device comprises at least one sensor,
8[b]	wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,
8[c]	wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting.

I. Claim 9

9[a]	The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises:
9[b]	receiving, using the communication device, at least one NFC indication corresponding to the at least NFC identification from the at least one supervisee device; wherein the receiving is performed over short range wireless communication comprising at least one of Bluetooth, Zigbee, Ultra-wideband, Wi-Fi and NFC, and
9[c]	identifying, using the processing device, the supervisee based on the at least one NFC indication, wherein the generating of the supervision notification is based on the identifying.

J. Claim 10

10[pre]	A system for facilitating supervision of individuals based on geofencing, the system comprising:
10[a]	a communication device configured for:

10[a][1]	receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor;
10[a][2]	receiving, using the communication device, a geographical location from the at least one supervisor device;
10[a][3]	receiving at least one supervisor data associated with a supervisee from at least one supervisee device; and
10[a][4]	transmitting a supervision notification to the at least one supervisor device;
10[b]	a processing device configured for:
10[b][1]	analyzing the geographical location based on the at least one security parameter;
10[b][2]	generating a geofence corresponding to a geographical area based on the analyzing;
10[b][3]	analyzing the at least one supervisee data based on the geofence; and
10[b][4]	generating the supervision notification based on the analyzing of the at least one supervisee data; and
10[c]	a storage device configured for storing the at least one supervisee data and the supervision notification, wherein:
10[d]	the geofence is characterized by a geofence area corresponding to the geographical area, wherein the geofence comprises a plurality of geofence grid boxes associated with the geofence area, wherein each geofence grid box is characterized by a grid box geofence area of the geofence area,
10[d][1]	wherein the communication device is further configured for receiving at least one grid parameter from the at least one supervisor device,
10[d][2]	wherein the processing device is further configured for: analyzing the at least one grid parameter;

10[d][3]	determining the grid box geofence area based on the analyzing of the at least one grid parameter; and
10[d][4]	generating a number of geofence grid boxes based on the determining.

K. Claim 11

11[a]	The system of claim 10, wherein the communication device is further configured for receiving at least one location indication associated with the geographical area from the at least one supervisor device, wherein the processing device is further configured for:
11[b]	identifying at least one location corresponding to the at least one location indication;
11[c]	analyzing the least one supervisee data based on the at least one location; and
11[d]	determining a location anomaly based on the analyzing of the at least one supervisee data based on the at least one location, wherein the generating of the supervision notification is based on the determining.

L. Claim 12

12[a]	The system of claim 10, wherein the supervision notification comprises at least one supervisee event, wherein the at least one supervisee event is associated with at least one action, wherein the processing device is further configured for:
12[b]	determining the at least one action based on the supervision notification; and
12[c]	performing the at least one action based on the determining, wherein the at least one action comprises an establishment of a communication session between the at least one supervisor device and the at least one supervisee device.

M. Claim 13

13[a]	The system of claim 10, wherein the processing device is further configured for identifying the supervisee based on the analyzing of the at least one supervisee data,
13[b]	wherein the storage device is configured for retrieving supervisee profile data associated with the supervisee based on the identifying, wherein the generating of the supervision notification is based on the retrieving.

N. Claim 14

14[a]	The system of claim 10, wherein the processing device is further configured for: identifying at least one object associated with the supervisee based on the analyzing of the at least one supervisee data; and
14[b]	determining a lethality of the at least one object based on the identifying, wherein the generating of the supervision notification is based on the determining.

O. Claim 15

15[a]	The system of claim 10, wherein the communication device is further configured for receiving at least one environment data associated the geographical area corresponding to the geofence, wherein the processing device is further configured for:
15[b]	analyzing the at least one environment data; and determining at least one threat based on the analyzing of the at least one environment data, wherein the generating of the supervisor notification is based on the determining.

P. Claim 16

16[a]	The system of claim 10, wherein the storage device is further configured for retrieving a blueprint associated with the geographical area corresponding to the geofence,
--------------	--

16[b]	wherein the processing device is further configured for analyzing the blueprint and the at least one supervisee data; and
16[c]	determining a location of the supervisee on the blueprint based on the analyzing of the blueprint and the at least one supervisee data, wherein the generating of the supervision data is based on the determining.

Q. Claim 17

17[a]	The system of claim 10, wherein the at least one supervisee device comprises at least one sensor,
17[b]	wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,
17[c]	wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting.

R. Claim 18

18[a]	The system of claim 10, wherein the supervisee is associated with at least one near field communication (NFC) identification,
18[b]	wherein the communication device is further configured for receiving at least one NFC indication corresponding to the at least NFC identification from the at least one supervisee device,
18[c]	wherein the processing device is further configured for identifying the supervisee based on the at least one NFC indication,
18[d]	wherein the generating of the supervision notification is based on the identifying.

PETITION

I. INTRODUCTION

Just over two months ago, PO sued Rave, a U.S. company, alleging infringement of the '757 Patent by Rave's software products. Claims 1-18 of the '757 Patent ("Challenged Claims"), however, issued based on a series of material errors by the Office. PO has admitted such errors occurred, even filing an application for reissue to correct them. But, after all pending claims were rejected in that reissue application, PO abandoned the application, leaving the original erroneous claims in force. EX[1012], 7-8, 23-35, 58-60. Those claims reflect even further Office error: the Staton '733 reference (EX[1013]) cited by the Office itself discloses the "geofence grid box" functionality that the Office found missing from the prior art. EX[1002], 222-223, 227. Petitioners request review to correct these errors.

II. REQUIREMENTS UNDER 37 C.F.R. 42.104

A. Grounds for Standing

Petitioners certify that the '757 Patent is eligible for *inter partes* review and that Petitioners meet the eligibility requirements set forth in 37 C.F.R. 42.104.

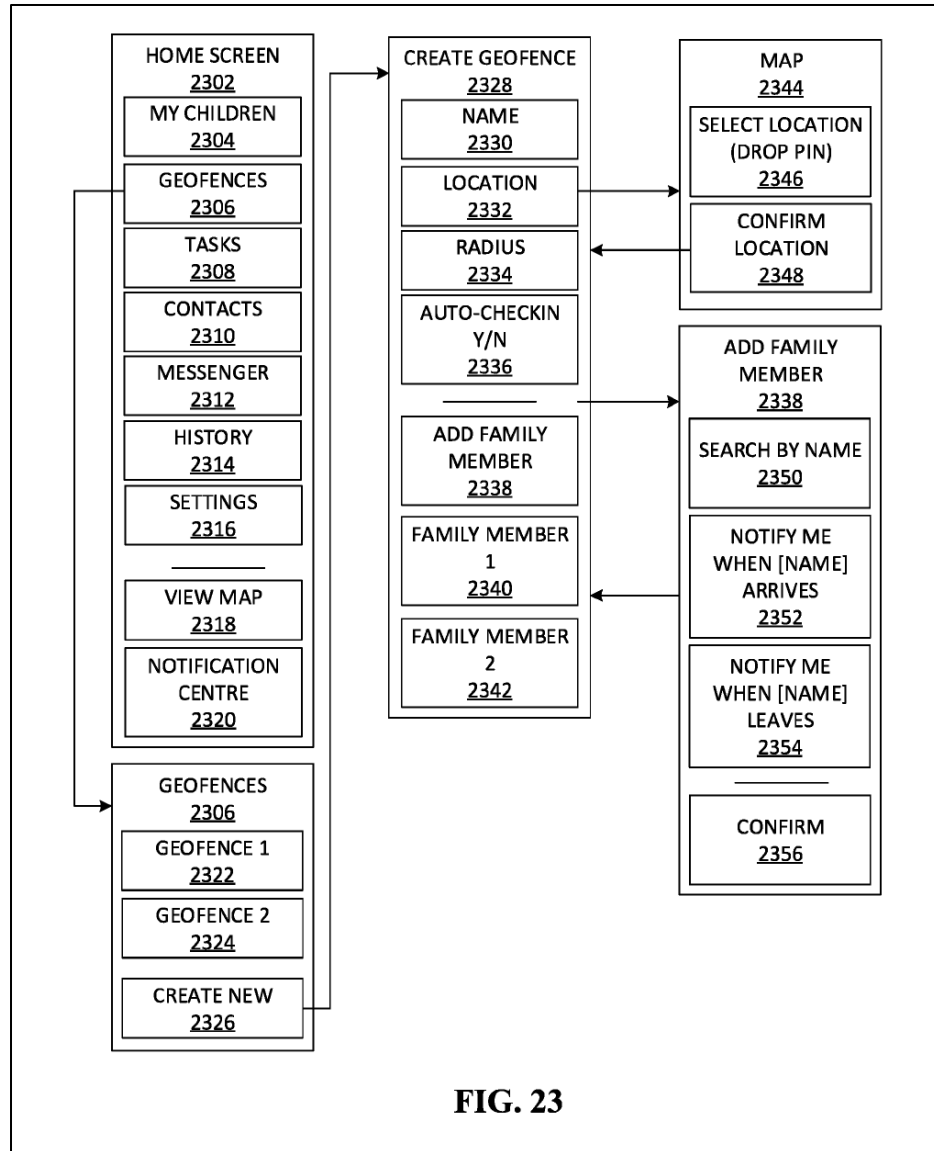
B. Identification of Challenge and Statement of Precise Relief Requested

Ground	'757 Patent Claims	Basis for Challenge
1	1-4, 6, 8, 10-13, 15, 17	Obvious in view of Staton + knowledge of a person of ordinary skill in the art ("POSITA")

Ground	'757 Patent Claims	Basis for Challenge
2	5, 7, 9, 14, 16, 18	Obvious in view of Staton + Noland + knowledge of a POSITA
3	1-4, 6-8, 10-13, 15-17	Obvious in view of Rauner + Azmoodeh + knowledge of a POSITA
4	5, 9, 14, 18	Obvious in view of Rauner + Azmoodeh + Noland + knowledge of a POSITA

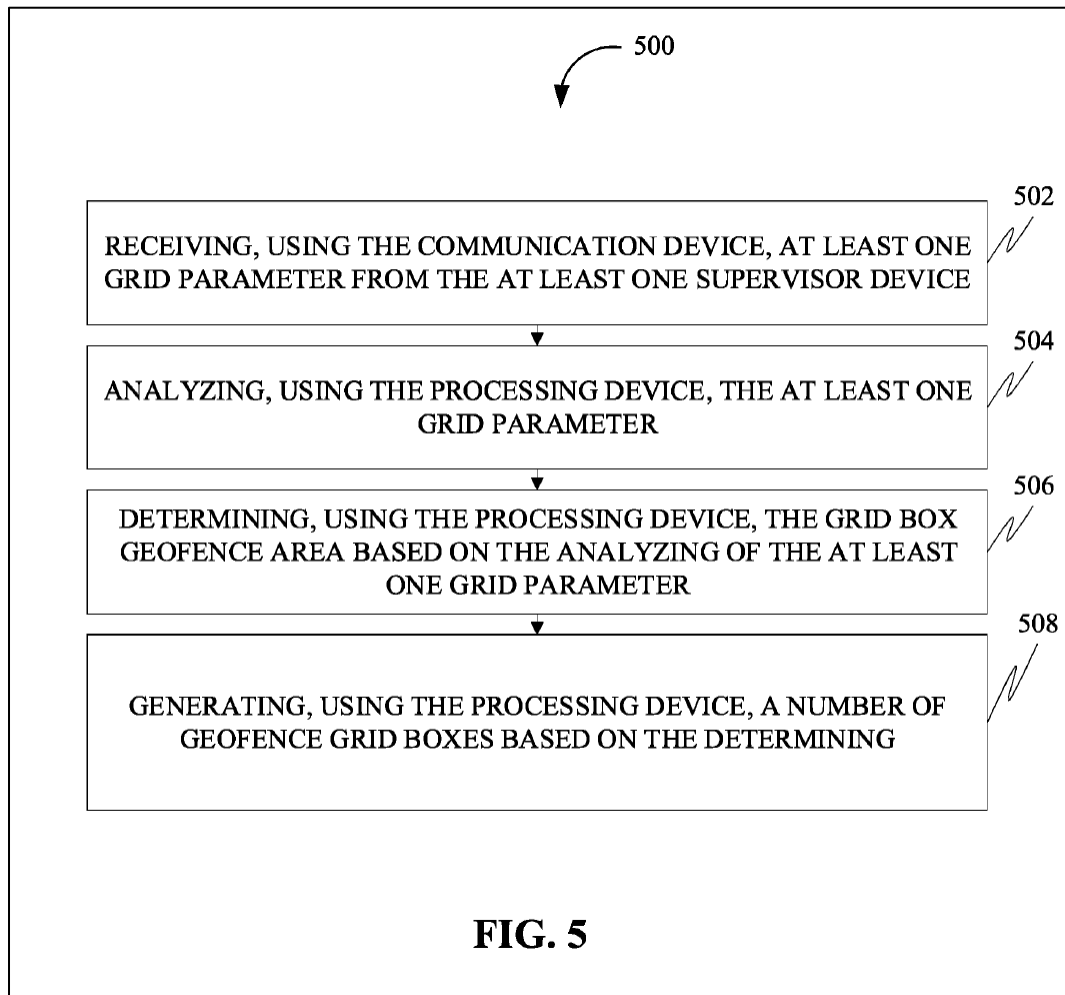
III. THE '757 PATENT AND PROSECUTION HISTORY

The '757 Patent purports to improve “conventional geofencing applications” that allegedly “do not allow easy access for a user to create the geofence.” EX[1001], 1:22-23. The patent describes a generic “communication device” that “receiv[es]” an unspecified security “parameter” and any “geographical location” from a “supervisor device” to create a geofence, which can be used to monitor a “supervisee.” *Id.*, 11:38-63, 12:1-14. For example, a supervisor “parent” can create a geofence using inputs, *e.g.*, “name,” “location,” or “radius,” and “drop pin” functionality to select the location (*id.* 18:52-19:6, Fig. 23 (boxes 2328 and 2344 below)) and then can receive a notification when a supervisee “child” reaches a geofence. *E.g., id.* 18:6-23.



The patent also describes that the geofence can comprise “geofence grid boxes.” EX[1001], 13:8-13. If so, the patent explains that the communication device receives a “grid parameter” from the supervisor, which the “processing device” analyzes to determine the area and number of geofence grid boxes. *Id.* 13:13-22; *id.* Fig. 5, 14:30-45. Beyond that, the patent does not explain what the “grid parameter” is, how it is received, or how it is used to create “geofence grid boxes.” EX[1005],

¶¶54-63, 85-90. The only figure describing the geofence grid boxes (Fig. 5) largely repeats the claim language:



Despite the limited disclosures, the Office allowed all issued claims during original prosecution based on these “geofence grid box” limitations, which the Examiner concluded did not exist in the cited prior art. EX[1002], 222-223 (reasons for allowance). The Office, however, missed that the cited Staton ’733 reference (EX[1013]; *see* EX[1002], 227) discloses the claimed functionality, which is replete in other prior art as well. EX[1005], ¶¶35-84, 93-97, 202-204.

IV. PRIORITY DATE AND LEVEL OF ORDINARY SKILL IN THE ART

The '757 Patent claims priority to Provisional Application No. 62/814,097 filed March 5, 2019. EX[1001] (21)-(22), (60). Petitioners assume without conceding that the Challenged Claims are entitled to that priority date.

As of March 5, 2019, a POSITA would have had a bachelor's degree in electrical engineering, computer science, or a similar field and two years' experience with location-based services or mobile applications, or equivalent experience. EX[1005], ¶33. Less education with more relevant experience could suffice. *Id.*

V. CLAIM CONSTRUCTION

“Geofence:” A POSITA would understand “geofence” to include a virtual geographic boundary and associated settings or parameters that trigger an alert upon entry or exit. EX[1005], ¶103-114. The specification describes it as:

a virtual perimeter for a real-world geographical area that... *allows an individual to trigger an alert to multiple users when the individual may enter and/or exit the geofence.*

EX[1001], 1:14-21.

§ 112(f) Terms: Applicant conceded during prosecution that § 112(f) applies to the below terms because they “use a generic placeholder (‘device’) coupled with functional language without reciting sufficient structure.” EX[1002], 208-209. Applicant identified the corresponding structure set forth below for each term, *id.*,

and Petitioners apply that construction herein:

Term	Corresponding Structure
“a communication device configured for: receiving...receiving...receiving...and transmitting”	Program or database inside a “server computer” that “handles messages between the server computer and external devices,” EX[1002], 209; EX[1001] Figs. 1, 2-10.
“a processing device configured for: analyzing...generating...analyzing...and generating...”	Program or database “inside of the server computer” that “receives data from the communication device” and “stores the processed data on the storage device,” EX[1002], 209; EX[1001] Figs. 1, 2-10.
“a storage device configured for storing...”	Program or database “inside of the server computer” that “stores” the data, EX[1002], 209; EX[1001] Figs. 1, 2-10.

Petitioners apply the plain meaning for all other terms in the Challenged Claims and submit that the claims are invalid regardless of their precise construction. *See* 37 C.F.R. §42.200; *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

VI. SUMMARY OF PRIOR ART

A. Staton (EX[1007])

Staton issued January 8, 2008 and is prior art under 35 U.S.C. §§ 102(a)(1)-

(2). Staton discloses monitoring individuals with geofences comprising geofence grid boxes. EX[1007], Abs., 3:6-18, Fig. 5; EX[1005], ¶¶115-120.

B. Noland (EX[1008])

Noland published on June 7, 2018 and is prior art under 35 U.S.C. §§ 102(a)(1)-(2). It discloses automated gunshot detection and emergency response. EX[1008], ¶¶[0015]–[0019]; EX[1005], ¶¶121-125.

C. Rauner (EX[1009])

Rauner was filed January 7, 2019, published May 30, 2019, and is a continuation of Application No. 15/865,245, filed January 8, 2018, and is therefore prior art under 35 U.S.C. § 102(a)(2). It uses geofences to monitor and coordinate emergency response. EX[1009], (22), (43), ¶¶[0048], [0239]; EX[1005], ¶¶126-131.

D. Azmoodeh (EX[1010])

Azmoodeh published on October 5, 2017 and is prior art under 35 U.S.C. §§ 102(a)(1)-(2). It uses geofence grid boxes to monitor devices within a geographic region. EX[1010], ¶¶[0015], [0022], [0046]; EX[1005], ¶¶132-135.

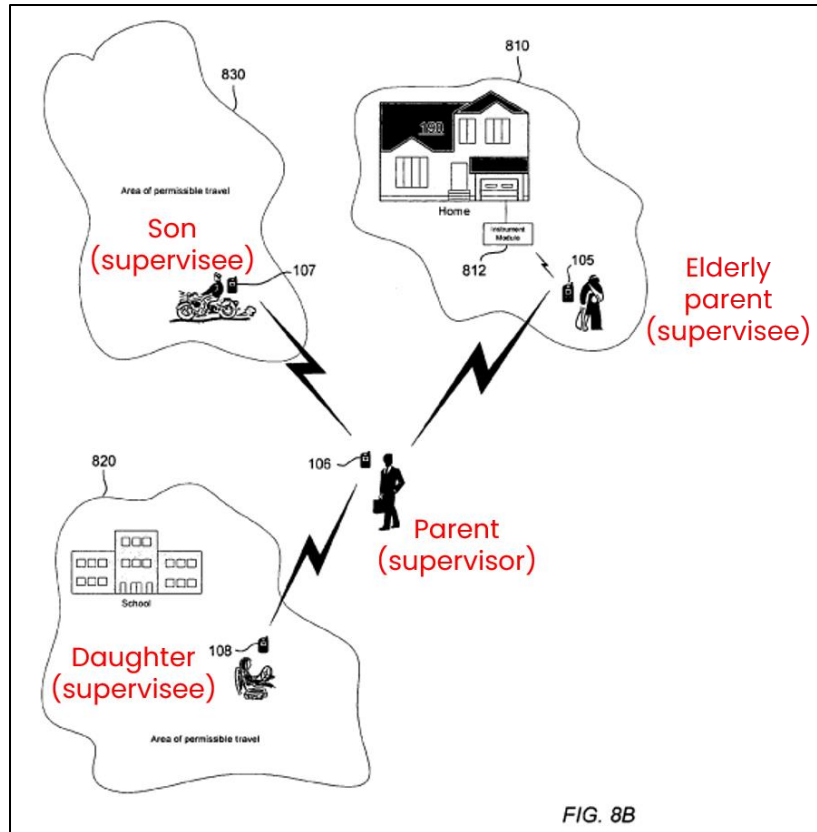
VII. GROUNDS OF UNPATENTABILITY

A. Ground 1: Obviousness of Claims 1-4, 6, 8, 10-13, 15, and 17 In View of Staton (EX[1007]) + Knowledge of a POSITA

1. Claim 1

a. 1[pre] “A method for facilitating supervision of individuals based on geofencing, the method comprising:”

To the extent it is limiting, Staton discloses the preamble. § V; EX[1005], ¶¶154-157. In Staton, the geofence’s virtual geographic boundary corresponds to Staton’s “geographical zones.” EX[1005], ¶¶154, 156; EX[1007], 1:20-22, 26:24-26; *id.* 8:11-14, 1:64-67. “[G]eofencing’ events” with settings/parameters track “entering or leaving a geographical area that has been geofenced.” *Id.* 13:65-67, 14:1-3. For example, in Fig. 8B, annotated below, “a parent can own a PDA 106 which monitors all of the other PDAs” and “the parent may...delineate specific areas where the son can travel, and areas where the son cannot travel.” *Id.* 27:11-15, 27:52-54.

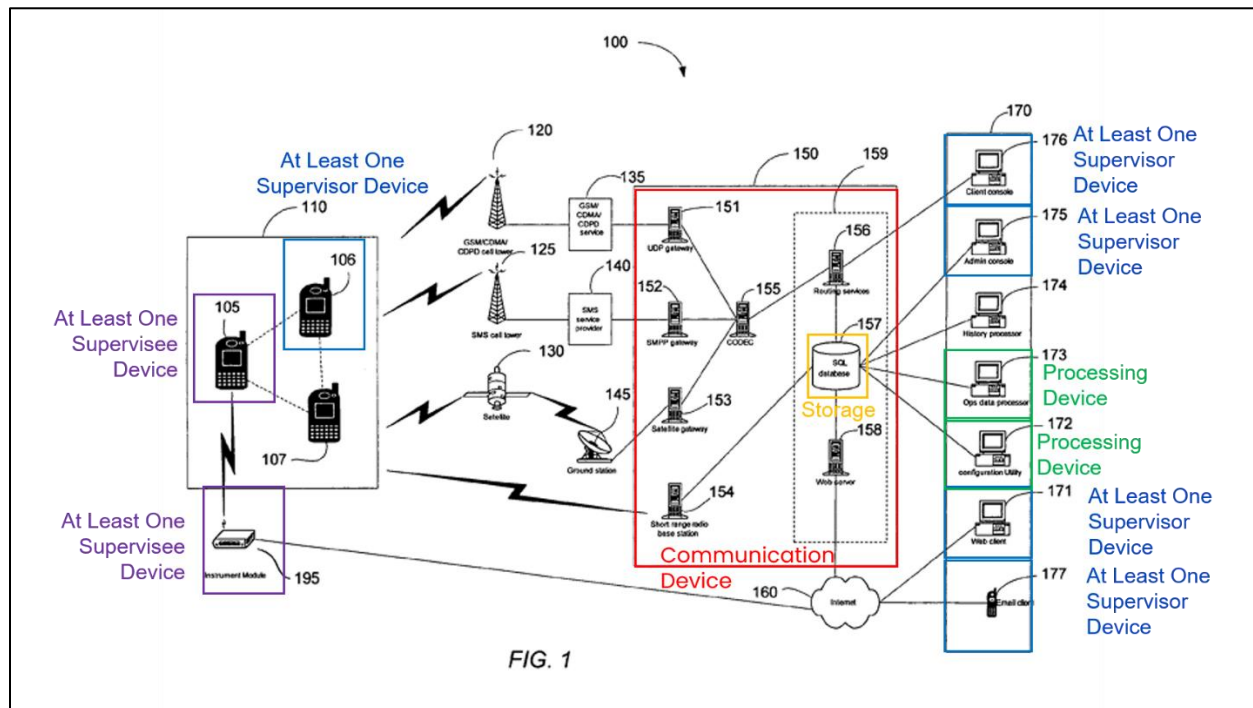


b. 1[a] “receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor;”

Staton discloses this limitation. EX[1005], ¶¶158-161.

Applicant’s §112(f) “**communication device**” is disclosed by Staton’s backend control system’s communication components—the functions, including programs, middleware, and software, running in the gateways, routing services, databases, web server, networks, and codec—that handle messaging between server-side components and client devices (red below). EX[1007], 6:44-48, 6:66-7:23; *id.* 7:6-15. Staton renders obvious that the communication device components are implemented on a common server, specifically suggesting and motivating that the

various parts of backend control system on a single computer system, with a reasonable expectation of success. EX[1007], 19:62-67 (“backend control system 150 can be configured to run on any combination of computer servers,” including where communication gateways “run on a common computer system”), Fig. 6; EX[1005], ¶¶141-149.

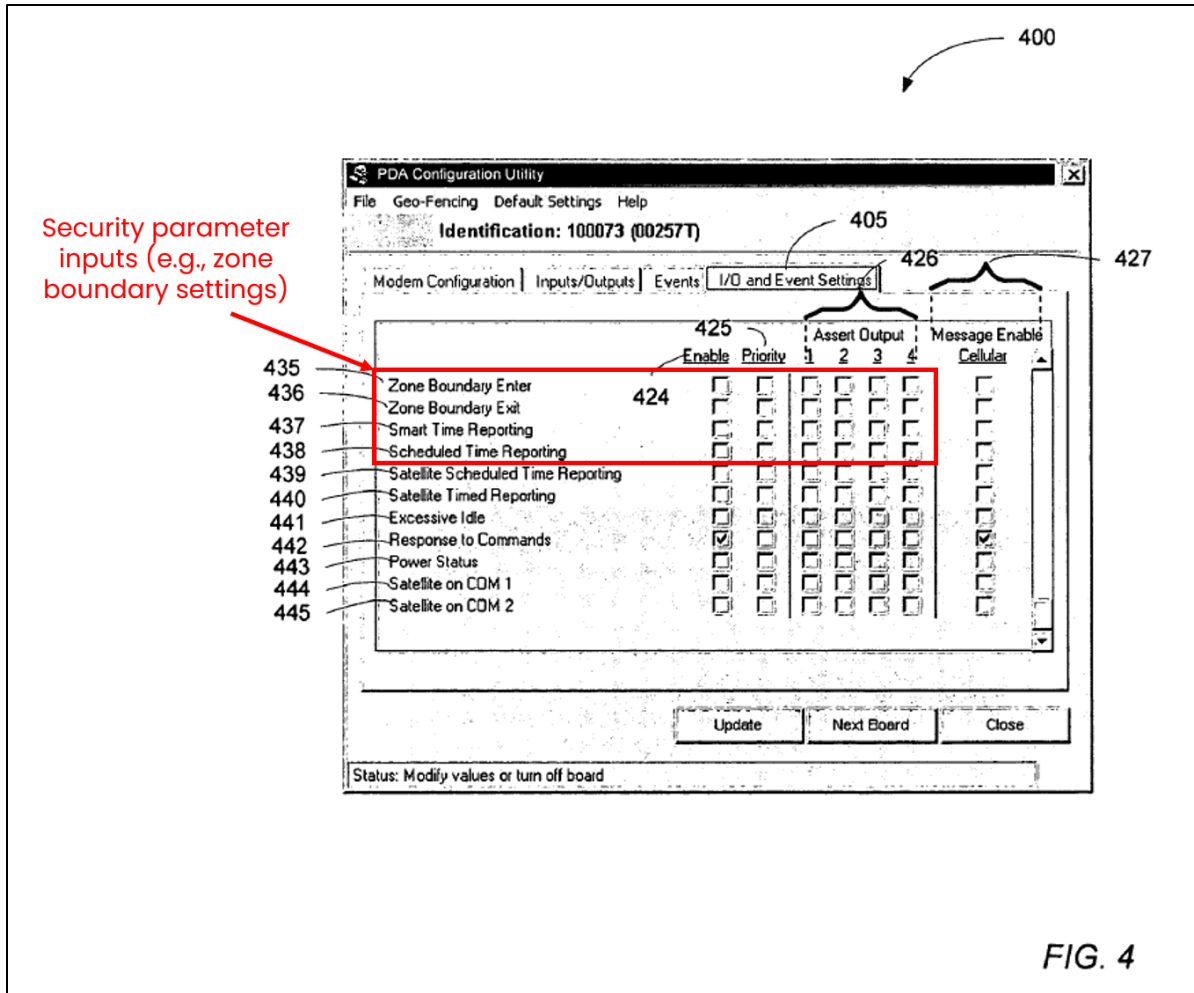


The “at least one security parameter” corresponds to the properties and rules associated with Staton’s geographical zones, *e.g.*, “a name, description and a flag determining if the zone is an off-limits zone or an enclosed zone.” EX[1007], 14:53-55. Security parameters also include “speed threshold,” “a ‘no-fly zone,’ flag,” “color coded “security threat,” *id.* 16:13-17, or configurable events such as “Zone Boundary Enter 435, Zone Boundary Exit 436, and Smart Time reporting 437

or Scheduled Time reporting 438,” *id.* 11:50-53. These zone properties, event rules, thresholds, and settings govern the supervisory monitoring behavior of the system and are “security parameters.”

The “**at least one supervisor device associated with at least one supervisor**” includes devices (blue above) that supervisors use for configuration and monitoring individuals, including PDA 106 (monitoring PDA), home computer (not depicted), web client 171, and client and administrator consoles 176 and 175. *See* EX[1007], 7:25-33; 15:17-22; 17:26-33; 24:12-25; EX[1005], ¶¶113, 150-153, 158.

In operation, Staton’s communication device “**receiv[es]**” the security parameters from the supervisor device. EX[1005], ¶160-161. The supervisor device’s user interface permits configuring the PDA through fields, checkboxes, and radio buttons, including entering zone boundaries, priority events, time reporting, event outputs, and messaging events. EX[1007], 11:27-50, 27:66-28:2. These parameters are sent to the backend control system’s communication components (**communication device**) for processing. *Id.* 11:27-50, 25:60-62.

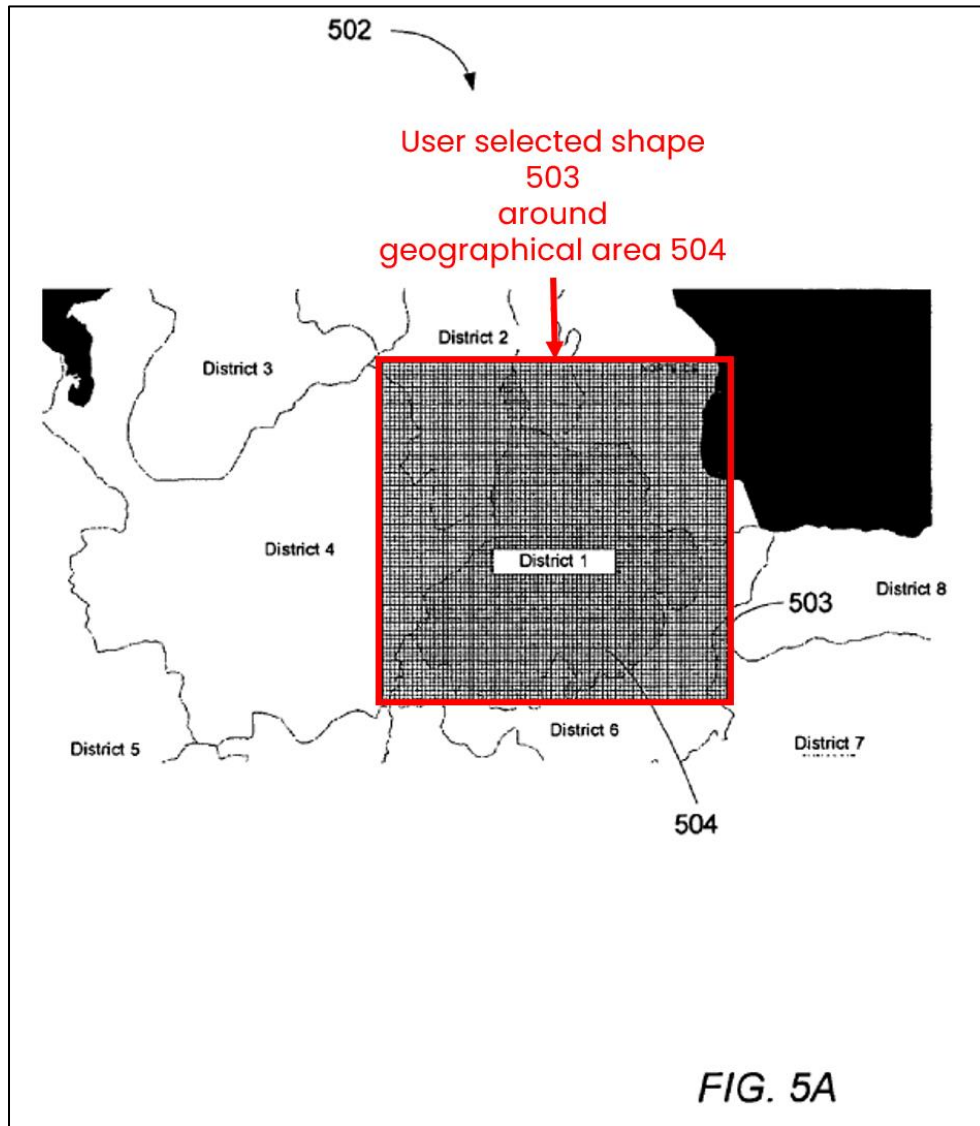


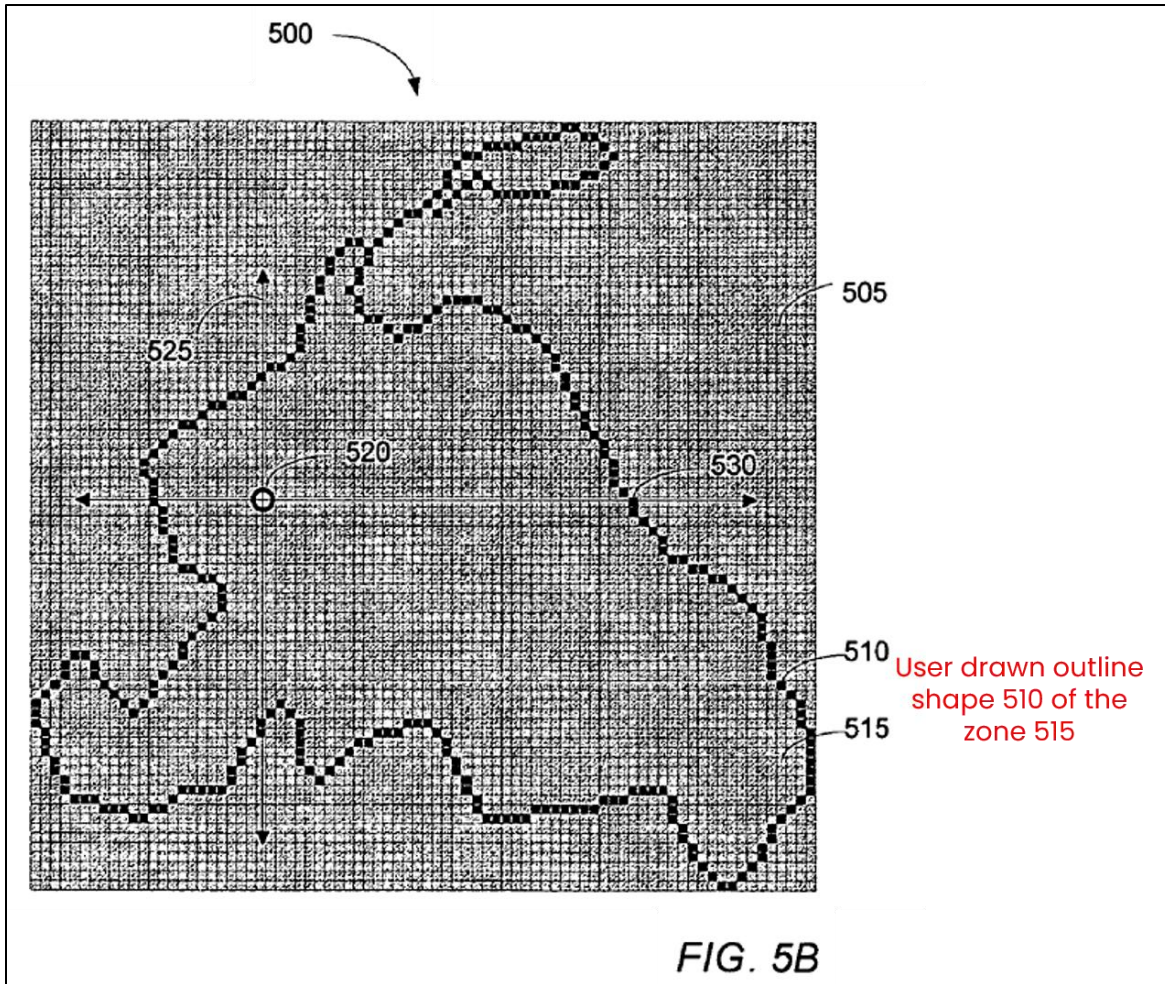
c. 1[b] “receiving, using the communication device, a geographical location from the at least one supervisor device;”

Staton discloses this limitation. EX[1005], ¶¶162-163.

The “**geographical location**” corresponds to the geographical areas/coordinates the supervisor defines to create geographical zones (examples below). *Id.* For example, “a geographical zone may be created by selecting a plurality of coordinates ...,” EX[1007], 14:56-59, or by “display[ing] a map on which the user selects a rectangular shape 503 around the geographical area 504 that

the user desires to define,” *id.* 15:27-30. *See also id.* 2:49-52 (“geographical zone” can be home, work, school, state, city, etc.), 6:14-22, 14:22-24 (“constructed through a combination of waypoints and/or zones”), 14:33-35 (“[E]ach waypoint defined by a coordinate and a radius.”).



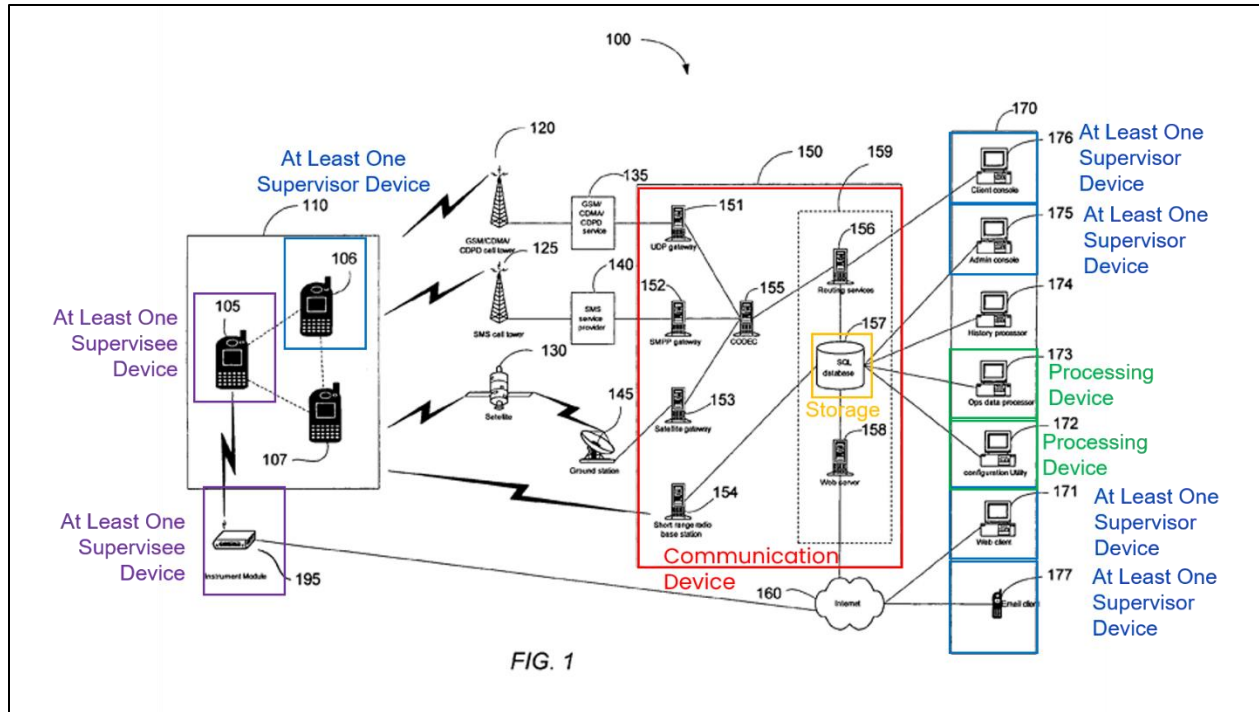


The geographical information is “receiv[ed], using the communication device” (communication components of backend control system) “from the at least one supervisor device” (supervisor functionality including home computer). EX[1005], ¶¶161-163; §VII.A.1.b. A supervisor inputs the geographical location using a home computer or other supervisor device, which connects to the configuration utility through a secure connection or web browser. EX[1007], 15:17-23, 27:26-27, 27:52-54, 27:66-28:2. The selected location is transmitted through

communications components of the backend control system (**communication device**) to the configuration utility. EX[1005], ¶163.

d. 1[c] “analyzing, using a processing device, the geographical location based on the at least one security parameter;”

Staton discloses this limitation. EX[1005], ¶¶164-167. Staton’s §112(f) “**processing device**” is disclosed by Staton’s processing components including operations data processor 173 and configuration utility 172 (green below), and response, notification, and event routers (not shown) which build and process geographical zones and notifications based on supervisor input. EX[1007], 15:4-9 (“Waypoints and zones are built by the operations data processor 173.”); 11:48-50 (“The user interface may be part of an application that resides in the configuration utility 172 (FIG. 1).”); 15:25-31 (“configuration application displays a map on which the user selects a rectangular shape 503”). It would have been obvious to implement the processing device on the same server as the communications device—indeed, Staton motivates that, as described for limitation 1[a]. §VII.A.1.b; EX[1005], ¶¶148-149. Staton’s processing device tracks the processing device in the ’757 Patent—both comprise one or more computing devices comprising hardware or software. EX[1001] 6:28-29, 28:59-29:14.

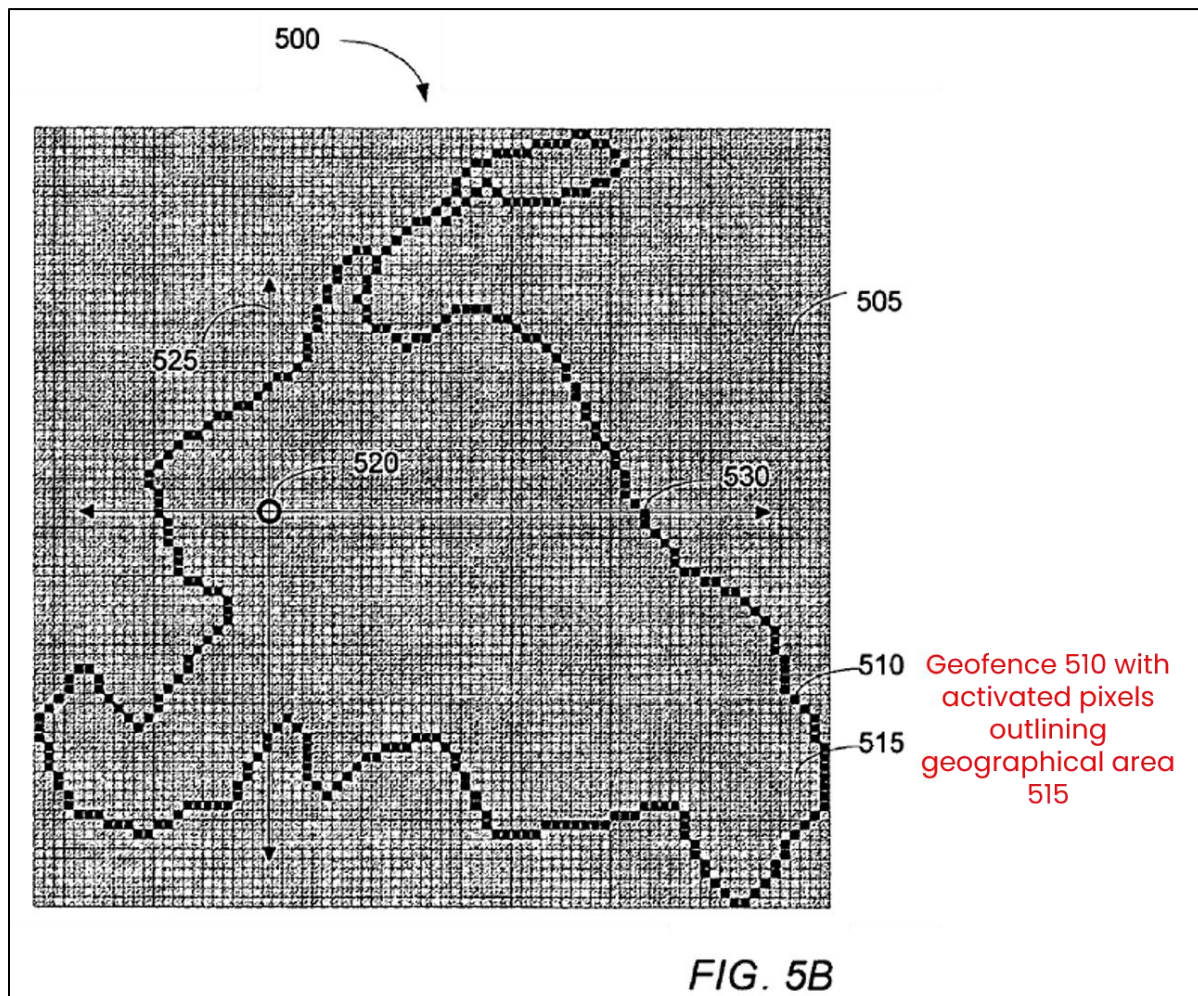


Staton discloses the processing device “**analyzing...the geographical location based on the at least one security parameter**” because the operations data processor and configuration utility process the supervisor-selected location using the zone’s security parameters to build the geographical zone to control the kind of zone generated and how it is analyzed. EX[1005], ¶¶164-166. For example, the off-limits/enclosed flag determines whether the resulting zone is a restricted or contained area. EX[1007], 14:53-55; EX[1005], ¶166. Other security parameter inputs likewise affect which locations are designated and how the zone operates by the operations data processor: danger levels identify unsafe areas, and speed or time thresholds help detect boundary crossings and schedule deviations. EX[1007], 16:14-15, 28:52-56, 11:59-67, 5:10-14; EX[1005], ¶¶166-167.

- e. 1[d] “generating, using the processing device, a geofence corresponding to a geographical area based on the analyzing;”

Staton discloses this limitation. EX[1005], ¶168-171; §V.

The “**geofence**,” shown below, is outline shape 510 of zone 515 in pixel map 500—a virtual boundary defined by pixels or coordinates for a real-world area. EX[1007], 2:53-65, 16:47-52. It also includes associated settings, such as triggering alerts upon entry or exit. *Id.* 14:1-3; 15:31-34.



The geofence is “**generat[ed], using the processing device,**” *e.g.*, the configuration utility and operations data processor, as described for limitation 1[c]. EX[1007], 15:4-5, 16:43-52, 26:39-41 (“Geofences can be waypoints, zones, routes, or a collection of waypoints...”). Staton confirms those server-side processing components generate the geofence: “Waypoints and zones are built by the operations data processor 173,” and the pixilated image may be “created in the configuring computer” and “simply loaded onto the PDA 105,” so that “the PDA 105 does not need to build or construct the image by itself.” *Id.* 15:4-5, 16:53-56. It is “**based on the analyzing**” because those components build the zone from the selected area and associated parameters, including off-limits/enclosed flags, speed thresholds, and event configurations. *Id.* 14:53-55, 16:13-20.

f. I[e] “receiving, using the communication device, at least one supervisee data associated with a supervisee from at least one supervisee device;”

Staton discloses this limitation. EX[1005], ¶¶172-174.

The “**at least one supervisee device**” is the device carried by/associated with the monitored individual (the supervisee), *e.g.*, PDA 105. *Id.* The “**at least one supervisee data**” is Staton’s geocoded location data, event messages, and other information transmitted from the supervisee device to the communication components of backend control system 150 (“**receiving, using the communication device**”). *Id.* For example, “the PDA 105 communicates with one of the plurality of

base stations 120, which in turn communicates with the service provider 135,” which sends data to backend control system 150 to “map[] the correct destination if any” for sending a notification. EX[1007], 8:14-19.

The data received by the backend control system constitutes “**supervisee data associated with a supervisee**” because it includes the monitored individual’s location and event data. EX[1005], ¶¶173-174; EX[1007], 16:18-23 (supervisee data including whether supervisee is in a geofence is transmitted from PDA 105), 8:11-14, 28:5-12, 29:19-30.

g. 1[f] “analyzing, using the processing device, the at least one supervisee data based on the geofence;”

Staton discloses this limitation. EX[1005], ¶175-190.

The response and notification routers of the backend control system (parts of the “**processing device**,” *see* §VII.A.1.d) **analyze supervisee data** in two ways:

(1) They analyze whether/to whom a supervision notification should be sent; *e.g.*, “[t]he remote notify router 681” receives geocoded location and event information and queries the resources database to determine whether a notification is required. EX[1007], 22:22-28. The analysis is “**based on the geofence**” because the data reflects geofence events such as entering or leaving a geofence. *Id.* 14:2-4, 14:12-13, 13:65-66.

(2) They analyze if a supervisor client console is tracking the supervisee PDA; *e.g.*, for an inbound event, the response router determines whether client

console is tracking the supervisee PDA and requires notification. *Id.* 21:47-51. That analysis is likewise “**based on the geofence**” because the console tracks PDAs within a waypoint or geographical zone. *Id.* 21:47-51, 17:30-33, 17:48-52.

To the extent PO asserts that this limitation requires a server-side comparison of the supervisee’s real-time location with the geofence boundary, that is not required, but Staton also renders that obvious. EX[1005], ¶180. In Staton, the supervisee’s PDA already performs this “simple calculation” using GPS data, loaded zones, and event data, but Staton is silent as to whether the server-side processing devices also perform the comparison. EX[1007], 16:6-9, 16:57-61, 26:44-50. A POSITA would have been motivated to add that functionality for performing the comparison at the server in addition to the client (1) for redundancy with the PDA calculation or (2) to allow the system to operate with lower-power client devices, or to conserve client battery power. EX[1005], ¶¶181, 185-187. A POSITA would have had a reasonable expectation of success in making this modification because the Staton server already receives the supervisee data, has the geofence map, and includes the geofencing software used by the PDAs. *See* §§VII.A.1.e-f (limitations 1[d]-1[e]); EX[1007], 26:63-65; EX[1005], ¶¶182-189. Moreover, selecting the server, the client, or both to perform the comparison of a supervisee’s location with the geofence boundary would have been a routine design choice well understood by

a POSITA. EX[1005], ¶188. Indeed, the '757 Patent itself recognizes that “one or more steps of the method may be performed by a server computer” or “a client computer,” EX[1001], 8:60-62, and expressly discloses that the server can be used to analyze data such as supervisee data, where it explains “the server 4108, in an instance, may be configured to analyze the location data.” *Id.* 25:40-41; *id.* 6:56-59 (“[T]he server computer may include a processing device configured for performing data processing tasks such as, for example, but not limited to, analyzing, identifying, determining, generating....”).

h. 1[g] “generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data;”

Staton discloses this limitation under either analysis method described below, as well as the alternative obviousness rationale described in limitation 1[f], EX[1005], ¶¶190-194:

(1) After analyzing geocoded location and event information, remote notify router 681 (portion of **processing device**) generates a **supervision notification** by formatting and encoding a message. EX[1007], 22:22-33. The notification is “**based on the analyzing**” of the **supervisee data** because the router generates it only after determining that the incoming event requires notification. *Id.*

(2) After determining that client console is tracking the PDA, response router 620 (portion of **processing device**) **generates a supervision notification** by routing the event message to that console. *Id.* 21:47-53. The notification is “**based on the analyzing**” of the **supervisee data** because the router tracks supervisee PDAs within a waypoint or geographical zone. *Id.* 17:30-33, 17:48-52.

- i. I[h] “transmitting, using the communication device, the supervision notification to the at least one supervisor device; and”*

Staton discloses this limitation for either notification pathway described in limitation 1[g]. EX[1005], ¶¶195-197:

(1) After remote notify router 681 formats and encodes the notification, the message enters the outbound SMTP or SMS queue and is sent through the corresponding gateway. EX[1007], 22:33-36. Those gateways are part of the backend control system’s **communication device** and **transmit** the message (**supervision notification**) to PDA 106 or another monitoring device (the “**at least one supervisor device**”). *Id.* 8:11-14, 8:21-25, 29:55-57.

(2) Response router 620 **transmits** the incoming message to client console 176 (**supervisor device**) through the backend control system’s communication networks (**communication device**). *Id.* 21:49-51; *see also id.* Fig. 6; EX[1005], ¶197.

j. 1[i] “storing, using a storage device, the at least one supervisee data and the supervision notification, wherein:”

Staton discloses this limitation. EX[1005], ¶¶198-199.

Applicant’s §112(f) “**storage device**” is the history recorder 641 and history database 642 and associated storage infrastructure (*e.g.*, history queue 640, resources database) within Staton’s backend control system. *Id.* It would have been obvious to implement the storage device on the same server as the communications and processing device—indeed, Staton motivates that, as described for limitation 1[a]. §VII.A.1.b; EX[1005], ¶¶148-149.

The history database stores “**supervisee data**” (geocoded location data and incoming messages from PDA 105) and “**supervision notifications**” (outbound event messages). *Id.* “[H]istory queue 640 receives the inbound [**supervisee data**] and outbound messages [**supervision notifications**] for all PDAs 105 and all of the messages from the instrument module 195” (EX[1007], 22:5-8), from which they are “fed...to the history recorder 641” and then “saved in a history database” for “reporting and statistical analysis” (*id.* 22:7-12). *Id.* 19:56-59 (“The history database 642 maintains records of all events and transactions....”).

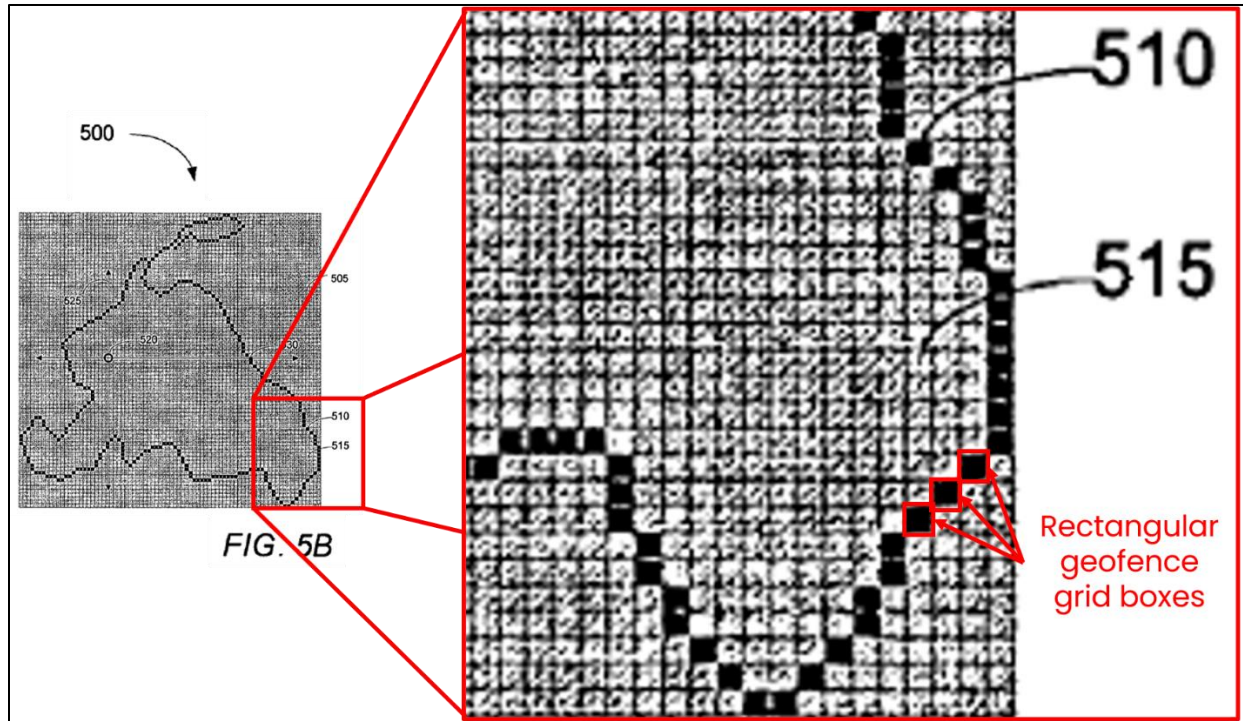
k. 1[j] “the geofence is characterized by a geofence area corresponding to the geographical area, wherein the geofence comprises a plurality of geofence grid boxes associated with the geofence area, wherein each geofence grid box is

characterized by a grid box geofence area of the geofence area, wherein the method comprises: ”

Staton discloses this limitation. EX[1005], ¶¶200-201.

Staton’s geofence is the outline shape 510 and zone 515 as represented in the pixel map 500. *See* §VII.A.1.e (limitation 1[d]). The “**geofence area corresponding to the geographical area**” is the area within the activated pixel boundary—*i.e.*, the zone 515 in outline shape 510—and corresponds to the geographical area. EX[1007], 16:49-51, 26:34-39.

Staton discloses “**the geofence comprising a plurality of geofence grid boxes associated with the geofence area,**” specifically, “dividing the identified geometrical area into a grid, allowing a user to select at least one section from within the grid in order to define a geographical area” (*id.* 3:10-12) and that the grid consists of “smaller rectangles” (grid boxes) that are mapped to pixels (*id.* 15:27-34) because “each pixel 505 is a square” box (*id.* 16:49). “These squares” (**geofence grid boxes**) “are then used to draw the outline shape 510 of the zone 515” (**geofence**), as annotated below. *Id.* 16:50-51.



Staton also discloses that “**each geofence grid box is characterized by a grid box geofence area of the geofence area,**” specifically that “a geographical area is...mapped to each pixel 505 of the pixel map 500” such that each pixel is a defined portion of the geographical zone 515. *Id.* 16:50-51. In the above example, the activated pixels collectively define the geofence area, and each activated pixel is a grid box geofence area of that geofence area. *Id.* 15:33-34 (“Each pixel in the grid can be activated to be part of the geographical zone.”); *id.* 2:57-65, 15:66-16:4.

- l. *1[j][1]* “receiving, using the communication device, at least one grid parameter from the at least one supervisor device, wherein the processing device is further configured for:”

Staton discloses this limitation. EX[1005], ¶¶205-207.

The “**at least one grid parameter**” is the resolution of the area definition selected through Staton’s configuration application:

The user can also select the resolution of the area definition. In other words, when the selected area is subdivided into a grid of rectangles, the grid includes a much higher number of vertical and horizontal lines, thus increasing the number of grid rectangles obtained from the subdivision. The increase in number [of] rectangles increases the resolution because each rectangle covers less geographical area. A user who desires to have great detail in defining the area may reduce the size of the grid rectangles and thus increase resolution of the area.

EX[1007], 15:46-55. This resolution parameter determines the grid’s granularity by determining the number and size of the geofence grid boxes, just as the claim recites.

EX[1005], ¶¶206-207; *see also* EX[1007], 14:34-44.

The grid parameter is “**receiv[ed]...from the at least one supervisor device**” **using** the backend control system’s communication infrastructure (“**communication device**,” *see* §VII.A.1.b (limitation 1[a])): the home computer connects to the configuration utility through the Internet or a secure connection, and device configuration is entered through the backend. EX[1007], 15:17-23, 25:60-63. Indeed, resolution selection is part of configuring zones, and Staton expressly teaches that configuring zones is performed by a supervisor (*e.g.*, parent): “[t]he parent may utilize the configuration software to delineate specific areas where the

son can travel,” and “area boundaries...are determined by the parents and can be changed at any time through the internet/cellular system.” *Id.* 27:52-54, 27:66-28:2; EX[1005], ¶¶205-207.

m. 1[j][2] “analyzing, using the processing device, the at least one grid parameter;”

Staton discloses this limitation. EX[1005], ¶¶208-209. When the user selects the resolution (“**grid parameter**”), the configuration application (part of the “**processing device**,” §VII.A.1.d (limitation 1[c])) **analyzes** that resolution value to determine how to subdivide the geographical area into a grid of rectangles. EX[1007], 15:4-15, 15:46-16:4. This processing is reflected in Staton’s explanation that when a higher resolution is selected, “the selected area is subdivided into a grid of rectangles, [and] the grid includes a much higher number of vertical and horizontal lines, thus increasing the number of grid rectangles obtained from the subdivision.” *Id.* 15:47-50. The resolution directly controls the number of grid lines and the resulting rectangle sizes, and “[t]he increase in number [of] rectangles increases the resolution because each rectangle covers less geographical area,” *id.* 15:51-52, so the grid dimensions are determined from the resolution parameter before generating the grid. EX[1005], ¶¶66, 209. The processing device **analyzes** the resolution, *e.g.*, converts the user-selected resolution value into specific grid dimensions (number of vertical and horizontal subdivisions, area per rectangle). EX[1005], ¶¶65-66, 209, 214. Indeed, the ’757 Patent itself confirms that

“analyzing” a grid parameter requires nothing more than processing it to determine grid box geofence areas, *see* EX[1001], 14:30-45 (Fig. 5 flowchart: analyzing grid parameter, then determining grid box geofence area based on the analyzing), and Staton’s resolution-to-grid computation performs precisely that function. *See* §VII.A.1.1 (limitation 1[j][1]).

n. 1[j][3] “determining, using the processing device, the grid box geofence area based on the analyzing of the at least one grid parameter; and”

Staton discloses this limitation. EX[1005], ¶¶210-214. Based on the resolution (**grid parameter**) analysis, the **processing device determines the grid box geofence area**—the geographical area represented by each pixel or grid box. EX[1005], ¶¶211-214. The resolution controls how finely the geographical area is subdivided (EX[1007], 15:46-55, 16:2-4), so Staton discloses the determining based on the analyzing because higher resolution means each grid rectangle covers less area (and vice versa). EX[1007], 15:46-55 (“A user who desires to have great detail in defining the area may reduce the size of the grid rectangles and thus increase resolution of the area”), 16:2-4; §VII.A.1.1.

o. 1[j][4] – “generating, using the processing device, a number of geofence grid boxes based on the determining.”

Staton discloses this limitation. EX[1005], ¶¶215-217. The processing device “**generat[es]...a number of geofence grid boxes**” by dividing the rectangle into a grid of smaller rectangles. EX[1007], 15:31-34, 16:48-49. The number is “**based on**

the determining” because higher resolution yields more rectangles, each covering less area. EX[1007], 15:48-65; EX[1005], ¶¶215-217.

2. Claim 2

- a. 2[a] “receiving, using the communication device, at least one location indication associated with the geographical area from the at least one supervisor device;”*

Staton discloses this limitation. EX[1005], ¶¶218-220.

The “**location indication associated with the geographical area**” is a parent-designated (supervisor-designated) permissible or non-permissible area, unsafe neighborhood, or predefined travel path (*e.g.*, designated “specific areas where the son can travel,” “non-permissible travel...outside of city limits,” “regular paths of travel from home to school and back”). EX[1007], 27:27-32, 27:52-57, 28:52–56. Each is “**receiv[ed]...from the at least one supervisor device**” using the “**communication device**” of backend control system, as with limitation 1[a]. *Id.* 25:60-62, 27:66-28:2; EX[1005], ¶220; §VII.A.1.b.

- b. 2[b] “identifying, using the processing device, at least one location corresponding to the at least one location indication;”*

Staton discloses this limitation. EX[1005], ¶221.

Operations data processor and configuration utility of backend control system 150 (part of the **processing device**) **identify a location corresponding to each indication** by translating the location indication into coordinates, a zone, route, or pixel map (*e.g.*, “[w]aypoints and zones” or non-permissible areas are built from the

parent's indications by the "operations data processor" and "loaded on to the PDAs with the configuration utility"). EX[1005], ¶221; EX[1007], 14:56–59, 15:4–9.

c. 2[c] "analyzing, using the processing device, the at least one supervisee data based on the at least one location; and"

Staton discloses this limitation for both types of analysis described in limitation 1[f]. EX[1005], ¶¶222-224.

(1) Remote notify router 681 (part of the **processing device**) analyzes supervisee event data (**supervisee data**) based on the identified location to determine notification requirements. *Id.* When a supervisee enters an unsafe neighborhood, deviates from a predefined path, or crosses a non-permissible area, the remote notify router receives the geocoded location and event information and "queries the resources database 670 to find out" if the event/configuration "requires a notification." EX[1007], 16:18-23, 22:22-28, 27:29-32.

(2) Response router 620 (part of the **processing device**) **analyzes** the data (**supervisee data**) **based on the location** by determining whether client console 176 is tracking the supervisee PDA in relation to the designated location and, if so, routing the event message to that console. *Id.* 21:47–51, 17:48-52 (client console allows viewing "all PDAs that are within a waypoint" or "within a geographical zone"); EX[1005], ¶223.

To the extent PO asserts that this limitation requires a server-side comparison of the supervisee's real-time location with the geofence boundary, Staton also renders that obvious for the same reasons explained in element 1[f]. EX[1005], ¶224; §VII.A.1.g.

d. 2[d] “determining, using the processing device, a location anomaly based on the analyzing of the at least one supervisee data based on the at least one location, wherein the generating of the supervision notification is based on the determining.”

Staton discloses this limitation. EX[1005], ¶¶225-226.

The “**determining, using the processing device, a location anomaly based on the analyzing of the at least one supervisee data based on the at least one location**” is the determination of a path deviation or entry into a prohibited or unsafe area relative to the supervisor-designated locations in limitation 2[a]. §VII.A.2.a; EX[1007], 27:29–32 (if daughter “deviates from such predefined paths,” a signal is sent “indicating a warning of path deviation”), 28:52–55 (“event alarms indicating that the unsafe neighborhood has been entered”), 28:8–17 (if supervisee “leaves the area, an event is immediately sent” to supervisor).

The “**generating of the supervision notification is based on the determining**” because detecting the anomaly triggers the notification pathways described for 1[g]-1[h]: remote notify router 681 formats and encodes the message, and/or response router 620 routes it to tracking console 176. EX[1007], 22:28-33, 21:47-51; EX[1005], ¶¶225-226; §§VII.A.1.h-i.

To the extent PO argues that the path-derivation or zone-entry determination must be performed by the server-side processing device rather than the PDA, it would have been obvious to perform it at the backend for the same reasons explained for limitation 1[f], particularly because Staton's control center already hosts the geofencing and event software. EX[1007], 26:62-72; §VII.A.1.g; EX[1005], ¶226.

3. Claim 3

- a. 3[a] “the supervision notification comprises at least one supervisee event, wherein the at least one supervisee event is associated with at least one action, wherein the method comprises:”*

Staton discloses this limitation. EX[1005], ¶227. Staton's **supervision notification** comprises **supervisee event** data, including “event reason or source, and any other relevant information.” EX[1007], 16:18–23; §§VII.A.1.h-i. The **supervisee event is associated with an action** because waypoint and zone events are “configurable to take one or more actions,” *e.g.*, trigger “making a telephone call, reporting to a control center, or starting an alarm.” EX[1007], 3:19–21, 16:32-33; EX[1005], ¶227.

- b. 3[b] “determining, using the processing device, the at least one action based on the supervision notification; and”*

Staton discloses this limitation. EX[1005], ¶228. After receiving the supervision notification, the **processing device** (processing components of backend control system 150, *see* §VII.A.1.d (limitation 1[c])) **determines the** action by “look[ing] up the correct PDAs...and other parties that must be contacted, such as

the police or 911” in resources database 670 and determining whether the event requires notification. EX[1007], 26:65–27:3, 22:22-28; EX[1005], ¶228.

- c. 3[c] “performing, using the processing device, the at least one action based on the determining, wherein the at least one action comprises an establishment of a communication session between the at least one supervisor device and the at least one supervisee device.”*

Staton discloses this limitation. EX[1005], ¶229. The remote notify router (part of the **processing device**) **performs the action** by processing the event, identifying the recipient, “format[ing] and encod[ing] the message,” and placing it in the outbound queue for transmission through the appropriate gateway. EX[1007], 22:28-36, 26:51-61 (message is “processed and analyzed to find out the final recipient”), 23:58-60, 24:60-64, 8:21-23 (backend “reroutes an event message, text message or any other information originating from PDA 105 to PDA 106”); EX[1005], ¶229. That rerouting **establishes a messaging session between the supervisee device (PDA 105) and the supervisor device (PDA 106)** through the backend. EX[1007], 8:21-25, 23:57-60.

In addition, when a supervisor receives notice that a child’s PDA deviated from a predefined path, the parent can call the child (**establishment of a communication session between supervisor device (parent’s PDA) and supervisee device (child’s PDA)**). EX[1007], 27:32-34; EX[1005], ¶229. To the extent PO argues the parent’s call is not “performed” “using” the processing device, it would

have been obvious to have the backend automatically initiate that call or message session upon a path-deviation event, as Staton already teaches “executing a pre-programmed operation such as making a telephone call.” EX[1007], 3:19-21; EX[1005], ¶229.

4. Claim 4

- a. 4[a] *“identifying, using the processing device, the supervisee based on the analyzing of the at least one supervisee data; and”*

Staton discloses this limitation. EX[1005], ¶¶230-232.

When the **processing device** of the backend control system 150 “processes a received message by one PDA,” it “relay[s] the data in the message to the correct PDA.” EX[1007], 24:64-67. This **identifies the supervisee based on the analyzing** of incoming **supervisee data** (PDA identification, location, and event information). EX[1005], ¶232.

Response router 620 (of the **processing device**) **identifies the supervisee** PDA by “determin[ing] if a client console 176 is tracking PDA 105” associated with the incoming event. EX[1007], 21:47–50; EX[1005], ¶231. Remote notify router 681 (of the **processing device**) likewise **identifies the supervisee by** “query[ing] the resources database 670 to find out if the configuration information or event information received requires a notification.” EX[1007], 22:22–28, 21:47-50; EX[1005], ¶232.

- b. 4[b] “retrieving, using the storage device, supervisee profile data associated with the supervisee based on the identifying, wherein the generating of the supervision notification is based on the retrieving.”

Staton discloses this limitation. EX[1005], ¶233. **Based on identifying the supervisee, the operations data processor (of the processing device) retrieves supervisee profile data** from resources database 670, part of the backend storage infrastructure, *see* §VII.A.1.j (limitation 1[i])). EX[1007], 24:12–16. The database stores “relational information of members and accounts” and “which PDAs are associated with which PDAs” (**supervisee profile data associated with the supervisee**). *Id.* 24:12-16, 24:60-64; EX[1005], ¶233.

The “**generating of the supervision notification is based on the retrieving**” because the remote notify router 681 (part of the **processing device**) then 'uses the retrieved profile data to determine whether and to whom to send notification, if so, “retrieves the contact information” before formatting and encoding the notification. EX[1007], 22:25–33; EX[1005], ¶233.

5. Claim 6

- a. 6[a] “receiving, using the communication device, at least one environment data associated the geographical area corresponding to the geofence;”

Staton discloses this limitation. EX[1005], ¶¶234-235.

Instrument module 195 connects to sensors measuring **environment data associated with a geographical area corresponding to the geofence**, including

“the levels of carbon monoxide, chlorine, smoke, smog, oxygen in the air, or temperature.” EX[1007], 3:35-37; *id.* 5:15-18. The sensors are zone-specific because the PDA “load[s] a specific configuration for that Zone such that it interacts with Zone-specific instruments” operating there. *Id.* 14:4–11.

The backend control system’s **communication device** receives this environment data from instrument module 195 through an Internet or other network connection. *Id.* 7:65-8:8, 19:25-36 (backend control system 150 receives a measurement of “high levels of smoke” and relays to the PDA); EX[1005], ¶235.

- b. 6[b] “analyzing, using the processing device, the at least one environment data; and determining, using the processing device, at least one threat based on the analyzing of the at least one environment data, wherein the generating of the supervisor notification is based on the determining.”*

Staton discloses this limitation. EX[1005], ¶¶236-237.

The **processing device analyzes the environment data** (in remote notify router of processing device), **determines a threat based on the analyzing** from dangerous smoke, carbon monoxide, or other conditions, and **generates a notification** reporting the threat **based on the determining**. *Id.* Remote notify router 681 “receives the geocoded location and event information,” “queries the resources database 670” to determine if notification is required, “retrieves the contact information for the appropriate PDA,” and “formats and encodes the message.” EX[1007], 22:16–36, 19:15-19 (environmental emergencies would be a “priority

message”); EX[1005], ¶236; §§VII.A.1.h-i, VII.A.5.a. Staton discloses that the initial determination of an event for a hazardous condition based on sensor data occurs in Staton’s PDA, but Staton’s backend remote notify router also determines a threat by receiving the event information and determining if a notification is required. EX[1005], ¶237.

To the extent PO argues that the initial determination of a hazardous event must occur on the backend server, it would have been obvious to do so in addition or as an alternative to PDA-processing, for the same reasons as described in limitation 1[f] (*i.e.*, redundancy, compatibility with lower-power client devices, or to conserve PDA battery power). EX[1005], ¶237; §VII.A.1.g. The environmental data already reaches the backend, whose processing device includes geofencing and event-processing software, giving a POSITA a reasonable expectation of success in making this straightforward modification. EX[1007], 7:65-8:8, 19:25-36, 26:52–61; EX[1005], ¶237; §VII.A.1.g.

6. Claim 8

a. 8[a] “the at least one supervisee device comprises at least one sensor”

Staton discloses that the **supervisee device** (*e.g.*, PDA 105) can **comprise** (“be in the same housing”) a **sensor** instrument module 195, which can, *e.g.*, monitor health signals (*e.g.*, “a heart monitor, an insulin level reader, blood pressure monitor, etc.”). EX[1007], 10:33-35, 8:38-40, 8:45-46; EX[1005], ¶238.

b. 8[b] “wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,”

The sensor instrument module of Staton can **detect** physiological **signals made by the supervisee** (*e.g.*, heartbeat, blood glucose, blood pressure). EX[1007], 8:46–48, claim 3 (monitored events include “poor health condition of the individual carrying the first portable device...”); EX[1005], ¶239.

c. 8[c] “wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting.”

The sensor instrument module of Staton **generates supervisee data based on the detected signal**; *e.g.*, “the instrument module 195 is equipped with logic that determines if the measurement taken has surpassed a predetermined threshold, and if so, the instrument module 195 transmits an event message [**supervisee data**] to the PDA 105.” EX[1007], 12:16-20; EX[1005], ¶240.

7. Claim 10

Claim 10 is a system claim corresponding in large part to method claim 1. Staton discloses a “**system for facilitating supervision of individuals based on geofencing**” (10[pre]), as described for 1[pre]. §VII.A.1.a. Claim 10’s other limitations are also invalid for largely the same reasons as claim 1, as set forth below:

10[a] “a communication device configured for: receiving...receiving...receiving...and transmitting...” See §VII.A.1.b (limitation 1[a] regarding communication device). Functions 10[a][1]-10[a][4] are also invalid

for the same reasons as 1[a]-1[b], 1[e], and 1[h]. §§V, VII.A.1.b-c, f, i; EX[1005], ¶¶242-246. Staton also discloses the recited “**supervisor** data...from at least one supervisee device”: the backend receives event data from PDA 105 associated with the supervisee and routes it to supervisor devices, so also includes supervisor data. EX[1007], 8:14-25; EX[1005], ¶¶241-246.

10[b] “a processing device configured for: analyzing...generating...analyzing...and generating....” See §VII.A.1.d (limitation 1[c] regarding processing device). Functions 10[b][1]-10[b][4] are invalid for the same reasons as 1[c]-1[d] and 1[f]-1[g]. §§V, VII.A.1.d-e, g-h; EX[1005], ¶¶247-252.

10[c] “a storage device configured for storing...” See §VII.A.1.j (limitation 1[i] regarding storage device). Function 10[c] is invalid for the same reasons as 1[i]. §§V, VII.A.1.j; EX[1005], ¶253.

10[d] grid-based limitations. The grid limitations 10[d], 10[d][1]-[4] are invalid for the same reasons as 1[j], 1[j][1]-[4]. §§VII.A.1.k-o. Staton also receives the grid parameter through the backend communication infrastructure, satisfying 10[d][1]. §VII.A.1.l.

If PO argues the three devices must be implemented in one server computer, Staton makes that arrangement obvious: Staton encourages and motivates implementing the various parts of the backend control system on a single computer

system, with a reasonable expectation of success, as described for limitation 1[a].
EX[1007], 19:62-67; §VII.A.1.b; EX[1005], ¶¶140-149, 254-259.

8. Claim 11

Claim 11[a]-[d] corresponds to claim 2[a]-[d], respectively, and is invalid for the same reasons as claims 2 and 10. §§VII.A.2, 7; EX[1005], ¶260.

9. Claim 12

Claim 12[a]-[c] corresponds to claim 3[a]-[c], respectively, and is invalid for the same reasons as claims 3 and 10. §§VII.A.3, 7; EX[1005], ¶261.

10. Claim 13

Claim 13[a]-[b] corresponds to claim 4[a]-[b], respectively, and is invalid for the same reasons as claims 4 and 10. §§VII.A.4, 7 EX[1005], ¶262.

11. Claim 15

Claim 15[a]-[b] corresponds to method claim 6[a]-[b], respectively, and is invalid for the same reasons as claims 6 and 10. §§VII.A.5, 7; EX[1005], ¶263.

12. Claim 17

Claim 17[a]-[c] corresponds to claim 8[a]-[c], respectively, and is invalid for the same reasons as claims 8 and 10. §§VII.A.6, 7; EX[1005], ¶264.

B. Ground 2: Obviousness of Claims 5, 7, 9, 14, 16, and 18 in view of Staton (EX[1007]) + Noland (EX[1008]) + Knowledge of a POSITA

Claims 5, 7, and 9 depend from claim 1, and claims 14, 16, and 18 depend from claim 10. Claims 1 and 10 are disclosed by Staton, §§VII.A.1, 7; the dependent claims in Ground 2 are rendered obvious by the combination of Staton with Noland.

1. A POSITA Would Have Combined Staton with Noland

A POSITA would have been motivated to combine Staton with Noland, with a reasonable expectation of success. First, both references are directed to the same field of endeavor as the '757 Patent: facilitating supervision of individuals based on geofencing. EX[1001], 1:7-10; EX[1005], ¶¶265-270. Staton discloses a geofencing-based supervision system that monitors persons in configurable zones and generates event notifications when boundaries or rules are violated. EX[1007], 13:65–14:19. Noland likewise monitors geographically defined areas, including school or building boundaries. EX[1008], ¶[0148]; EX[1005], ¶268.

Second, a POSITA would have incorporated Noland's weapon detection, facility blueprints, and NFC identification into Staton to improve the quality and urgency of supervision notifications. EX[1005], ¶271. Weapon type and lethality would inform responses to threats; blueprints would pinpoint their locations; and NFC would identify the relevant person or device. EX[1008], ¶¶[0034], [0074], [0148]; EX[1005], ¶272-275.

Third, the combination would have yielded predictable results, and a POSITA would have had a reasonable expectation of success in making it. EX[1005], ¶276. Staton's architecture accepts external sensors and devices through its backend control system. EX[1007], 6:34–8:8. A POSITA would have recognized that Noland's threat sensing devices, capability of locating threats on a blueprint/floorplan, and system gateway for processing represent precisely the type of expandable sensor integration that Staton's architecture was designed to accommodate, and it was within the level of skill of a POSITA to integrate Noland's devices/gateway into Staton's system. EX[1005], ¶276-278. In particular, a POSITA would have integrated Noland's threat sensing devices as instruments of Staton's zone-specific instrument module 195, which interacts with the supervisee's PDA 105 in that zone and "can be in the same housing" as the PDA. EX[1007], 10:33-35, 14:4-11; EX[1008], ¶¶[0016], [0091]; EX[1005], ¶276. It would also have been a straightforward modification to integrate this functionality in Staton's processing, communication, and storage devices. *E.g.*, §§VII.A.1.b, d, j; EX[1005], ¶278. Both Staton's backend control system 150 and Noland's system gateway receives, analyzes, and acts on incoming data; integrating Noland's functions would therefore require only routine software changes. EX[1007], 6:34-8:8; EX[1005], ¶278.

Moreover, NFC was a known short-range alternative. EX[1005], ¶¶275, 305-307. Noland teaches identifying persons through NFC/RFID identifiers linked to

employee and student IDs. EX[1008], ¶¶[0034], [0074], [0148]. Staton’s zone-specific instrument module 195 already links to PDA 105 over “WiFi, Bluetooth, wireless USB,” and reports “through the internet 160 to the backend control system 150.” EX[1007], 7:60-8:8, 10:38-42. A POSITA would have added an NFC reader to instrument module 195 to confirm who is present in a zone, a routine addition to an existing short-range hub with a reasonable expectation of success. EX[1005], ¶¶279, 307.

2. Claim 5

Staton and Noland render claim 5 obvious. EX[1005], ¶¶280-284.

- a. 5[a] *“identifying, using the processing device, at least one object associated with the supervisee based on the analyzing of the at least one supervisee data; and”*

Noland discloses “**identifying...at least one object associated with the supervisee**”—an identified weapon in the supervisee’s geofenced zone. *Id.* Specifically, in the combined system, Noland’s system gateway 110 analyzes sound data from the threat sensing devices integrated with the supervisee device (**based on analyzing supervisee data**) to “determine whether the sound waveform indicates a valid gunshot or gunshots and, if so, to further determine the general type of weapon...and establish the location or room number of the shooter(s).” EX[1008], ¶¶[0107]-[0108]; §VII.B.1.

- b. 5[b] *“determining, using the processing device, a lethality of the at least one object based on the identifying, wherein the*

generating of the supervision notification is based on the determining.”

Noland discloses “**determining...a lethality**” of the object “**based on the identifying.**” EX[1005], ¶¶285-288. In the combined system, Noland’s system gateway 110 (integrated into Staton’s processing device) “utiliz[es] lookup tables of waveforms of gunshots of numerous firearms firing numerous different bullets ...,” EX[1008], ¶[0111], classifies the weapon, *id.* ¶[0127], and ties the kind of weapon being fired to “the level of the threat” posed to human life. *Id.* ¶[0156]. For example, the system “advise[s] the first responders as to the kind(s) of weapon is being fired to enable the first responders to know the level of the threat...and necessary tactics.” *Id.*; EX[1005], ¶285.

The combined system then “**generat[es] the supervision notification...based on the determining.**” EX[1005], ¶287. The determined weapon type/caliber are included in alert messages and “sent via the Internet 120 to designated mobile devices 130 and local authorities 132.” EX[1008], ¶[0096]. In the combined system, this lethality information is incorporated into the supervision notification transmitted to the supervisor device, as described for claim 1. §§VII.A.1.h-i, VII.B.1; EX[1005], ¶288.

3. Claim 7

Staton and Noland render claim 7 obvious. EX[1005], ¶¶289-300.

- a. 7[a] “retrieving, using the storage device, a blueprint associated with the geographical area corresponding to the geofence;”

Noland discloses that **blueprints** associated with the geofence where the threat sensing device is installed, including “proximity information of floor plans” and “building layouts,” are pre-loaded into the system’s storage. EX[1008], ¶[0034]; *id.* ¶[0113] (geometry and location of each room “integrated into the schematics of the facility for dissemination to first responders”); EX[1005], ¶¶290-292. In the combined system, these facility schematics would have been stored in and **retrieved** using part of **the storage device** (resources database 670/history database 642) to “create and format the alert message content,” which includes a schematic overlay. EX[1008], ¶[0179]; EX[1005], ¶¶289-294; §VII.B.1.

- b. 7[b] “analyzing, using the processing device, the blueprint and the at least one supervisee data; and”

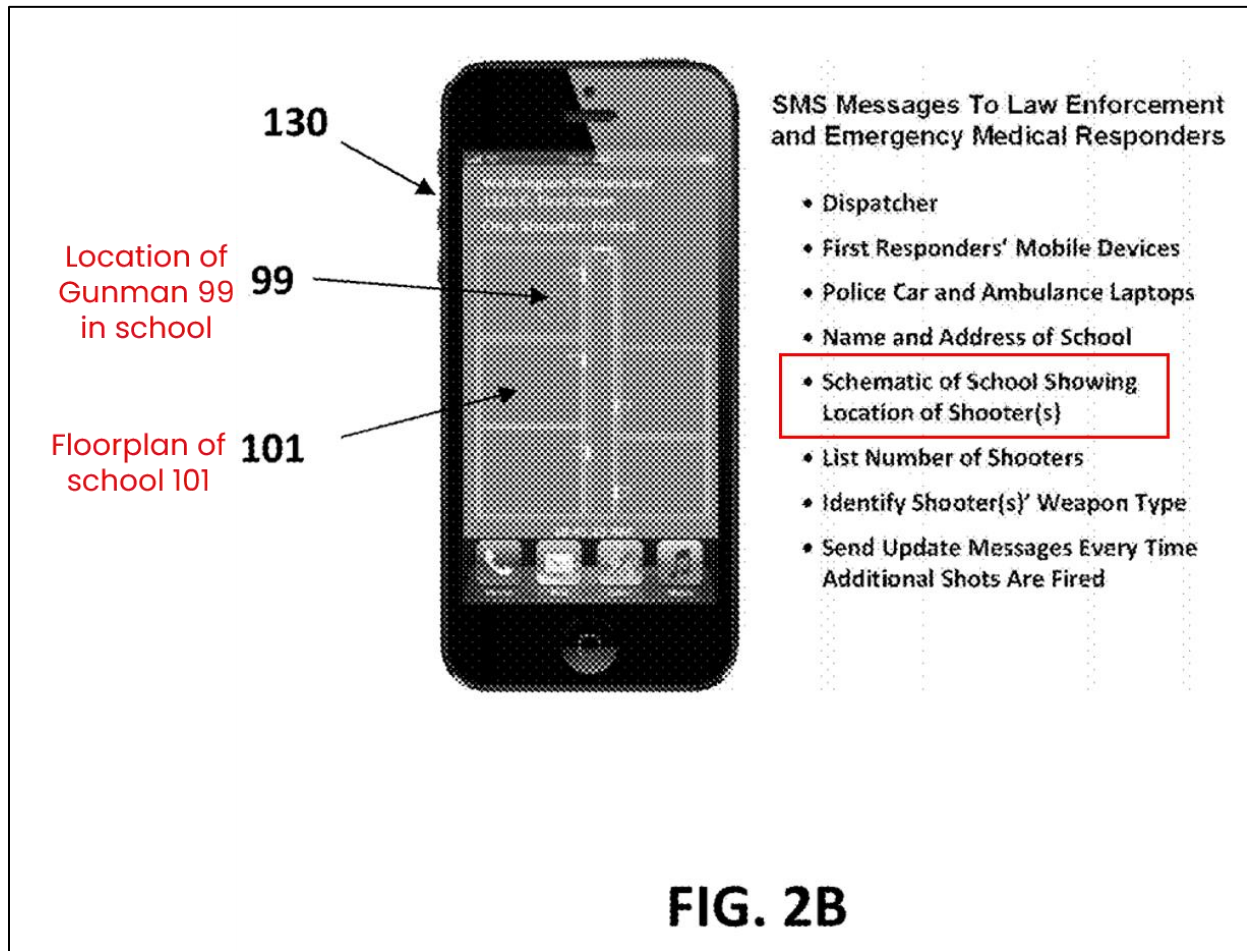
In the combined system, Noland’s system gateway 110 integrated with Staton’s processing device **analyzes the blueprint** and threat data (**supervisee data**) to determine “the general type of weapon...and establish[es] the location or room number of the shooter(s)” and correlates the “known location of the threat sensing device” with the stored room geometry and facility schematics. EX[1008], ¶¶[0107], [0111], [0113]; EX[1005], ¶¶295-297; §VII.B.1.

- c. 7[c] “determining, using the processing device, a location of the supervisee on the blueprint based on the analyzing of the blueprint and the at least one supervisee data, wherein the

generating of the supervision data is based on the determining.”

The combined system **determines**, using the system gateway 110 integrated with Staton’s **processing device, location of the supervisee on the blueprint** based on the analysis described in 7[b] and **generates** and sends a **supervision data based on the determining**. EX[1005], ¶¶298-300; §VII.B.1. The notification content comprises and is based on “a schematic of the school overlaid by icons showing shooter location” and the supervisee data that triggered the threat assessment. EX[1008], ¶¶[0179], [0097], Fig. 2B; EX[1005], ¶¶298-300. Although not depicted in the annotated figure below, Noland also tracks “where injured persons are located inside the school” and otherwise “track[s] a location of, or presence of” persons at the facility. EX[1008], ¶¶[0148], [0155]. In the combined system, it would have been obvious to plot other supervisees’ Staton-reported GPS location, EX[1007], 16:18-23, on Noland’s facility schematic using the same overlay technique so that supervisors and responders can locate supervisees relative to the threat. EX[1005],

¶¶298-300.



4. Claim 9

Staton and Noland render Claim 9 obvious. EX[1005], ¶¶301-310.

a. 9[a] “the supervisee is associated with at least one identification, wherein the method comprises:”

In the combined system, the **supervisee is associated with an NFC identification:**

Noland’s RFID “ID badge[s]” and “mobile devices” carry identifiers read by NFC devices, and stored information is linked to “employee IDs, student IDs, RFIDs.”

EX[1008], ¶¶[0034], [0074]; EX[1005], ¶¶301-303. Staton’s resource database 670

“keeps records of all the instrument modules and PDAs” and relates each PDA to its member; in the combined system, the NFC identification would have been stored there. EX[1007], 19:59-61, 24:58-64; EX[1005], ¶¶301-303; §VII.B.1.

- b. 9[b] “receiving, using the communication device, at least one NFC indication corresponding to the at least one supervisee device; wherein the receiving is performed over short range wireless communication comprising at least one of Bluetooth, Zigbee, Ultra-wideband, Wi-Fi and NFC, and”*

In the combined system, the NFC reader added to instrument module 195 **receives the NFC indication from the supervisee device** over NFC (**short range wireless communication comprising NFC**), EX[1008], ¶¶[0074], [0148], and module 195 reports it “through the internet 160 to the backend control system 150,” whose gateways (of **communication device**) **receive** it. EX[1007], 7:62-8:10, 19:60-20:6; EX[1005], ¶¶304-306; §§VII.A.1.b, VII.B.1. Staton’s module and PDA also communicate via “WiFi, Bluetooth.” EX[1007], 10:38-42, 9:1-3, 9:10-12.

- c. 9[c] “identifying, using the processing device, the supervisee based on the at least one NFC indication, wherein the generating of the supervision notification is based on the identifying.”*

Staton’s processing device **identifies the supervisee** by looking up the NFC identifier in resources database 670, as Noland identifies “the owners of those phones” (**supervisees**) from near-field sensor reads, and generates a supervision

notification based on the identifying, as described for claim 4. EX[1008], ¶[0148]; EX[1007], 24:58-64; EX[1005], ¶¶307-310; §§VII.A.4.a-b.

5. Claim 14

Claim 14[a]-[b] recites the “processing device” of claim 10 (Ground 1) performing the functions of limitations 5[a]-[b], and is invalid for the same reasons as claim 5 and 10 (Ground 1). §§VII.B.2, VII.A.7; EX[1005], ¶311.

6. Claim 16

Claim 16[a]-[c] recites the “processing device” and “storage device” of claim 10 (Ground 1) performing the functions of limitations 7[a]-[c], and is invalid for the same reasons as claim 7 and 10 (Ground 1). §§VII.B.3, VII.A.7; EX[1005], ¶312.

7. Claim 18

Claim 18 is a system claim reciting the “processing device” of claim 10 performing substantially the same (or broader) functions as claim 9, and are invalid for the same reasons as claims 9 and 10 (Ground 1). §§VII.B.4, VII.A.7. Claim 18 also specifies NFC identification in the preamble, but NFC identification is already covered in claim 9. EX[1005], ¶313.

C. Ground 3: Obviousness of Claims 1-4, 6-8, 10-13, and 15-17 in view of Rauner (EX[1009]) + Azmoodeh (EX[1010]) + Knowledge of a POSITA

1. A POSITA Would Have Combined Rauner With Azmoodeh

First, both references are in the same field of endeavor as the '757 Patent, facilitating supervision of individuals based on geofencing. EX[1001], 1:7-10; EX[1005], ¶¶322-325. Rauner uses geofences to monitor and coordinate emergency response across campuses, buildings, and municipalities. EX[1009], ¶¶[0048], [0239]. Azmoodeh uses geofences to monitor the distribution and activity of devices within a geographic region. EX[1010], ¶[0015]. Although Azmoodeh's primary application is content delivery, its grid-cell technique is domain-independent and addresses the same problem of subdividing and monitoring a geofenced area using location data. EX[1009], ¶¶[0048], [0239]; EX[1010], ¶[0015]; EX[1005], ¶¶64, 135.

Second, Rauner already discloses a GPS-integrated "alphanumeric grid" overlaying its geofences, EX[1009], ¶[0094], associating building schematics with geofences, *id.* ¶[0215], and plotting device locations into those schematics using X-Y-Z axis coordinates, *id.* ¶[0198]. However, Rauner's grid and schematics function as coordinate overlays for display and location-correlation purposes and do not expressly subdivide the geofenced area into defined portions or make the number of such cells user-configurable. EX[1005], ¶¶83, 326, 375-376. Azmoodeh fills that

gap by dividing the geofenced area “into a grid that comprises a set of cells, where each cell represents portions...of the physical location within the geo-fenced area....” EX[1010], ¶[0022]. The “number of cells within the region may be defined based on a size of the geo-fence, or based on user input.” *Id.* ¶[0046]; EX[1005], ¶¶326-332.

Third, a POSITA would have added Azmoodeh’s cell subdivision to improve Rauner’s granularity and flexibility, consistent with Azmoodeh’s stated benefit of allowing the geofence to “more accurately encompass the location of interest.” EX[1010], ¶[0023]. Rauner’s system already localizes individuals within geofences by “cross referencing the area indicated by the geofence and the locations associated with the individuals” (EX[1009], ¶[0244]) and determines whether devices are within particular structures (*id.* ¶[0198]). Adding Azmoodeh’s cell subdivision would give the system a framework for determining not just that a device is within the geofence, but a more granular position within it. EX[1010], ¶[0047] (usage data “indicat[es] a location of a device within the geo-fenced area”). Moreover, because Rauner serves environments ranging from single buildings to metropolitan areas (EX[1009], ¶[0048]), a POSITA would have recognized that making the grid resolution user-configurable, as Azmoodeh teaches, would allow administrators to tailor granularity to each deployment context, making the system more flexible and expanding marketing opportunities to users with diverse geolocating needs.

EX[1005], ¶¶325-332. This is a natural extension of Rauner's existing administrative interface, through which the administrator already configures trigger words, thresholds, maps, and geographic areas. EX[1009], ¶¶[0089]–[0094]; EX[1005], ¶328.

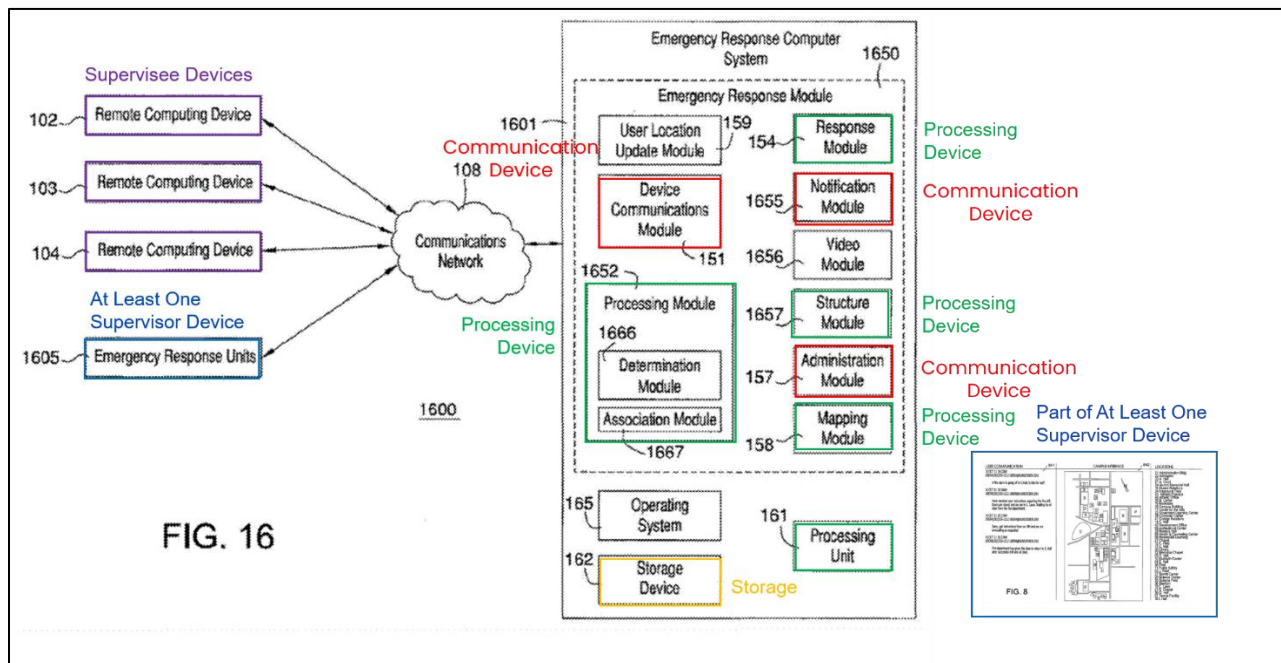
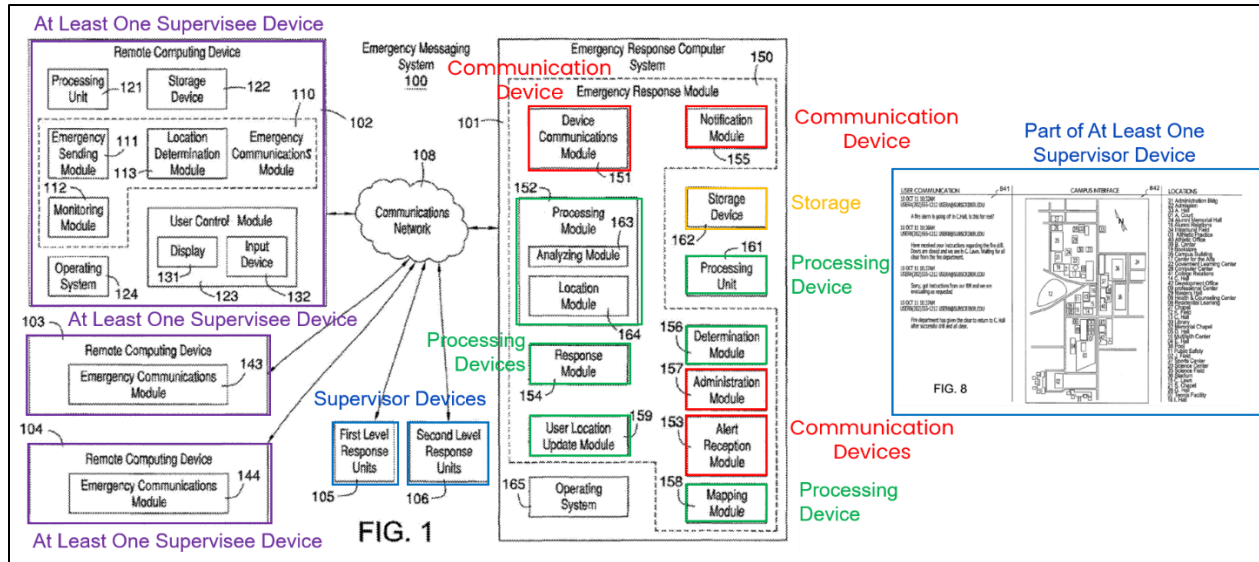
Fourth, a POSITA would have expected success because the combination requires only adding Azmoodeh's cell-subdivision routine, under which the number of cells is "defined based on a size of the geo-fence, or based on user input" (EX[1010], ¶[0046]), to Rauner's mapping module 158, which already creates a GPS-integrated "alphanumeric grid" and calculates coordinate ranges for each grid box (EX[1009], ¶¶[0093]–[0094]). Both references implement geofencing as processor-executed software (*id.* ¶[0097]; EX[1010], ¶[0033]). Dividing a known geofence area by a user-specified cell count or size is basic arithmetic on coordinates Rauner already computes, and Rauner's administrator already enters configuration values through administration module 157 (EX[1009], ¶[0092]). This is a known technique applied to a known system with predictable results. EX[1005], ¶¶330-332.

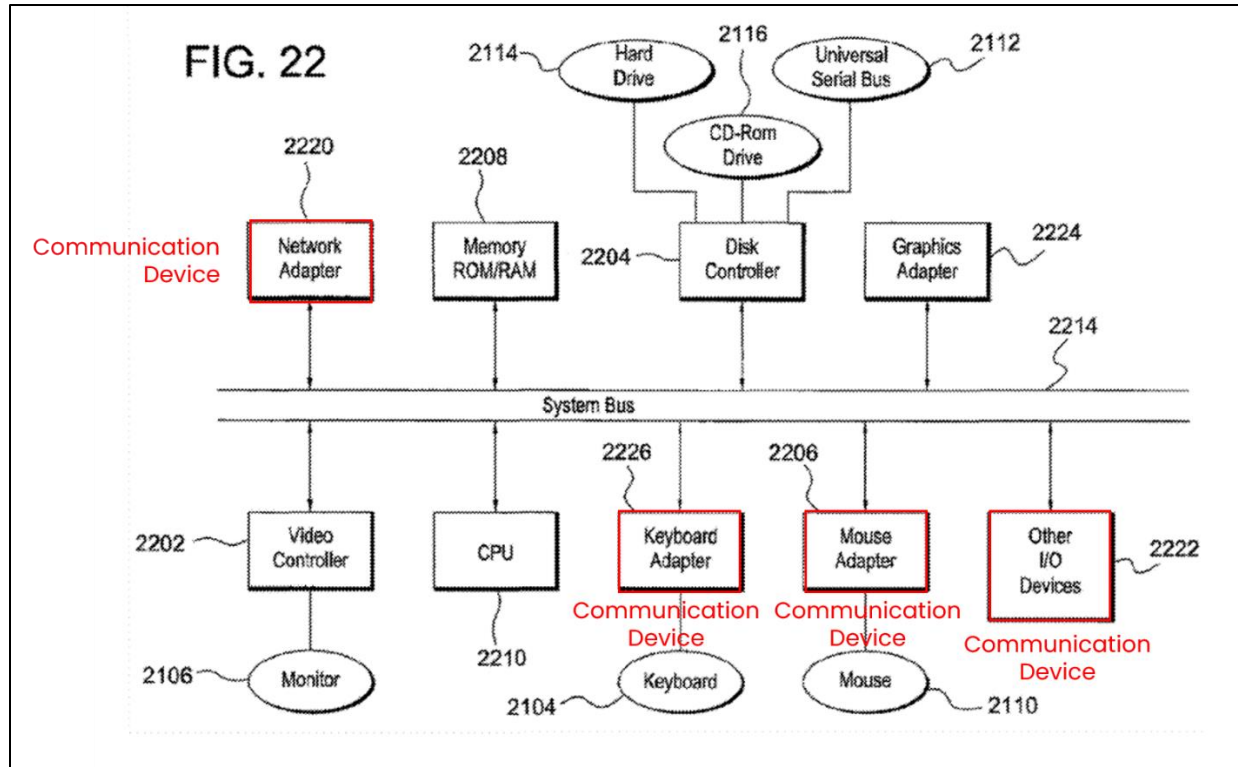
2. Claim 1

a. 1[pre] “A method for facilitating supervision of individuals based on geofencing, the method comprising:”

To the extent the preamble is limiting, Rauner¹ discloses it. EX[1005], ¶¶333-334. Rauner discloses **supervising individuals** (students, faculty, staff, workers) **based on geofences** to monitor locations and coordinate emergency response. *Id.*; EX[1009], ¶¶[0048], [0239]. The system is annotated below to show the communication device (red), supervisor device (blue), processing device (green), storage device (orange), and supervisee device (purple), all of which are described further herein. EX[1005], ¶¶314-321. The system uses geofences to filter events, target communications, generate census reports, and coordinate emergency response. EX[1009], ¶¶[0037], [0176], [0244].

¹ Rauner describes two related embodiments: (1) the core architecture (system 100, ¶¶[0047]–[0095]); and (2) an extension with additional modules (system 1600, ¶¶[0157]–[0200]), including structure module 1657, running on the same processing unit 161 and accessing the same storage device 162. EX[1005], ¶129, 318. Grounds 3-4 rely on the second embodiment, which also includes the components of embodiment 1. EX[1009], ¶¶[0162]–[0166]; EX[1005], ¶130, 319-320.





b. 1[a] “receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor;”

Rauner discloses this limitation. EX[1005], ¶¶335-345.

Applicant’s §112(f) “**communication device**”² (red above) is the communications function (including programs, middleware, and software) of emergency response computer system 101, including device communications module 151 (DCM), which communicates with remote computing devices over

² Rauner expressly discloses that the communication device is implemented on the same server as the processing device and storage device. EX[1009], ¶¶[0054], [0097] (computer system 101 includes processing unit, device communications module, and storage device, and constituent modules); EX[1005], ¶¶316-317, 321.

communications network 108, notification module 155/1655, which works through DCM to transmit notifications, administration module 157, which communicates with system administrators, alert reception module 153, which receives event or alert notifications from third-party sources, and the communications modules shown in Fig. 22, including network adapter 2220, keyboard adapter 2226, mouse adapter 2206, and other input/output devices 2222 coupled to system bus 2214. EX[1009], ¶¶[0067], [0069], [0081], [0085], [0203]-[0204]; EX[1005], ¶¶315, 335.

The “**at least one supervisor device**” is the set of devices used by supervisory personnel to configure, monitor, and receive outputs from the system, including: the system administrator’s terminal interface (*e.g.*, EX[1009], Figs. 8-14, *see* insert of Fig. 8, blue above), which provides inputs to and receives outputs from the backend server’s administration module 157 (EX[1009], ¶¶[0085], [0089]; EX[1005], ¶336); the PSAP computers (not shown above), which access the cloud hosted emergency response system through a browser interface (EX[1009], ¶[0031]); and the first and second level response unit devices (blue above), which receive notifications and reports from the system (*id.* ¶¶[0057]–[0058], [0137]).

The **security parameters** include mass-event and Clery trigger words (*e.g.*, “homicide” and “murder”), distance thresholds, mass event trigger limits, and escalation rules designated and **associated** with the administrator (**supervisor**). *Id.* ¶¶[0076], [0089]-[0090], [0092]; EX[1005], ¶337-340. The administration module

(part of **communication device**) receives these **security parameters** from the administrator's terminal (part of **supervisor device**) when the administrator "logs into administration module 157 and enters [the] configuration page" to designate trigger words and configure thresholds (*id.* ¶[0089]). EX[1009], ¶¶[0031], [0085], [0089]; EX[1005], ¶¶341-345.

c. 1[b] "receiving, using the communication device, a geographical location from the at least one supervisor device;"

Rauner discloses this limitation. EX[1005], ¶¶346-347. The "**geographical location**" is the map and geospatial data uploaded by the administrator through the administrator terminal interface (part of **supervisor device**) and **received by** the administration module (part of **communication device**), as with limitation 1[a]. EX[1009], ¶¶[0094]-[0095]; §VII.C.2.b. The administrator defines geographic areas by "clicking," "draw[ing]," "drag[ging]," "select[ing]," or using a "pin drop" to define the area. EX[1009], ¶¶[0094]-[0095].

d. 1[c] "analyzing, using a processing device, the geographical location based on the at least one security parameter;"

Rauner discloses this limitation. EX[1005], ¶¶348-354. Applicant's §112(f) "**processing device**" is processing unit 161 including its processing module 152/1652, analyzing module 163, response module 154, determination module 156/1666, and mapping module 158. *Id.*

The administrator inputs **security parameters** (trigger words, Clery event terms, distance thresholds, escalation rules (EX[1009], ¶¶[0076], [0089]–[0090], [0092]–[0094])), which inform the areas the system monitors. EX[1005], ¶¶339, 349–350; EX[1001], 11:38–43 (broadly disclosing any type of parameters for security-monitoring purposes). The mapping module of the **processing device analyzes the supervisor’s geographical location input based on those parameters** because they determine which areas warrant monitoring. EX[1009], ¶¶[0076], [0089]–[0094]; EX[1005], ¶350.

Other disclosures further show analysis of geographic location using security parameters. EX[1005], ¶¶351–354. For example, Rauner also “compares the geographic area” identified in third-party warnings “with all stakeholder defined areas” and “compares the content” of the warnings “to select appropriate emergency plans(s).” EX[1009], ¶[0218]. Rauner’s response module also jointly analyzes trigger-word content, message frequency, and location to determine response levels, assigning a second-level response when a predetermined number of trigger messages are “sent from locations within a predetermined distance of each other.” *Id.* ¶¶[0079], [0121], [0123]–[0124], Claim 8.

- e. 1[d] “generating, using the processing device, a geofence corresponding to a geographical area based on the analyzing;”*

Rauner discloses this limitation. EX[1005], ¶¶355-356; §V. Mapping module 158 of the **processing device generates** the **geofences**—graphic boundaries or representations of defined geographic areas with associated settings to trigger an alert—**based on the inputs and analysis** described in limitations 1[b]-1[c]. EX[1009], ¶¶[0093], [0239], [0215], [0244]; §§VII.C.2.c-d. The administrator uploads a map, selects features, and configures security parameters, and the mapping module processes these inputs to produce the geofence. *Id.* ¶¶[0089]–[0094]; EX[1005], ¶356.

- f. 1[e] “receiving, using the communication device, at least one supervisee data associated with a supervisee from at least one supervisee device;”*

Rauner discloses this limitation. EX[1005], ¶¶357-358. Rauner’s remote computing devices 102–104 (**supervisee devices**) are carried by monitored users (supervisees). They transmit emergency trigger messages and location information regarding the supervisee (**supervisee data**) that are **received** by device communications module 151 (of **communication device**). EX[1009], ¶¶[0105], [0111]; EX[1005], ¶¶357-358. The devices also periodically report their locations, as often as every ten seconds. EX[1009], ¶¶[0072], [0182].

g. 1[f] “analyzing, using the processing device, the at least one supervisee data based on the geofence;”

Rauner discloses this limitation. EX[1005], ¶¶359-363. Processing unit 161’s processing, analyzing, determination, and structure modules (**processing device**) **analyze supervisee data based on the geofence** in several ways. They identify affected devices within a geofenced area, cross-reference geofences with individual locations for census reports, determine whether devices are in a geofenced building, and use overlapping geofences to route events based on device location. EX[1009], ¶¶[0037], [0176], [0195], [0198], [0244]; EX[1005], ¶360-363.

h. 1[g] “generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data;”

Rauner discloses this limitation. EX[1005], ¶¶364-367. Analyzing, response, and determination modules on processing unit 161 (of **processing device**) **generate supervision notifications based on the geofence analysis of the supervisee data**. EX[1009], ¶¶[0076], [0078]–[0082]. Examples include 911 notices (*id.* ¶[0050]), mass-event warnings (*id.* ¶[0082]), and geofence-based census reports produced by cross-referencing the geofence with individual locations (*id.* ¶[0244]). *See also id.* ¶¶[0050], Claims 1, 6; EX[1005], ¶365-367.

- i. *1[h] “transmitting, using the communication device, the supervision notification to the at least one supervisor device; and”*

Rauner discloses this limitation. EX[1005], ¶¶368-371. Device communications module 151 and notification module 155 (parts of **communication device**) **transmit supervision notifications** of 1[g] **to supervisor devices**. EX[1009] ¶[0067]; §§VII.C.2.h. Rauner identifies response units, administrators, subscribers, and selected system administrators as recipients of emergency notices, emails, alerts, and reports. *Id.* ¶¶[0050], [0067], [0083], [0137], [0168], [0119], Claim 1; EX[1005], ¶¶368-371.

- j. *1[i] “storing, using a storage device, the at least one supervisee data and the supervision notification, wherein:”*

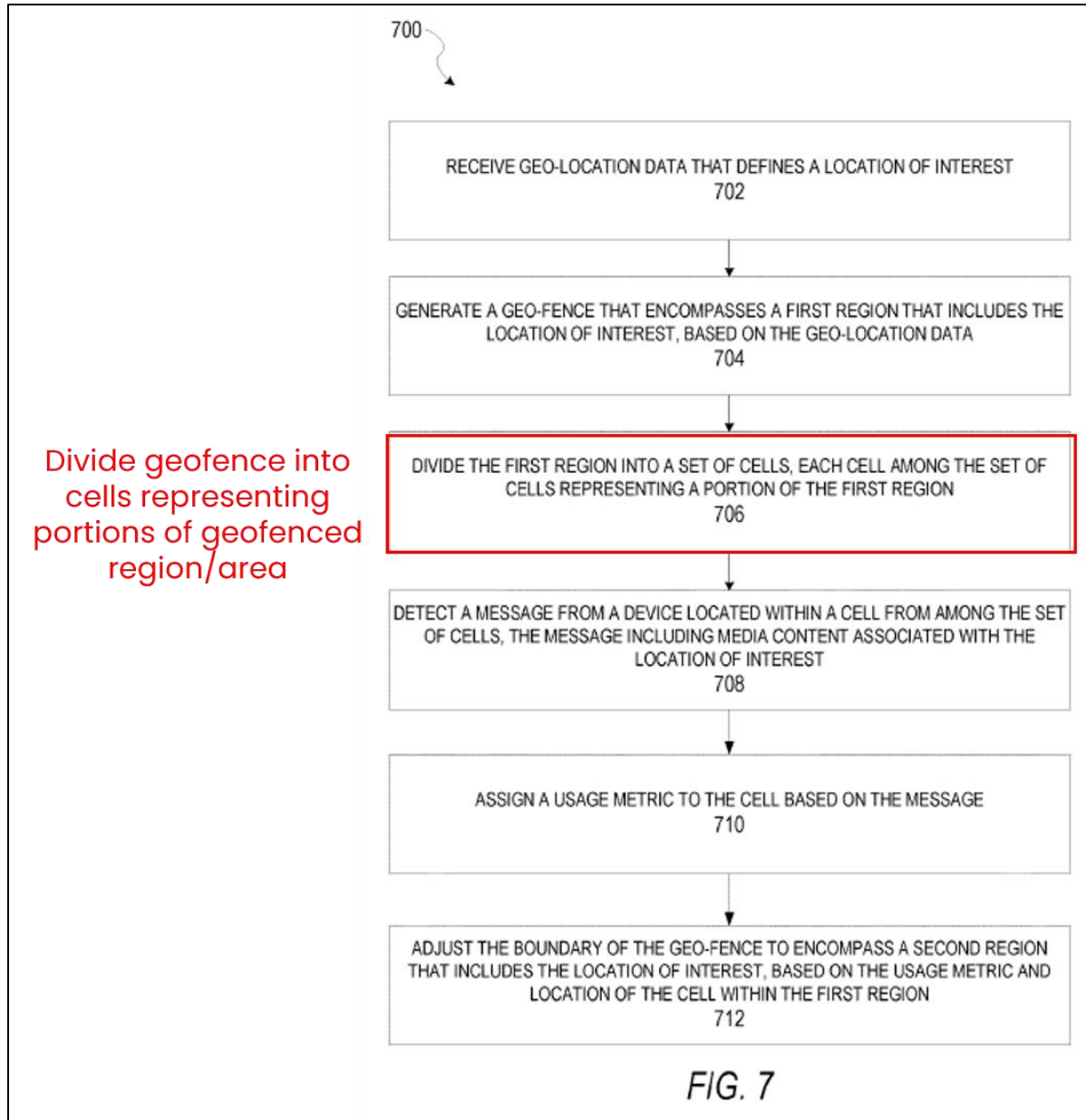
Rauner discloses this limitation. EX[1005], ¶¶372-374. Applicant’s §112(f) “**storage device**” is storage device 162, which **stores both supervisee data** (locations of supervisees) **and supervision notifications** (911 notice and mass event warning messages). EX[1009], ¶¶[0075], [0072] (supervisee data); *id.* ¶¶[0050], [0083] (notifications).

- k. *1[j] “the geofence is characterized by a geofence area corresponding to the geographical area, wherein the geofence comprises a plurality of geofence grid boxes associated with the geofence area, wherein each geofence grid box is characterized by a grid box geofence area of the geofence area, wherein the method comprises:”*

The combination of Rauner and Azmoodeh renders this limitation obvious. EX[1005], ¶¶375-377. As described in §VII.C.1, when combined, Rauner’s

geofence characterized by a geofence area corresponding to the geographical area and associated grid overlay are supplemented by Azmoodeh's teaching that grid cells structurally subdivide the geofence (**geofence area corresponding to the geographical area**), with each cell (each of the **plurality of geofence grid boxes associated with the geofence area**) representing a defined portion (**grid box geofence area of the geofence area**) and the cells together covering the whole.

§VII.C.1; EX[1005], ¶¶375-377.



EX[1010], Fig. 7 (annotated).

- l. 1[j][1] “receiving, using the communication device, at least one grid parameter from the at least one supervisor device, wherein the processing device is further configured for:”

The combination of Rauner and Azmoodeh renders this limitation obvious.

EX[1005], ¶¶378-379; §VII.C.1. The **grid parameter** is user input defining the

number of cells. EX[1010], ¶[0046]; EX[1009], ¶¶[0089]–[0094]. The administration module (part of **communication device**) receives the **grid parameter** from the administrator terminal (part of **supervisor device**), allowing the administrator to configure the grid. §VII.C.1; EX[1010], ¶[0046]; EX[1009], ¶¶[0089]–[0094]; EX[1005], ¶379.

m. 1[j][2] “analyzing, using the processing device, the at least one grid parameter;”

The combination of Rauner and Azmoodeh renders this limitation obvious. EX[1005], ¶¶380-381. In the combined system, the **grid parameter** (user input defining number of grid cells) is **analyzed** by the mapping module (portion of **processing device**), which analyzes the user-supplied cell count to set the number of cells in the region. §VII.C.1; EX[1009], ¶¶[0093]–[0094]; EX[1010], ¶[0046]; EX[1005], ¶381.

n. 1[j][3] “determining, using the processing device, the grid box geofence area based on the analyzing of the at least one grid parameter; and”

The combination of Rauner and Azmoodeh renders this limitation obvious. EX[1005], ¶¶382-384. In the combined system, mapping module on processing unit 161 (part of **processing device**) **determines the grid box geofence area** by calculating coordinate ranges and associating coordinates with each grid box. §VII.C.1; EX[1009], ¶[0094]. Because Azmoodeh’s cells represent portions of the geofenced area, **the area of each cell is determined** depending on the total geofence

area and user-supplied cell count (is **based on the analyzing of the at least one grid parameter**). EX[1009], ¶¶[0093]-[0094]; EX[1010] ¶¶[0022], [0046]; EX[1005], ¶¶383-384.

- o. 1[j][4] “generating, using the processing device, a number of geofence grid boxes based on the determining.”*

The combination of Rauner and Azmoodeh renders this limitation obvious. EX[1005], ¶¶385-388. In the combined system, a **number of geofence grid boxes** is **generated using** the mapping module 158 (portion of **processing device**) (EX[1009], ¶[0093]), which creates “an alphanumeric grid over the graphical representation.” *Id.* ¶[0094]. §VII.C.1. The geofence is divided “into a set of cells, each cell among the set of cells representing a portion of the first region,” with the number determined by user input (**based on the area determination**). §VII.C.1; EX[1010], Claim 1, ¶[0046]; EX[1005], ¶¶385-387.

3. Claim 2

- a. 2[a] “receiving, using the communication device, at least one location indication associated with the geographical area from the at least one supervisor device;”*

Rauner discloses this limitation. EX[1005], ¶¶389-393. The “**location indication**” is (1) a name of a geofenced structure or feature (**associated with the geographical area**) supplied by the administrator through the terminal interface (part of **supervisor device**), EX[1009], ¶[0094]; and/or (2) building schematics **associated** with a geofenced building (**geographical area**) (*id.* ¶[0215]). *Id.* Claim

2. In either case, the indication is **received** through administration module 157 (part of **communication device**), as with limitation 1[a]. *Id.* ¶¶[0094], [0215], Claim 2, [0031]; EX[1005], ¶¶390-393.

b. 2[b] “identifying, using the processing device, at least one location corresponding to the at least one location indication;”

Rauner discloses this limitation. EX[1005], ¶¶394-395. The mapping module (of **processing device**) **identifies the location corresponding to the location indication** by translating the named feature or building schematic into geospatial coordinates. EX[1009], ¶[0094] (calculating a coordinate range and associating it with the feature); EX[1005], ¶¶394-395.

c. 2[c] “analyzing, using the processing device, the at least one supervisee data based on the at least one location; and”

Rauner discloses this limitation. EX[1005], ¶¶396-398. The structure module 1657 and/or determination module 156/1666 (part of **processing device**) **analyze** by cross-referencing supervisee-device locations (**supervisee data**) with administrator-designated structures and locations within the geographic area (**the location**). EX[1009], ¶¶[0198], [0139], [0189]; EX[1005], ¶¶396-398.

d. 2[d] “determining, using the processing device, a location anomaly based on the analyzing of the at least one supervisee data based on the at least one location, wherein the generating of the supervision notification is based on the determining.”

Rauner discloses this limitation. EX[1005], ¶¶399-403. Rauner discloses at least two **location anomalies** and associated notifications **determined** by the

processing device. EX[1009], Claim 8, ¶¶[0078], [0082], [0123]; EX[1005], ¶¶399-403:

(1) Threat escalation event **notifications based on determining location anomalies**, which in turn are based on **analyzing supervisee data at the location**, EX[1009], ¶[0208] (“creating a Threat Escalation Event when the frequency of call/text events exceeds a defined threshold” for a defined location), *id.* (same when “the content of call/text events meets defined criteria” for a defined location), ¶[0209] (Threat Escalation Event distributed by “cross referencing the stakeholder location with the location(s) of the underlying events”).

(2) Spatial clustering escalation **notifications based on determining location anomalies**, which in turn are **based on analyzing** if trigger messages from supervisee devices (**supervisee data**) “were sent from **locations** within a predetermined distance of each other,” *id.* ¶¶[0121], [0124] (ten messages with trigger word “gun” sent within 500 meters triggers second-level response), Claim 8.

4. Claim 3

a. 3[a] “the supervision notification comprises at least one supervisee event, wherein the at least one supervisee event is

associated with at least one action, wherein the method comprises:”

Rauner discloses this limitation. EX[1005], ¶¶404-405. The “**supervisee event**” is Rauner’s Emergency Event—an emergency call or text that takes the device location and pairs it with the user and provides a **supervision notification**, as described in 1[g]. EX[1009], ¶¶[0208], [0050]); §VII.C.2.h. The supervisee event is **associated with an action**—distributing that location and profile through an emergency-response workflow to recipients selected based on location, proximity, status, hierarchy, or event type. EX[1009], ¶¶[0050], [0110], [0208]; §VII.C.2.h; EX[1005], ¶405.

b. 3[b] “determining, using the processing device, the at least one action based on the supervision notification; and”

Rauner discloses this limitation in two ways. EX[1005], ¶¶406-407.

(1) Response module 154 and determination module 156 on processing unit 161 (portion of **processing device**) **determine** the emergency-response workflow for acting on the Emergency Event (an **action**) **based on the supervision notification**. EX[1009], ¶¶[0078]-[0081], [0110], [0167], [0169]; EX[1005], ¶¶406-407.

(2) The same modules **determine** response level and which first- or second-level units to notify (**an action**) based on message frequency, content, and

location derived from **(based on) the supervision notification**. EX[1009], ¶¶[0079]-[0080], [0252]; EX[1005], ¶406.

- c. 3[c] “performing, using the processing device, the at least one action based on the determining, wherein the at least one action comprises an establishment of a communication session between the at least one supervisor device and the at least one supervisee device.”*

Rauner discloses this limitation. EX[1005], ¶¶408-410. Processing unit 161 **(processing device) performs the action based on the determining**, where the **action establishes** group messaging **(communication session)** between emergency-response **(supervisor)** and caller **(supervisee)** devices. EX[1009], ¶[0110]; *see also id.* ¶¶[0169], [0049], [0038]; EX[1005], ¶408-410.

5. Claim 4

- a. 4[a] “identifying, using the processing device, the supervisee based on the analyzing of the at least one supervisee data; and”*

Rauner discloses this limitation. EX[1005], ¶411-413. **Based on analyzing** the emergency event received from the user **(supervisee data)**, processing unit 161 **(processing device) identifies** the caller’s supervisee profile **(the supervisee)** with the emergency communication event. EX[1009], ¶¶[0050], [0110], [0169]; §§VII.C.2.f-g; EX[1005], ¶412-413.

- b. 4[b] “retrieving, using the storage device, supervisee profile data associated with the supervisee based on the identifying,*

wherein the generating of the supervision notification is based on the retrieving.”

Rauner discloses this limitation. EX[1005], ¶¶414-416. Rauner stores user profile data (**supervisee profile data**) in **storage device** 162, including name, contact, emergency, and location information, **based on the identifying**. EX[1009], ¶[0099]. **Based on identifying the supervisee**, the system **retrieves the profile associated with the supervisee using the storage device** and pairs it with the event. EX[1009], ¶¶[0099], [0208]; EX[1005], ¶¶414-416.

The **supervision notification generation** is **based on the retrieving** because the notification incorporates the retrieved profile data: the 911 notice includes the user name, reports include name and phone number, and census reports include contact and location information. EX[1009], ¶[0050], Claim 6, ¶[0244]; EX[1005], ¶415.

6. Claim 6

- a. 6[a] *“receiving, using the communication device, at least one environment data associated the geographical area corresponding to the geofence;”*

Rauner discloses this limitation. EX[1005], ¶¶417-421. Rauner’s system **receives environment data associated with the geographical area corresponding to the geofence** in two ways:

- (1) The system receives georeferenced sensor feeds—traffic, motion, heat, air quality, water quality, radiation, or moisture (**environment data**)—from

external monitoring systems. EX[1009], ¶¶[0212]-[0213], Claim 14. A POSITA would have understood device communications module 151 or network adapter 2220, parts of the **communication device**, to receive them. EX[1005], ¶420.

(2) Alert reception module 153, part of the **communication device**, receives event or alert notifications from agencies such as FEMA, USGS, CDC, NOAA, and FDA. EX[1009] ¶[0069]. These include geographic parameters for tornado, radiation, and other threats (**environment data**); the system compares them with stakeholder-defined geofences to determine a response. *Id.* ¶¶[0069], [0214], [0218], [0242]-[0243]; EX[1005], ¶¶421, 424.

b. 6[b] “analyzing, using the processing device, the at least one environment data; and determining, using the processing device, at least one threat based on the analyzing of the at least one environment data, wherein the generating of the supervisor notification is based on the determining.”

Rauner discloses this limitation, for each type of environmental data described in 6[a]. EX[1009], ¶¶[0169], [0172], [0213]; EX[1005], ¶¶422-425.

(1) The **processing device analyzes** whether sensor data within the defined area (**environmental data**) meets the trigger requirements (**determines a threat**), and distributes the sensor data to mobile or web services “as an event” (**generates a supervision notification based on the determining**). EX[1009], ¶¶[0213], [0214], [0243]; *see also* §VII.C.2.h-i.

(2) The **processing device** compares (**analyzes**) georeferenced event locations with data from available sensor(s) (**environmental data**) to **determine a threat** and distributes an emergency warning with sensor output (**generates a supervision notification based on the determining**).
EX[1009], ¶[0214]; §§VII.C.2.h-i.

7. Claim 7

a. 7[a] “retrieving, using the storage device, a blueprint associated with the geographical area corresponding to the geofence;”

Rauner discloses this limitation. EX[1005], ¶¶426-428. Rauner’s structure module 1657 **retrieves** a schematic (a **blueprint**) for a geofenced structure (**associated with the geographical area corresponding to the geofence**) from storage device 162 (**storage device**). EX[1009], ¶[0174]. It cross-references the emergency location with geofenced building schematics and selects the appropriate building plan. EX[1009], ¶¶ [0195], [0215]; EX[1005], ¶428.

b. 7[b] “analyzing, using the processing device, the blueprint and the at least one supervisee data; and”

Rauner discloses this limitation. EX[1005], ¶429. Structure module 1657 (of **processing device**) **analyzes** the retrieved schematic and remote-device locations (**supervisee data**) to determine whether devices are in the structure at the emergency location. EX[1009], ¶[0198]; EX[1005], ¶429.

c. 7[c] “determining, using the processing device, a location of the supervisee on the blueprint based on the analyzing of the blueprint

and the at least one supervisee data, wherein the generating of the supervision data is based on the determining.”

Rauner discloses this limitation. EX[1005], ¶¶430-432. Based on analyzing the blueprint and supervisee data, structure module 1657 (part of **processing device**) **determines** and plots the **locations** of remote devices (**supervisees**) into the building schematic. EX[1009], ¶[0198]. The structure module 1657 then **generates supervision data “based on the determining”** when it “provide[s] information about a location” “to the emergency response units.” *Id.* ¶¶[0174], [0197]–[0198]. It may also use those locations to trigger ingress, egress, or evacuation plans. *Id.* ¶[0199]; §§VII.C.2.h-i (supervision notification structures).

8. Claim 8

a. 8[a] “the at least one supervisee device comprises at least one sensor,”

Rauner discloses this limitation. EX[1005], ¶433. Rauner’s remote computing device 102 (**the supervisee device**) includes a microphone sensor as part of input device 132. EX[1009], ¶¶[0061]–[0062]; EX[1001], 24:39-43 (“audio sensors (such as a microphone”); EX[1005], ¶433.

b. 8[b] “wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,”

Rauner discloses this limitation. EX[1005], ¶¶434-435. The microphone detects a **signal made by the supervisee**—the user’s voice. EX[1009], ¶[0105], [0180]; EX[1005], ¶¶434-435.

c. 8[c] “wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting.”

Rauner discloses this limitation. EX[1005], ¶¶436-437. The microphone’s audio recording **generates supervisee data based on the detecting**, which emergency sending module 111 transmits with the supervisee’s location to device communications module 151. EX[1009], ¶¶[0111], [0113]; EX[1005], ¶¶436-437.

9. Claim 10

Rauner discloses system claim 10, for the same reasons as described for 1[pre], and the remaining limitations for the same reasons as claim 1, with the same constructions and function mappings. §VII.C.2.a; §§V, VII.C.2. The mappings are as follows:

10[a]/communication device: See §§VII.C.2.b (limitation 1[a] communication device), VII.C.2.b-c, f, i (functions of 10[a][1]-10[a][4]), V; EX[1005], ¶¶438-443. For 10[a][3]’s “**supervisor data**,” the supervisee’s device transmits data incorporating supervisor-configured profile information, including the user profile created through administration module 157 and associated with the emergency event. EX[1009], ¶¶[0085], [0099], [0110]; EX[1005], ¶¶438-443.

10[b]/processing device: See §§VII.C.2.d (limitation 1[c], processing device), VII.C.2.d-e, g-h (functions of 10[b][1]-10[b][4]), V; EX[1005], ¶¶444-448.

10[c]/storage device: *See* §§VII.C.2.j (limitation 1[i], storage device), V; EX[1005], ¶449.

10[d] grid-based limitations: met for the same reasons as claim 1, §§VII.C.2.k-o. In the combined system, the grid parameter is also received by the **communication device.** §VII.C.2.1.

If PO argues the communication, processing, and storage devices must be implemented in one server computer, Rauner discloses that, too. EX[1009], ¶¶[0054], [0097]; EX[1005], ¶¶317, 321, 450-455.

10. Claim 11

Claim 11[a]-[d] corresponds to claim 2[a]-[d], respectively, and is invalid for the same reasons as claim 2 and 10. §§VII.C.3, 9; EX[1005], ¶456.

11. Claim 12

Claim 12[a]-[c] corresponds to claim 3[a]-[c], respectively, and is invalid for the same reasons as claim 3 and 10. §§VII.C.4, 9; EX[1005], ¶457.

12. Claim 13

Claim 13[a]-[b] corresponds to claim 4[a]-[b], respectively, and is invalid for the same reasons as claim 4 and 10. §§VII.C.5, 9; EX[1005], ¶458.

13. Claim 15

Claim 15[a]-[b] corresponds to method claim 6[a]-[b], respectively, and is invalid for the same reasons as claim 6 and 10. §§VII.C.6, 9; EX[1005], ¶459.

14. Claim 16

Claim 16[a]-[c] corresponds to claim 7[a]-[c], and is invalid for the same reasons as claim 7 and 10. §§VII.C.7, 9; EX[1005], ¶460.

15. Claim 17

Claim 17[a]-[c] corresponds to claim 8[a]-[c], respectively, and is invalid for the same reasons as claim 8 and 10. §§VII.C.8, 9; EX[1005], ¶461.

D. Ground 4: Obviousness of Claims 5, 9, 14, 18 in view of Rauner (EX[1009]) + Azmoodeh (EX[1010]) in further view of Noland (EX[1008]) + Knowledge of a POSITA

Claims 1 and 10 are disclosed by Rauner in view of Azmoodeh, §VII.C, and dependent claims 5, 9 (depending from claim 1) and 14, 18 (depending from claim 10) are rendered obvious in combination with Noland.

1. A POSITA Would Have Been Motivated to Combine the Rauner and Azmoodeh System with Noland

First, all three references and the '757 Patent are directed to facilitating supervision of individuals based on geofencing. EX[1001], 1:7-10; EX[1005], ¶¶462-465. Noland's threat-sensing system supervises students, staff, and other occupants of schools and facilities, and uses geofences defining "a school attendance zone or a specific building boundary that can be monitored," making it analogous to the combined Rauner+Azmoodeh system. EX[1008], ¶¶[0015]–[0019], [0061], [0148]; EX[1005], ¶¶465-467; §VII.C.1.

Second, Rauner already generally contemplates external sensors, including gunshot detection, and cross-references georeferenced events with supervisor-defined areas before distributing alerts. EX[1009], ¶¶ [0211]-[0212], [0216], [0223]. Noland's gateway improves on that gunshot-detection capability by providing specific implementation details for detecting and classifying different types of weapons. §VII.B.1; EX[1005], ¶¶468-470.

Third, a POSITA would have had a reasonable expectation of success in combining Noland's structures in the Rauner+Azmoodeh system. Noland's system gateway outputs weapon type, caliber, shooter location, and shot count, while Rauner consumes external event data and distributes it through geofence-based channels. EX[1008], ¶¶[0096], [0100], [0107]; EX[1009], ¶¶[0211]-[0214]. Integrating the gateway into Rauner's processing pipeline would require only directing that output to the existing event-processing system. EX[1005], ¶475. Both components function as server-side processors that receive, analyze, and act on incoming sensor data. EX[1005], ¶475.

Fourth, a POSITA would also have been motivated to add Noland's NFC-based personnel identification capability into the Rauner+Azmoodeh system. As described for Ground 2, Noland teaches identifying persons via NFC/RFID identifiers read by near-field devices at a geofenced facility. EX[1008], ¶¶[0034], [0074], [0148]; §VII.B.1. Rauner stores user profiles, tracks individuals in

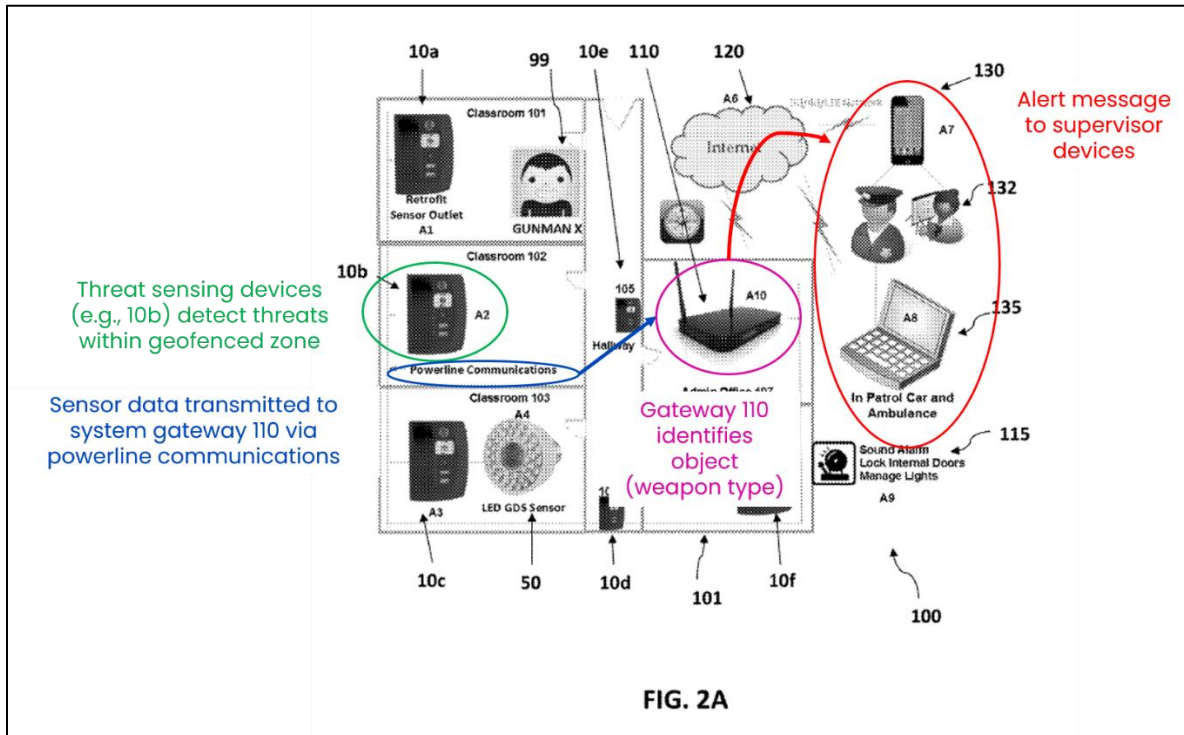
geofenced areas, and already ingests external sensor events at its server. EX[1009], ¶¶[0037], [0099], [0211]-[0212], [0244]. A POSITA would have installed Noland's NFC reader at the geofenced facility and reported its reads to Rauner's server like any other external sensor event. EX[1005], ¶473. Azmoodeh lists generic "RFID tag reader components" and "NFC smart tag detection components," EX[1010], ¶¶[0066]-[0067], [0060], but is silent on using them to identify persons or monitor geofence entry and exit. Noland supplies that application. EX[1005], ¶¶471-474. In the combined system, NFC would confirm who is present in a zone and complement Rauner's GPS tracking, using a known technique with predictable results. *Id.*

2. Claim 5

- a. 5[a] *"identifying, using the processing device, at least one object associated with the supervisee based on the analyzing of the at least one supervisee data; and"*

The combined system renders this limitation obvious. EX[1005], ¶¶476-481. As described for Ground 2, Noland's weapon detection discloses **identifying an object**, §VII.B.2.a, and it would have been obvious to integrate Noland's gateway into Rauner+Azmoodeh's **processing unit** to identify the weapon in the supervisee's geofenced zone (**object associated with the supervisee**) **based on analyzing the supervisee data**. EX[1005], ¶480; §VII.D.1. Noland Fig. 2A, annotated below, illustrates this: threat sensing devices 10a–10n report gunshot data to system

gateway 110, which determines “the general type of weapon” and the shooter’s location. EX[1008], ¶¶[0091], [0107]; EX[1005], ¶481.



b. 5[b] “determining, using the processing device, a lethality of the at least one object based on the identifying, wherein the generating of the supervision notification is based on the determining.”

The combined system renders this limitation obvious. EX[1005], ¶¶482-488. As described for Ground 2, Noland’s gateway (as integrated into Rauner+Azmoodeh’s **processing device**) **determines the object’s lethality** and **generates** an alert. §§VII.B.2.b, VII.D.1. In the combined system, Rauner’s notification framework incorporates that alert (**based on the determining**) into the **supervision notification** sent to supervisors. EX[1005], ¶¶482-488; §§VII.C.2.h-i (supervision notification structures).

3. Claim 9

- a. 9[a] “wherein the supervisee is associated with at least one identification, wherein the method comprises:”*

Rauner discloses this limitation. EX[1005], ¶489. Each **supervisee is associated** with a unique user ID and stored profile **identification**) containing identifying and contact information. EX[1009], ¶¶[0050], [0099]; §VII.C.5.a; EX[1005], ¶489. In the combined system, the supervisee’s NFC identifier is stored with that profile. EX[1008], ¶¶[0034], [0074]; EX[1005], ¶489; §VII.D.1.

- b. 9[b] “receiving, using the communication device, at least one NFC indication corresponding to the at least NFC identification from the at least one supervisee device; wherein the receiving is performed over short range wireless communication comprising at least one of Bluetooth, Zigbee, Ultra-wideband, Wi-Fi and NFC, and”*

The combined system renders this limitation obvious. EX[1005], ¶¶490-494. As in Ground 2, Noland’s NFC reader at the geofenced facility **receives the NFC indication corresponding to an NFC identification from the supervisee device over NFC**. EX[1008], ¶¶[0074], [0148]; §VII.B.4.b (9[b]). In the combined system, the reader reports that indication to Rauner’s server as Rauner receives other external sensor events, where device communications module 151 or network adapter (part of **communication device**) receives it. EX[1009], ¶¶[0067], [0211]-[0212]; §VII.D.1; EX[1005], ¶494.

- c. 9[c] “identifying, using the processing device, the supervisee based on the at least one NFC indication, wherein the*

generating of the supervision notification is based on the identifying.”

The combined system renders this limitation obvious. EX[1005], ¶¶495-499. As in Ground 2, the **supervisee is identified based on the NFC indication** by looking up the NFC identifier in stored profiles, as Noland identifies “the owners of those phones.” EX[1008], ¶[0148]; §VII.B.4.c (9[c]). In the combined system, Rauner’s processing unit 161 (**processing device**) performs the lookup and incorporates the stored profile into the supervision notification. §§VII.C.2.g-h, VII.C.5, VII.D.1; EX[1005], ¶¶497-498.

4. Claim 14

Claim 14[a]-[b] recites the “processing device” of claim 10 (Ground 3) performing the functions of limitations 5[a]-[b], and is invalid for the same reasons as claim 5 and 10 (Ground 3). §§VII.D.2, VII.C.9; EX[1005], ¶500.

5. Claim 18

Claim 18 is invalid for the same reasons as claims 9 and 10 (Ground 3). §§VII.D.3, VII.C.9. Claim 18 specifies NFC identification in the preamble, but NFC identification is already covered in claim 9. EX[1005], ¶501.

VIII. SECONDARY CONSIDERATIONS

Petitioners are aware of no evidence of secondary considerations that would meaningfully rebut a finding of obviousness.

IX. CONCLUSION

Petitioners respectfully request that the Challenged Claims be cancelled.

Respectfully submitted,

October 8, 2026

/ Eliot D. Williams /

Eliot D. Williams (Reg. No. 50,822)
Katharine Burke
(*pro hac vice* application forthcoming)
Sam Kassa
(*pro hac vice* application forthcoming)
BAKER BOTTS L.L.P.
700 K Street Northwest Suite 900,
Washington, DC 20001-5692
202.639.7700

Matthew Thompson (Reg. No. 80,905)
BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, NY 10112-4498
212.408.2580

*Attorneys for Petitioners, Rave Wireless,
Inc. and Motorola Solutions, Inc.*

CERTIFICATE OF SERVICE

In accordance with 37 C.F.R. §§42.6(e) and 42.105, the undersigned certifies that on October 8, 2026 a complete and entire copy of the **PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,468,757 UNDER 35 U.S.C. §§311-319 AND 37 C.F.R. §§42.100 *ET SEQ.*** (“Petition”) including exhibits and testimony relied upon were served via overnight mail on the Patent Owner at the correspondence address of record for the subject patent and via electronic mail on counsel for Patent Owner in the District Court Litigation, as included below:

The Law Office of Michael J. Scheer
5531 Murietta Avenue
Sherman Oaks CA 91401

Robert M. Harkins
CHERIAN HARKINS DUNHAM LLP
555 12th Street, Suite 2140
Oakland, CA 94607
bobh@chdlaw.com

Date: October 8, 2026

/ Eliot D. Williams /

Eliot D. Williams (Reg. No. 50,822)
Katharine Burke
(*pro hac vice* application forthcoming)
Sam Kassa
(*pro hac vice* application forthcoming)
BAKER BOTTS L.L.P.
700 K Street Northwest Suite 900,
Washington, DC 20001-5692
202.639.7700

Matthew Thompson (Reg. No. 80,905)

BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, NY 10112-4498
212.408.2580

*Attorneys for Petitioners, Rave Wireless,
Inc. and Motorola Solutions, Inc.*

CERTIFICATION UNDER 37 C.F.R. §42.24(d)

Pursuant to 37 C.F.R. §42.24(d), the undersigned hereby certifies that the word count under §42.24(a)(1) for the foregoing Petition for *Inter Partes* Review totals 13,973 words, within the 14,000 word limit allowed under §42.24(a)(1)(i).

Date: October 8, 2026

/ Eliot D. Williams /

Eliot D. Williams (Reg. No. 50,822)
Katharine Burke
(*pro hac vice* application forthcoming)
Sam Kassa
(*pro hac vice* application forthcoming)
BAKER BOTTS L.L.P.
700 K Street Northwest Suite 900,
Washington, DC 20001-5692
202.639.7700

Matthew Thompson (Reg. No. 80,905)
BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, NY 10112-4498
212.408.2580

*Attorneys for Petitioners, Rave Wireless,
Inc. and Motorola Solutions, Inc.*