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
Patent 11,468,757

IPR2027-00010
Patent 12,154,421

_____

DECLARATION OF MR. DAVID H. WILLIAMS

Table of Contents

EXHIBIT LIST....22
I. SUMMARY OF OPINIONS....25
II. BACKGROUND AND EDUCATION....26
III. LEGAL FRAMEWORK....34
IV. LEVEL OF SKILL IN THE ART....38
V. TECHNOLOGICAL BACKGROUND....39
A. Location Technologies, driven by The 1996 Telecommunications Act, were utilized for a wide variety of commercial Location-Based Services (LBS) starting in the early 2000s....40
B. Sharing of Location Information with others, including supervisors/supervisor-type roles, has been well-known since well before the patent priority date....42
C. The use of commercial location boundary-related capabilities and applications began at least by the year 2000, with related concepts beginning much earlier....44
D. The use of grids in Location-Based Services and Geofences was also well known prior to the patent priority date....49
E. Architecture enabling geofences has varied from server-based systems to device-based systems to hybrids, varying as needed by available resources and use case specifics as well as technology advancements....55
1. Server-based....55
2. Device-based....57
3. Hybrids....57
F. Message handling, event processing, and data storage were conventionally implemented as cooperating software components on shared server infrastructure....60
G. The use of many of the above capabilities was well-known in a variety of industries prior to the Asserted Patents, with various use cases involving specific types and organizations of geofences, grids, and underlying map data....61
VI. THE CHALLENGED PATENTS....63
A. '757 PATENT....63
1. Priority....63
2. Overview of the '757 Patent....63

B. ’421 Patent 69
1. Priority 69
2. Overview of the ’421 Patent 70
VII. CLAIM CONSTRUCTION 71
VIII. DESCRIPTION OF THE PRIOR ART 75
A. Staton (Ex.1007) 75
B. Noland (Ex.1008) 78
C. Rauner (Ex.1009) 80
D. Azmoodeh (Ex.1010) 83
E. Smith (Ex.1011) 84
IX. INVALIDITY OF ’757 PATENT CLAIMS 1-18 UNDER 35 U.S.C. § 103 87
A. Ground 1: Claims 1-4, 6, 8, 10-13, 15, 17 are Rendered Obvious By Staton + Knowledge of a POSITA 87
1. Relevant Architecture 87
a. Architecture of Staton 87
b. A POSITA’s Understanding of the Architecture 93
2. Claim 1 96
a. 1[pre]: “A method for facilitating supervision of individuals based on geofencing, the method comprising:” 96
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;” 98
c. 1[b]: “receiving, using the communication device, a geographical location from the at least one supervisor device;” 102
d. 1[c]: “analyzing, using a processing device, the geographical location based on the at least one security parameter;” 106
e. 1[d]: “generating, using the processing device, a geofence corresponding to a geographical area based on the analyzing;” 110
f. 1[e] : “receiving, using the communication device, at least one supervisee data associated with a supervisee from at least one supervisee device;” 115

g. 1[f]: “analyzing, using the processing device, the at least one supervisee data based on the geofence;”.....117

h. 1[g]: “generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data;”.....127

i. 1[h]: “transmitting, using the communication device, the supervision notification to the at least one supervisor device; and” 130

j. 1[i]: “storing, using a storage device, the at least one supervisee data and the supervision notification, wherein:” 132

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:”.....134

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:”.....137

m. 1[j][2]: “analyzing, using the processing device, the at least one grid parameter;”.....139

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” 140

o. 1[j][4]: “generating, using the processing device, a number of geofence grid boxes based on the determining.”.....142

3. Claim 2 145

a. 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;”.....146

b. 2[b]: “identifying, using the processing device, at least one location corresponding to the at least one location indication;” 147

c. 2[c]: “analyzing, using the processing device, the at least one supervisee data based on the at least one location; and” 148

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.”.....152

4. Claim 3 155

a. 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:” 155

b. 3[b]: “determining, using the processing device, the at least one action based on the supervision notification; and” 155

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.” 156

5. Claim 4 159

a. 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” 159

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.” 161

6. Claim 6 162

a. 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;” 162

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.” 163

7. Claim 8 166

a. 8[a]: “The method of claim 1, wherein the at least one supervisee device comprises at least one sensor” 166

b. 8[b]: “wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,” 166

c. 8[c]: “wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting.” 167

8. Claim 10 167

a. 10[pre]: “A system for facilitating supervision of individuals based on geofencing, the system comprising:” 167

b. 10[a]: “a communication device configured for:” 168

c. 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;” 168

d. 10[a][2]: “receiving, using the communication device, a geographical location from the at least one supervisor device;” 168

e. 10[a][3]: “receiving at least one supervisor data associated with a supervisee from at least one supervisee device; and” 169

f. 10[a][4]: “transmitting a supervision notification to the at least one supervisor device;” 169

g. 10[b]: “a processing device configured for:” 169

h. 10[b][1]: “analyzing the geographical location based on the at least one security parameter;” 170

i. 10[b][2]: “generating a geofence corresponding to a geographical area based on the analyzing;” 171

j. 10[b][3]: “analyzing the at least one supervisee data based on the geofence; and” 171

k. 10[b][4]: “generating the supervision notification based on the analyzing of the at least one supervisee data; and” 171

l. 10[c]: “a storage device configured for storing the at least one supervisee data and the supervision notification, wherein:” 172

m. 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,” 172

n. 10[d][1]: “wherein the communication device is further configured for receiving at least one grid parameter from the at least one supervisor device” 172

o. 10[d][2]: “wherein the processing device is further configured for: analyzing the at least one grid parameter;” 173

p. 10[d][3]: “determining the grid box geofence area based on the analyzing of the at least one grid parameter; and” 173

q. 10[d][4]: “generating a number of geofence grid boxes based on the determining.”.....173

9. Claim 11: “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: identifying at least one location corresponding to the at least one location indication; analyzing the at least one supervisee data based on the at least one location; and 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.” 174

10. Claim 12: “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: determining the at least one action based on the supervision notification; and 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.”.....175

11. Claim 13: “*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, 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*.”.....175

12. Claim 15: “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: 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.”.....176

13. Claim 17: “*The system of claim 10, wherein the at least one supervisee device comprises at least one sensor, wherein the at least one sensor is configured for detecting at least one signal made by the supervisee, wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting*.” 176

B. Ground 2: Obviousness of Claims 5, 7, 9, 14, 16, and 18 over Staton In View Of Noland + Knowledge Of A POSITA 176

1. A POSITA Would Have Combined Staton with Noland 177

2. Claim 5 183

a. 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" 183

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." 184

3. Claim 7 186

a. 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;" 186

b. 7[b]: "analyzing, using the processing device, the blueprint and the at least one supervisee data; and" 188

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." 189

4. Claim 9 191

a. 9[a]: "The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises:" 191

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" 193

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." 194

5. Claim 14: "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 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." 196

6. Claim 16: "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, wherein the processing device is further configured for analyzing the blueprint and the at least one supervisee data; and 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." 196

7. Claim 18: "The system of claim 10, wherein the supervisee is associated with at least one near field communication (NFC) identification, 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, wherein the processing device is further configured for identifying the supervisee based on the at least one NFC indication, wherein the generating of the supervision notification is based on the identifying." .. 197

C. Ground 3: Claims 1-4, 6-8, 10-13, and 15-17 Are Rendered Obvious By Rauner In View Of Azmoodeh + Knowledge Of A POSITA 197

1. Rauner + Azmoodeh Combined Architecture 197

2. A POSITA Would Have Been Motivated to Combine Rauner With Azmoodeh 201

3. Claim 1 208

1[pre]: "A method for facilitating supervision of individuals based on geofencing, the method comprising:" 208

a. 1[a]: "receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor;" 210

b. 1[b]: "receiving, using the communication device, a geographical location from the at least one supervisor device;" 215

c. 1[c]: "analyzing, using a processing device, the geographical location based on the at least one security parameter;" 216

d. 1[d]: "generating, using the processing device, a geofence corresponding to a geographical area based on the analyzing;" 219

e. 1[e] : "receiving, using the communication device, at least one supervisee data associated with a supervisee from at least one supervisee device;" 220

f. 1[f]: “analyzing, using the processing device, the at least one supervisee data based on the geofence;”.....221

g. 1[g]: “generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data;”.....223

h. 1[h]: “transmitting, using the communication device, the supervision notification to the at least one supervisor device; and” 225

i. 1[i]: “storing, using a storage device, the at least one supervisee data and the supervision notification, wherein:” 226

j. 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:”.....228

k. 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:”.....231

l. 1[j][2]: “analyzing, using the processing device, the at least one grid parameter;”.....232

m. 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” 233

n. 1[j][4]: “generating, using the processing device, a number of geofence grid boxes based on the determining.”.....234

4. Claim 2 236

a. 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;”.....236

b. 2[b]: “identifying, using the processing device, at least one location corresponding to the at least one location indication;” 237

c. 2[c]: “analyzing, using the processing device, the at least one supervisee data based on the at least one location; and” 239

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.”.....240

5. Claim 3 242

a. 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:” 242

b. 3[b]: “determining, using the processing device, the at least one action based on the supervision notification; and” 243

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.” 244

6. Claim 4 246

a. 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” 246

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.” 247

7. Claim 6 248

a. 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;” 248

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.” 251

8. Claim 7 253

a. 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;” 253

b. 7[b]: “analyzing, using the processing device, the blueprint and the at least one supervisee data; and” 254

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.”.....255
9. Claim 8 257
a. 8[a]: “The method of claim 1, wherein: the at least one supervisee device comprises at least one sensor” 257
b. 8[b]: “wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,” 258
c. 8[c]: “wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting.”.....258
10. Claim 10 259
a. 10[pre]: “A system for facilitating supervision of individuals based on geofencing, the system comprising:” 259
b. 10[a]: “a communication device configured for:”.....260
c. 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;” 260
d. 10[a][2]: “receiving, using the communication device, a geographical location from the at least one supervisor device;” 260
e. 10[a][3]: “receiving at least one supervisor data associated with a supervisee from at least one supervisee device; and” 260
f. 10[a][4]: “transmitting a supervision notification to the at least one supervisor device;”.....261
g. 10[b]: “a processing device configured for:” 261
h. 10[b][1]: “analyzing the geographical location based on the at least one security parameter;” 261
i. 10[b][2]: “generating a geofence corresponding to a geographical area based on the analyzing;” 262
j. 10[b][3]: “analyzing the at least one supervisee data based on the geofence; and”.....262
k. 10[b][4]: “generating the supervision notification based on the analyzing of the at least one supervisee data; and” 262
l. 10[c]: “a storage device configured for storing the at least one supervisee data and the supervision notification, wherein:”.....262

m. 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,”.....263

n. 10[d][1]: “wherein the communication device is further configured for receiving at least one grid parameter from the at least one supervisor device” 263

o. 10[d][2]: “wherein the processing device is further configured for: analyzing the at least one grid parameter;”.....263

p. 10[d][3]: “determining the grid box geofence area based on the analyzing of the at least one grid parameter; and”.....263

q. 10[d][4]: “generating a number of geofence grid boxes based on the determining.”.....264

11. Claim 11: “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: identifying at least one location corresponding to the at least one location indication; analyzing the at least one supervisee data based on the at least one location; and 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.” 264

12. Claim 12: “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: determining the at least one action based on the supervision notification; and 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.”.....265

13. Claim 13: “*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, 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.*”.....265

14. Claim 15: "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: 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." 266

15. Claim 16: "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, wherein the processing device is further configured for analyzing the blueprint and the at least one supervisee data; and 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." 267

16. Claim 17: "*The system of claim 10, wherein the at least one supervisee device comprises at least one sensor, wherein the at least one sensor is configured for detecting at least one signal made by the supervisee, wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting*." 267

D. Ground 4: Claims 5, 9, 14, and 18 Are Rendered Obvious By Rauner In View Of Azmoodeh And Further In View Of Noland + Knowledge Of A POSITA.....268

1. A POSITA Would Have Been Motivated To Combine The Rauner-Azmoodeh Combination With Noland.....269

2. Claim 5 275

a. 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;".....275

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." 278

3. Claim 9 281

a. 9[a]: "The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises:".....281

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" 282

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." 284

4. Claim 14: "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 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." 286

5. Claim 18: "The system of claim 10, wherein the supervisee is associated with at least one near field communication (NFC) identification, 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, wherein the processing device is further configured for identifying the supervisee based on the at least one NFC indication, wherein the generating of the supervision notification is based on the identifying." ..287

X. INVALIDITY OF '421 PATENT CLAIMS 1-24 UNDER 35 U.S.C. § 103 287

A. Ground 1: Claims 1-4, 6, 10-14, 16, and 20-21 of the '421 Patent Is Rendered Obvious By Staton (Ex.1007) + Knowledge Of A POSITA 288

1. Claim 1 288

a. Scope of this opinion and relationship to my '757 analysis.....288

b. Claim 1 of the '421 Patent is substantially similar to claim 1 of the '757 Patent.....289

2. Claim 2 291

3. Claim 3 292

4. Claim 4 292

5. Claim 6 293

6. Claim 10 293

a. 10[a]: The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises: 293

b. 10[b]: receiving, using the communication device, at least one indication corresponding to the at least one identification from the at least one supervisee device; and 294

c. 10[c]: identifying, using the processing device, the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying. 295

7. Claim 11 296

8. Claim 12 298

9. Claim 13 298

10. Claim 14 299

11. Claim 16 299

12. Claim 20 300

a. 20[a]: The system of claim 11, wherein the supervisee is associated with at least one identification, ...300

b. 20[b]: wherein the communication device is further configured for receiving at least one indication corresponding to the at least one identification from the at least one supervisee device, ...300

c. 20[c]: wherein the processing device is further configured for identifying the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying. 301

13. Claim 21: The system of claim 11, wherein each geofence grid box is further characterized by: a) storing at least one emergency contact number associated with the geographical area represented by the grid box geofence area; b) wherein the emergency contact number includes a 911 service or equivalent emergency service specific to then geographical area of the grid box; and c) wherein the processing device is configured to automatically select and transmit supervisee data to the stored emergency contact number upon detecting an emergency situation within the corresponding grid box geofence area. 302

a. 21[a]: The system of claim 11, wherein each geofence grid box is further characterized by: a) storing at least one emergency contact number associated with the geographical area represented by the grid box geofence area; 302

b. 21[b]: b) wherein the emergency contact number includes a 911 service or equivalent emergency service specific to then geographical area of the grid box; and 303

c. 21[c]: c) wherein the processing device is configured to automatically select and transmit supervisee data to the stored emergency contact number upon detecting an emergency situation within the corresponding grid box geofence area.....303

B. Ground 2: Claims 5, 7, 8, 15, 17-19, 22, 23, and 24 of the '421 Patent Are Rendered Obvious By Staton (Ex.1007) In View Of Noland (Ex.1008) + Knowledge Of A POSITA.....304

1. A POSITA would have combined Staton with Noland.....304

2. Claim 5.....307

3. Claim 7.....307

4. Claim 8.....308

a. 8[a]: The method of claim 1, wherein the at least one supervisee device comprises at least one sensor,.....308

b. 8[b]: wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,.....309

c. 8[c]: wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting.....309

5. Claim 15.....310

6. Claim 17.....310

7. Claim 18.....311

8. Claim 19.....311

a. 19[a]: The system of claim 18, wherein: the at least one signal made by the supervisee comprises shaking the supervisee device abruptly, pressing a button, or speaking a specific phrase, wherein: the at least one sensor is configured for detecting the at least one signal,.....311

b. 19[b]: and the supervisee device is configured to optionally make an emergency call when the at least one sensor detects the at least one signal; 312

c. 19[c]: wherein a phone number dialed in the emergency call is determined based on the geofence.....312

9. Claim 22.....313

a. 22[i]: the at least one supervisee device comprises at least one sensor, 315

b. 22[j]: wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,.....316
c. 22[k]: wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting, ...317
d. 22[l]: wherein the supervisee data comprises audio and video recordings;.....317
e. 22[m]: wherein the at least one sensor is selected from one or more nearby sensors based on the most proximal nearby sensor by geographical location in real-time; and 318
f. 22[n]: wherein the at least one sensor tracks the supervisee as the supervisee moves between the one or more nearby sensors. 320
10. Claim 23 322
a. 23[a]: The method of claim 22, wherein: the supervision notification is sent to a first distinct group of one or more supervisor devices correlated with the geographical location; 322
b. 23[b]: the first distinct group of one or more supervisor devices is comprised of nearby first responders and dispatchers; and 323
c. 23[c]: the supervision notification may be sent to a second distinct group of one or more supervisor devices based on the location and expertise of the second distinct group. 324
11. Claim 24: The method of claim 22, wherein: wherein the supervisee is associated with at least one identification, wherein the communication device is further configured for receiving at least one indication corresponding to the at least one identification from the at least one supervisee device, wherein the processing device is further configured for identifying the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying. 325
C. Ground 3: Claim 9 of the '421 Patent Is Rendered Obvious By Staton (Ex.1007) In View Of Smith (Ex.1011) + Knowledge Of A POSITA.....326
1. A POSITA would have combined Staton with Smith 326
2. Claim 9 329
a. 9[a]: The method of claim 1, wherein: the at least one security parameter comprises an altitude,.....330
b. 9[b]: the at least one grid parameter comprises a building floor, and..331
c. 9[c]: the building floor is estimated from the altitude.....332

D. Ground 4: Claims 1-4, 6-8, 10-14, and 16-21 of the '421 Patent Are Rendered Obvious By Rauner (Ex.1009) In View Of Azmoodeh (Ex.1010) + Knowledge Of A POSITA 334
1. A POSITA would have combined Rauner with Azmoodeh 334
2. Claim 1 336
3. Claim 2 338
4. Claim 3 338
5. Claim 4 339
6. Claim 6 339
7. Claim 7 340
8. Claim 8 340
9. Claim 10 342
a. 10[a]: The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises: 342
b. 10[b]: receiving, using the communication device, at least one indication corresponding to the at least one identification from the at least one supervisee device; and 343
c. 10[c]: identifying, using the processing device, the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying. 344
10. Claim 11 346
11. Claim 12 347
12. Claim 13 348
13. Claim 14 348
14. Claim 16 349
15. Claim 17 349
16. Claim 18 350
17. Claim 19 351
a. 19[a]: The system of claim 18, wherein: the at least one signal made by the supervisee comprises shaking the supervisee device abruptly, pressing a button, or speaking a specific phrase, wherein: the at least one sensor is configured for detecting the at least one signal,..... 351

b. 19[b]: and the supervisee device is configured to optionally make an emergency call when the at least one sensor detects the at least one signal; 352

c. 19[c]: wherein a phone number dialed in the emergency call is determined based on the geofence. 353

18. Claim 20 355

a. 20[a]: The system of claim 11, wherein the supervisee is associated with at least one identification, ...355

b. 20[b]: wherein the communication device is further configured for receiving at least one indication corresponding to the at least one identification from the at least one supervisee device, ...355

c. 20[c]: wherein the processing device is further configured for identifying the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying. 356

19. Claim 21 356

a. 21[a]: The system of claim 11, wherein each geofence grid box is further characterized by: a) storing at least one emergency contact number associated with the geographical area represented by the grid box geofence area; 357

b. 21[b]: b) wherein the emergency contact number includes a 911 service or equivalent emergency service specific to then geographical area of the grid box; and 359

c. 21[c]: c) wherein the processing device is configured to automatically select and transmit supervisee data to the stored emergency contact number upon detecting an emergency situation within the corresponding grid box geofence area....360

E. Ground 5: Claims 5, 15, and 22-24 of the '421 Patent Are Rendered Obvious By Rauner (Ex.1009) In View Of Azmoodeh (Ex.1010) And Further In View Of Noland (Ex.1008) + Knowledge Of A POSITA 361

1. A POSITA would have combined the Rauner-Azmoodeh system with Noland 362

2. Claim 5 365

3. Claim 15 365

4. Claim 22 366

a. 22[l]: wherein the supervisee data comprises audio and video recordings;....368

b. 22[m]: wherein the at least one sensor is selected from one or more nearby sensors based on the most proximal nearby sensor by geographical location in real-time; and 369

c. 22[n]: wherein the at least one sensor tracks the supervisee as the supervisee moves between the one or more nearby sensors. 370

5. Claim 23 373

a. 23[a]: The method of claim 22, wherein: the supervision notification is sent to a first distinct group of one or more supervisor devices correlated with the geographical location; 373

b. 23[b]: the first distinct group of one or more supervisor devices is comprised of nearby first responders and dispatchers; and 374

c. 23[c]: the supervision notification may be sent to a second distinct group of one or more supervisor devices based on the location and expertise of the second distinct group. 375

6. Claim 24: The method of claim 22, wherein: wherein the supervisee is associated with at least one identification, wherein the communication device is further configured for receiving at least one indication corresponding to the at least one identification from the at least one supervisee device, wherein the processing device is further configured for identifying the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying. 377

F. Ground 6: Claim 9 of the '421 Patent Is Rendered Obvious By Rauner (Ex.1009) In View Of Azmoodeh (Ex.1010) And Further In View Of Smith (Ex.1011) + Knowledge Of A POSITA....377

1. A POSITA would have combined the Rauner-Azmoodeh system with Smith....378

2. Claim 9 382

a. 9[a]: The method of claim 1, wherein: the at least one security parameter comprises an altitude,....382

b. 9[b]: the at least one grid parameter comprises a building floor, and..383

c. 9[c]: the building floor is estimated from the altitude....385

XI. CONCLUSION....386

Appendix I: Claim Listing....388

XII. ’757 Patent Claims 388

generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data; 388

storing, using a storage device, the at least one supervisee data and the supervision notification, wherein: 388

XIII. ’421 Patent Claims 396

generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data; 396

storing, using a storage device, the at least one supervisee data and the supervision notification, wherein: 396

EXHIBIT LIST

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

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

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

I, David Williams, hereby declare the following:

I. SUMMARY OF OPINIONS

1. I have been asked by counsel for Rave Wireless, Inc. and Motorola Solutions, Inc. (collectively, "Petitioners") to provide this declaration addressing the validity of claims 1-18 of U.S. Patent No. 11,468,757 ("'757 Patent") and claims 1-24 of U.S. Patent No. 12,154,421 ("'421 Patent"). It is my opinion that each of these claims is invalid in view of the prior art.

2. The opinions that follow demonstrate that claims 1-18 of the '757 Patent are invalid at least based on the following grounds:

Ground	Claims	Reference(s)
1	1-4, 6, 8, 10-13, 15, 17	Staton + knowledge of a POSITA
2	5, 7, 9, 14, 16, 18	Staton + Noland + knowledge of a POSITA
3	1-4, 6-8, 10-13, 15-17	Rauner + Azmoodeh + knowledge of a POSITA
4	5, 9, 14, 18	Rauner + Azmoodeh + Noland + knowledge of a POSITA

3. The opinions that follow demonstrate that claims 1-24 of the '421 Patent are invalid at least based on the following grounds:

Ground	Claims	Reference(s)
1	1-4, 6, 10, 11-14, 16, 20, 21	Staton + knowledge of a POSITA
2	5, 7, 8, 15, 17-19, 22-24	Staton + Noland + knowledge of a POSITA
3	9	Staton + Smith + knowledge of a POSITA
4	1-4, 6-8, 10-14, 16-21	Rauner + Azmoodeh + knowledge of a POSITA
5	5, 15, 22-24	Rauner + Azmoodeh + Noland + knowledge of a POSITA
6	9	Rauner + Azmoodeh + Smith + knowledge of a POSITA

II. BACKGROUND AND EDUCATION

4. In formulating my opinions, I have relied upon my training, knowledge, and experience in the relevant art. A copy of my current curriculum vitae is provided as Ex.1006, and it provides a comprehensive description of my academic and employment history over the last forty-plus years. I have over 35 years of experience in wireless location services, including experience designing, implementing, and managing numerous location-based service (LBS) applications such as mobile social networking, family tracking, and

mobile resource management, as well as working in all fields within the location services ecosystem including all forms of location determination technologies, map data, handset technologies, and associated Information Technology systems including identification, authentication, privacy, security, and other related capabilities such as network engineering and operations.

5. I am currently the President of the company E911-LBS Consulting, and I have been with the company since 2002. As the President of E911-LBS Consulting, I provide services across the entire wireless value chain, particularly with respect to technology and business strategic planning and product design and development associated with LBS, Global Positioning Satellite (GPS) systems, E911, WiFi-Based and other medium/long-range Real-Time Location Systems (RTLS), Radio Frequency Identification (RFID), Bluetooth, Near Field Communications (NFC), and beacon-based and other short-range communications/location systems, and other location determination and sensing technologies and services.

6. I have extensive expertise in all aspects of LBS delivery across the wireless location ecosystem including enabling network, map data, geospatial platform, chipset, data management, device, services, and location determination infrastructure and integration providers. I am an expert in all related aspects of LBS, including data privacy and security management.

7. For example, in the 1995 to 2000 timeframe, as an Associate Partner in the Communications & High Technology Practice of Accenture (one of the world's leading technology companies), I focused on using wireless location technologies to provide services to the public sector and commercial markets. In particular, from 1998 to 2000, I led the development of the LBS product/technology strategy and roadmap for Nextel Communications, Inc. My work with Nextel resulted in some of the earliest LBS applications in the U.S. market and included extensive research into the potential use of various technologies in providing and enabling a wide array of location-based services. Many of the Nextel products selected for development and implementation included various forms of worker and asset tracking, matching—based on their location—workers with other workers, or workers with assets (*e.g.*, field equipment, vehicles, etc.). This work also included leading the development of the underlying network and Information Technology architectures that would be required to support the LBS applications product strategy and roadmap.

8. In 2003, I led the development of part of AT&T Wireless's E911 infrastructure, including the development of systems, processes, and reporting infrastructure to manage and track the deployment of time difference of arrival-based location determination technologies. I managed the testing and Federal Communications Commission reporting of network location inaccuracies, with a particular focus on detecting and troubleshooting out-of-norm technology

deployment and inaccurate location conditions. From 2005 to 2007, I worked with NAVTEQ—the leading provider of map data and services essential to creating LBS applications—to develop the company's web developer website content and tools. Specifically, I designed and managed the site map and overall content, including the development of comprehensive technical and business web content for all NAVTEQ map product and service lines. Through the developer site, application developers and business managers became intimately familiar with map data, Geographical Information System (GIS) platforms, and location-based services to successfully develop and launch their LBS applications. For example, I developed the content to highlight key types of map data and to provide technical details on how NAVTEQ tools can be used in LBS design for various consumer and business applications.

9. I also have extensive LBS application product design and implementation experience, which includes data privacy and security management. For example, from 2007 to 2010, I managed the design, development, and launch of several consumer and business-oriented LBS applications for AT&T Mobility. These LBS applications included mobile social networking, family tracking, local search, 411-with-LBS, mobile resource management, and asset tracking. I also developed corporate-wide location data privacy policies and associated systems and process implementations for all LBS customers.

10. My AT&T work extensively involved authentication of location-related use of LBS applications. In particular, I was the Product Realization Manager (the person responsible for implementation of a product) for several LBS apps that allowed the sharing of location information, including between multi-device applications. One of these applications was the Loopt social networks application. This role and work required extensive knowledge of how the app worked (including its use of geofences), and even required design modifications in order for it to "fit into" AT&T's network and IT infrastructure, as well as to implement AT&T's privacy and security policies. The work also included designing/modifying AT&T's network and IT infrastructure to allow/enable the Loopt app to seamlessly work with AT&T's location infrastructure and various IT systems used for functions including Sales, Customer Care, Fulfillment, Billing/Accounts Receivable, and various network and IT operations. The work also included extensive work with AT&T Legal to develop and implement AT&T's location privacy policies. The integration of the application into the above required extensive authorization-related design work to ensure that a given user could appropriately access the various AT&T systems and subsystems, as well as the application, under the appropriate conditions/circumstances, including appropriately authorizing the use of and the sharing of users' location with other users and/or systems and applications. This work in location-related data security and privacy networking resulted in a patent:

U.S. Patent 8,613,109, titled "*Method and Apparatus for Providing Mobile Social Networking Privacy*," that issued on December 17, 2013, of which I was the only non-employee inventor.

11. Much of the above work was replicated in my lead implementation role for AT&T FamilyMap, focused on child tracking and family safety. Capabilities included location sharing across family members, geofence creation (*e.g.* at school, at home), and monitoring and alert generation when rule conditions were met (*e.g.* alert if child goes more than 100 feet from house).

12. This work was replicated in various forms for other LBS applications for which I was the Lead Product Realization Manager, including Slifter Local Search, 411-with-LBS, AT&T Navigator, and Telenav Mobile Resource Management and Asset Management products. The Telenav work in particular involved supervisor—supervisee related functionality involving location sharing between field workers and supervisors, and using that information to schedule and optimize additional field service visits based on location, areas served, available routes and conditions, and time, assets, and services required.

13. I also served as the Lead Product Realization Manager for an early LBS-based golfing game system (called CaddyHawk), which enabled the use of location to track and improve a golfer's game based on his/her position on the course relative to the hole and/or other obstacles/constraints on the golf course.

14. In addition to the Location-Based Services applications, enabling location technologies, wireless communications, and privacy and security experience and expertise described above, I also have many years of Information Technology experience. For example, as a consultant in the Information Technology practices of Deloitte Consulting (originally Touche Ross), Booz Allen & Hamilton, and Andersen Consulting (now Accenture), I served in key technology development and technology leadership roles in numerous projects designing and implementing mainframe, mini-computer, and client-server based computing systems across a wide variety of industries and a wide variety of functions/applications.

15. I also led the design and development of a number of different communications networks associated with the above computing systems, including wide- and local-area networks, utilizing both wired and wireless technologies, involving private and public (*e.g.*, Internet-based) communications backbones. This communications system expertise includes underlying expertise in the electrical characteristics of communications signals, extending back to the early 1980s with my Electrical Engineering degree from Purdue University in 1983 and my work as an EE in the design of the Analog-to-Digital Signal Converter unit for the F-15 fighter jet radar system while with Hughes Aircraft Company Radar Systems Division from 1983-1985.

16. I have authored multiple books on wireless location, including:

- *The Definitive Guide to GPS, RFID, Wi-Fi, and Other Wireless Location-Based Services* (2005 and 2009 versions);
- *The Definitive Guide to Wireless E911 (2004 and 2005 versions)*; and
- *The Definitive Guide to Mobile Positioning and Location Management (co-author)*

17. I have been deposed in over 75 matters, and testified in court and similar venues 17 times. I have been an expert on matters involving over 200 patents, and in over 60 criminal/civil forensics matters. Several of these patent and forensics matters have involved the establishing, monitoring, and use/alert generation associated with geofences.

18. In addition to the AT&T patent, I am the sole or lead inventor in 13 location and context-related patents, primarily aimed at "bad" behavior monitoring and preemptive modification/prevention.

19. I received a B.S. degree in Electrical Engineering from Purdue University in 1983 with top honors. I received a MBA degree in Information Systems Management from The University of Texas at Austin in 1987, also with top honors.

20. My *curriculum vitae* contains further details on my education, experience, publications, and other qualifications to render an expert opinion.

Ex.1006. My work on these matters is being billed to counsel for Petitioners at a flat rate of $550 per hour, with reimbursement for actual expenses. My compensation is not contingent upon the outcome of these proceedings.

III. LEGAL FRAMEWORK

21. I understand that a patent claim is not patentable under 35 U.S.C. § 103 if the differences between the patent claim and the prior art are such that the claimed subject matter as a whole would have been obvious at the time the claimed invention was made to a person having ordinary skill in the art to which the subject matter pertains. Obviousness, as I understand it, is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and, to the extent that they exist and have an appropriate nexus to the claimed invention (as opposed to prior art features), secondary indicia of non-obviousness.

22. I have been informed that whether there are any relevant differences between the prior art and the claimed invention is to be analyzed from the view of a person of ordinary skill in the art at the time of the invention. As such, my opinions below as to a person of ordinary skill in the art are as of the time of the invention, even if not expressly stated as such; for example, even if stated in the present tense.

23. In analyzing the relevance of any differences between the claimed invention and the prior art, I have been informed that I must consider the impact, if

any, of such differences on the obviousness or non-obviousness of the invention as a whole, not merely some portion of it. The person of ordinary skill faced with a problem is able to apply his or her experience and ability to solve the problem and also look to any available prior art to help solve the problem.

24. An invention is obvious if a person of ordinary skill in the art, facing the wide range of needs created by developments in the field, would have seen an obvious benefit to the solutions tried by the applicant. When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, it would be obvious to a person of ordinary skill to try the known options. If a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique would have been obvious.

25. It is my understanding that a teaching in the prior art directed to the subject matter of the claimed invention is not needed and that one may take into account the inferences and creative steps that a person of ordinary skill in the art would have employed in reviewing the prior art at the time of the invention. For example, if the claimed invention combined elements known in the prior art and the combination yielded results that were predictable to a person of ordinary skill in the art at the time of the invention, then this evidence would make it more likely that the claim was obvious. On the other hand, if the combination of known elements yielded

unexpected or unpredictable results, or if the prior art teaches away from combining the known elements, then this evidence would make it more likely that the claim that successfully combined those elements was not obvious.

26. I understand that hindsight must not be used when comparing the prior art to the claims for obviousness.

27. It is my understanding that obviousness may also be shown by demonstrating that it would have been obvious to modify what is taught in a single piece of prior art to create the subject matter of the patent claim. Obviousness may be shown by showing that it would have been obvious to combine the teachings of more than one item of prior art. In determining whether a piece of prior art could have been combined with other prior art or combined with or modified in view of other information within the knowledge of one of ordinary skill in the art, the following are examples of approaches and rationales that may be considered:

- Combining prior art elements according to known methods to yield predictable results;
- Simple substitution of one known element for another to obtain predictable results;
- Use of a known technique to improve similar devices (methods, or products) in the same way;
- Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;

RAVE/MSI, EX1005, p. 37

- Applying a technique or approach that would have been "obvious to try" (choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success);
- Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; or
- Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

28. I understand that the rationale for modifying a reference and/or combining references may come from sources such as explicit statements in the prior art, or the knowledge of one of ordinary skill in the art, including any need or problem known in the field at the time, even if different from the specific need or problem addressed by the inventor of the patent claim.

29. I understand that even if a *prima facie* case of obviousness is established, the final determination of obviousness must also consider "secondary considerations" if presented. In most instances, the patentee raises these secondary considerations of non-obviousness. In that context, the patentee argues an invention would not have been obvious in view of these considerations, which include: (a) commercial success of a product due to the merits of the claimed invention; (b) a long-felt, but unsatisfied need for the invention; (c) failure of others to find the

solution provided by the claimed invention; (d) deliberate copying of the invention by others; (e) unexpected results achieved by the invention; (f) praise of the invention by others skilled in the art; (g) lack of independent simultaneous invention within a comparatively short space of time; (h) teaching away from the invention in the prior art.

30. I further understand that secondary considerations evidence is only relevant if the offering party establishes a connection, or nexus, between the evidence and the claimed invention. The nexus cannot be to prior art features. The establishment of a nexus is a question of fact.

IV. LEVEL OF SKILL IN THE ART

31. I understand that the claims of a patent are judged from the perspective of a hypothetical Person of Ordinary Skill in the Art ("POSITA") at the time the claimed invention of the patent was made. The "art" is the field of technology to which the patent is related. I understand that the purpose of using the view point of a POSITA is for objectivity.

32. In my opinion, the POSITA must generally be capable of understanding the general computer systems principles that are applicable to the pertinent art. I understand that the factors to be considered in determining the level of ordinary skill in the art to be: (1) the educational level of active workers in the field, including the named inventors of the patent; (2) the type of problems encountered in the art; (3)

prior art solutions to those problems; (4) the rapidity with which innovations are made; and (5) the sophistication of the technology in the art.

33. In my opinion, a POSITA for the '757 and '421 patents at the relevant time would have a bachelor's degree in computer science, electrical engineering, or a related technology field, and at least two years of experience in a field related to location-based services or mobile applications, or equivalent experience. Alternatively, a POSITA in the relevant timeframe would have an advanced degree, such as a master's degree, in computer science, electrical engineering, or a related technology field, and at least one year of experience related to location-based services or mobile applications, or a related technology field, such as security monitoring. A person with less education but more relevant practical experience, or more relevant education but less practical experience, may also qualify as a POSITA. Each of the factors that I outlined above supports this formulation.

34. Based on my education, training, and professional experience in the field of the claimed invention, I am familiar with the level and abilities of a POSITA at the time of the claimed invention. Additionally, I was a POSITA as of the time of the claimed invention.

V. TECHNOLOGICAL BACKGROUND

35. Prior to the March 5, 2019 priority date of the Asserted Patents, all the technology at issue was broadly applied and well known by developers in the

wireless/mobile communications industry, including in the wireless Location-Based Services field. In my opinion, no individual elements of the claims of the Asserted Patents were novel at the time of the alleged invention, and there was nothing novel or inventive about the manner in which those elements were combined in the claims. Further, there were no technological barriers to combining these elements to form the claimed invention. Indeed, combining these elements would have yielded predictable results.

36. Specifically, the advent of and developments related to the use of geofences and location sharing in supervisory-related location-based services demonstrate that the elements described and claimed in the Asserted Patents, including the use of grids and generation of alerts were well-known before the actual respective filing dates of the Asserted Patents. Indeed, even the alleged point of novelty of the Asserted Patents comprising the grid box limitations was well-known.

A. Location Technologies, driven by The 1996 Telecommunications Act, were utilized for a wide variety of commercial Location-Based Services (LBS) starting in the early 2000s.

37. The modern Location-Based Services (LBS) industry in the United States was triggered by the 1996 Telecommunications Act, which resulted in a mandate requiring wireless carriers and Public Safety Answering Points (PSAPs) to provide the location of a wireless caller who dialed 911, referred to as Enhanced 911 or E911. The mandate established accuracy and penetration deadlines met through a

two-phased approach, first using the serving cell tower and sector as a proxy for the caller's location, and then determining the caller's location more precisely using either Global Positioning System (GPS) or network Time Difference of Arrival (TDOA) techniques.

38. Either kind of technology, though varying in accuracy, could theoretically enable reasonably accurate commercial location applications, including geofences. In fact, in a number of these early carrier commercial LBS planning efforts, geofencing was examined for its potential applicability. For example, Nextel in the late 1990s assessed the potential and feasibility of its use in various potential Mobile Resource Management (MRM) applications for tracking and managing workers and assets, which among various supervisor functions extensively relied on location data sharing between workers and supervisors.[1]

39. LBS in the United States began to take off in 2003-2005, with the launch of Nextel's worker tracking product in 2003 (*see* Ex.1030) and Mobile Locator search app in 2004 (*see* Ex.1031), and a variety of LBS applications by Sprint starting in 2005-2006, such as its Family Locator. *See* Ex.1032.

[1]I was personally involved with Nextel in planning for LBS in the 1998-2000 timeframe. Ex.1006, 4.

B. Sharing of Location Information with others, including supervisors/supervisor-type roles, has been well-known since well before the patent priority date

40. The sharing of location information between users and devices was a major functional element of many LBS applications, including sharing a caller's location with PSAP dispatchers, a child's location with a parent, and a worker's location with a supervisor. Accordingly, there is substantial prior art relating to location sharing dating from at least the year 2000. *See e.g.,* Ex.1027 (U.S. Patent No. 6,618,593), and Ex.1028 (U.S. Patent No. 8,103,729).

41. Because these applications monitored one person on behalf of another, they required the supervising user to configure the terms of the monitoring relationship before any monitoring occurred. A POSITA would have understood that configuration to comprise a set of related parameters: which individuals or devices are monitored, which geographic boundaries apply, which conditions or thresholds constitute a reportable event, who receives the resulting report, and through what channel(s). Permission and access-rights settings were one component of that configuration set, but they were not the whole of it. The parameters that determined when an alert would fire (trigger), and what the system would do in response, were equally part of the security configuration of the monitoring system, because they determined whether and how the monitored person was in fact supervised.

42. In my opinion, a POSITA before March 5, 2019 would have understood the configuration values that govern security-related monitoring of a person within a geographic boundary, including zone properties, restricted-area or off-limits flags, speed or distance thresholds, danger or threat designations, boundary-entry and boundary-exit event rules, scheduled or periodic reporting rules, and lists of words or conditions that escalate a message into a security event, to be examples of security parameters of the monitoring system. Those values are what distinguish a system that merely records location from a system that supervises a person, and a POSITA designing such a system would have expected the supervising user to supply them.

43. Contemporaneous location-sharing art also recited supervisor-selected alert thresholds alongside access permissions. For example, U.S. Patent No. 6,714,791, titled *System, Apparatus and Method for Location-Based Instant Messaging*, with a priority date of February 23, 2001, describes buddy-list functionality in which "[t]he creator of the buddy list 1100 may also set alert levels specifying a range of user locations within which an alert should be generated." Ex.1017, 13:62-64. The alert level is significant because it is not an access permission at all; it is a supervisor-selected threshold that determines when the system generates an alert.

44. Thus, by March 5, 2019, the sharing of location information between a supervising user and a monitored user was not merely known but ubiquitous, and so

was the practice of having the supervising user configure the terms of that monitoring in advance. A POSITA would have expected any supervision-oriented location service to receive, from the supervisor, both the geographic area of interest and the parameters controlling what is treated as a reportable security event within it.

C. The use of commercial location boundary-related capabilities and applications began at least by the year 2000, with related concepts beginning much earlier.

45. https://jornada.nmsu.edu/files/bibliography/07-018.pdfhttps://en.wikipedia.org/wiki/GeofenceThe explicit use of a virtual boundary, as well as bounding box language and map grid coordinates, appeared around the year 2000 with U.S. Patent No. 6,353,390 (Beri et al.), filed December 31, 1999 (issued March 2002), titled "Method and System of Configuring a Boundary and Tracking an Object Thereby." The invention included user-defined virtual boundaries (also called "bounding boxes"), inputs including map grid coordinates, and object tracking against that boundary over a wireless network. Ex.1018.

46. Unsurprisingly, given the 1996 Telecommunications Act driving E911 design and implementation (along with tight implementation timetables), techniques for creating "virtual perimeters" and determining a device's location relative to those boundaries were well known in Public Safety applications shortly after the 1996 Act.

Indeed, Public Safety entities were very aware of issues related to geospatial boundaries and public safety, particularly with respect to PSAP boundaries/jurisdictions, which determined how 911 calls were routed to get to the best (*e.g.*, closest) PSAP to handle the emergency. For example, in a 2002 industry whitepaper titled "*A Public Safety Answering Point Managers' Guide to GIS*," the guide stated:

> Another often-overlooked aspect of GIS data is that you need to extend the data past your area of jurisdiction. You need to have a "buffer area" of several miles around the PSAP boundary. Wireless cell calls may come into the PSAPs from outside your boundary.

Ex.1020, 11.

47. The actual term "geo-fencing" in a mobile-device patent appeared around this time, with U.S. Patent No. 6,721,652 (Sanqunetti), filed November 22, 2002 (issued April 2004), "Implementing Geo-Fencing on Mobile Devices." Predefined geo-fencing boundaries were used in a coordinate system with overlapping rectangular boundaries. Ex.1019.

48. Additionally, boundary-crossing detection coupled to notification was expressly claimed well known in the art. U.S. Patent No. 7,133,685 ("the '685

Patent"), titled Monitoring Boundary Crossings in a Wireless Network, describes in its abstract:

> A method of providing location-based services for a mobile unit operating in a wireless network including network structures. The method includes receiving an identifier associated with the mobile unit. The method also includes monitoring a location of the mobile unit using the identifier and a network-assisted location finding system to identify a crossing of a service zone boundary by the mobile unit. The service zone boundary is defined by reference to at least one of the network structures. The service zone boundary also corresponds to a geographic zone boundary. The method further includes transmitting service information to a system user in response to the crossing of the service zone boundary.

Ex.1021 [Abstract].

49. As another example, 2004 U.S. Patent No. 7,164,986 ("the '986 Patent"), titled Method and system for tracked device location and route adherence via geofencing, described the following in its Abstract (emphasis added):

> A device tracking location adherence and route adherence technology, is disclosed that at least provides a tracked device receiving, a set of coordinates associated with a boundary area, and obtaining a position of the tracked device. Based upon the received coordinates and the detected position of the tracked device, a determination is made as to whether the tracked device is located inside the boundary area or outside the boundary area. An alert signal is then generated and transmitted if the result of the determining is different from an immediately previous obtained result. The system allows, for example, drastic reduction in the amount of data traffic required within a system since the tracked device performs much of the necessary processing. This is especially advantageous where a fleet of tracked devices are employed within a network.

Ex.1022 [Abstract].

50. As of the priority date, geofencing was a well-understood location-service concept. U.S. Patent Application No. 2014/0155094 A1 ("Zises") explains that "A geofence can be defined as a perimeter or boundary around a physical

location or mobile object," that it "can be as simple as a radius around a physical location defining a circular region," and that it "can be any geometric shape or an arbitrary boundary drawn on a map." Ex.1014, ¶¶[0042]-[0043], [0054]. Zises further describes a location module that receives GPS-type coordinates, including longitude and latitude, and determines whether a current location is within a parent geofence. *Id.* A POSITA therefore understood that a geofence could be represented by a radius, an arbitrary mapped boundary, or coordinate data, and that containment was determined by evaluating a reported coordinate against that representation.

51. Zises also describes a plurality of geofences in which "each Best Buy store location[] would be covered by a much smaller child geofence" within a larger collection of geographically related locations, so that nesting smaller regions inside a larger region was a routine way to obtain more localized results. Ex.1014, ¶[0033]. Nesting a smaller geofence inside a larger one is distinct from subdividing a single geofence into a grid of cells that together make up the whole enclosed area, and I address grid-based subdivision separately below.

52. The means for fixing a device's position and for detecting boundary events were likewise familiar. U.S. Patent Application No. 2016/0358432 A1 ("Branscomb") describes a location-aware device determining location through "GPS, iBeacon, WiFi and etc." and a fence-delivery network that converts between geographic coordinates and geofence information. Branscomb further describes

"automatic notification of geofence identification" including "the standard notification of approach, enter, exit, and dwell." The technical significance is that a device's position is compared with a stored boundary and a notice or other configured response is produced when the positional status changes. Ex.1015, ¶¶[0077], [0151].

53. Geofences and their underlying technical aspects, including the generation of alerts and notifications based on a device's position relative to a boundary, were therefore well known throughout the industry well before the priority date of the Asserted Patents.

D. The use of grids in Location-Based Services and Geofences was also well known prior to the patent priority date.

54. When a grid is applied to a geographic area, each cell can be georeferenced, meaning that the cell is associated with a defined extent of real-world area expressed in the same coordinate frame as the position fixes the system will evaluate. A POSITA would have understood that a system cannot determine which cell contains a reported coordinate unless it knows the geographic extent that each cell occupies.

55. Prior-art systems in this field made the granularity of grids user-selectable. U.S. Patent No. 7,317,927 ("Staton") states: "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 the resolution of the area." Ex.1007, 15:46-55. U.S. Patent No. 7,881,733 ("Staton '733") contains the same disclosure. Ex.1013, 13:60-14:8.

56. The reason a POSITA would have made resolution selectable rather than fixed is that a single system may be asked to monitor areas differing enormously in physical size and in the precision the application requires. Staton gives the illustration directly, explaining that an increased resolution allows a user to define the geographical area of a house, whose perimeter has detail identifiable only at very high resolution, while a user concerned only with roughly knowing that a state has been entered does not need great resolution and may configure the resolution for that area to be low. Ex.1007, 15:52-59; Ex.1013, 14:1-14. A POSITA would have recognized this as the ordinary engineering tradeoff between spatial precision on the one hand and storage, index size, and per-fix computation on the other.

57. Standardized military and civilian grid reference systems also assign an alphanumeric identifier to each cell of a progressively subdivided geographic surface, so that a position can be reported either as a coordinate pair or as the identifier of the cell containing it, with the length of the identifier expressing the

resolution. Rauner reflects the ordinary availability of such systems, disclosing that GPS or location-coordinate information may be translated into Military Grid Reference System (MGRS) form and that the resulting coordinate and MGRS information can be stored in user profiles in a database. Ex.1009 ¶[0068]. Hierarchical grid addressing schemes of the same general character existed in the commercial art from the mid-1990s. *See, e.g.*, U.S. Patent No. 5,839,088 (Ex.1025); U.S. Patent No. 6,339,744 (Ex.1026).

58. Regular spatial tessellation, the dividing of Euclidean space into regions that fully cover the area with no gaps or overlaps, has been a basic engineering tool in wireless communications since the cellular concept was formulated, and a POSITA in this field would have been thoroughly familiar with dividing a geographic area into a regular array of adjacent cells. U.S. Patent No. 9,510,141 (filed March 2013) is an example of the use of this concept in location-based applications. Ex.1033.

59. http://www.google.com/patents/US6339744Explicit grid-based geofence systems in patents included Samsung SDS U.S. Patent No. 10,257,644 (filed May 2016), in which an area was stored as one or more grids and membership in those grids was determined using truncated coordinates. Ex.1023. IBM U.S. Patent No. 9,747,380 divided a map into grid elements, hashed device locations into cells, and tested which cells overlapped a geofence. Ex.1024.

60. Staton, which I address in detail below, describes the use of grids with geofences:

> In another aspect, the data representative of each geographical zone is a pixilated image. The pixilated image can be created by the steps of allowing a user to identify a geometrical zone in a computer map using two coordinate attributes, 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, and associating the at least one section to a pixel in a pixilated computer image such that the pixels selected by the user in the identified geometrical area are identified as being in the geographical zone. The grid can divided into a number of sections so as to achieve a high enough resolution to be able to correctly delineate the geographical zone.

Ex.1007, 3:5-17.

61. Staton thus describes the grid, the selection of sections within it, the association of each section with a pixel, and the division of the grid into a number of sections sufficient to achieve the resolution needed to delineate the zone.

62. By 2016-2018, geofence-related systems also used grid-based spatial partitioning with configurable sizing. U.S. Patent Application No. 2018/0075108 A1 ("Park") describes a "geo-partitioner" based on a grid approach, a dynamic grid generated from spatial clustering, and a decision about grid range implemented by "a configuration parameter, a grid size, a grid size effect factor, and the number of geometries." Ex.1016, ¶¶[0082]-[0083], [0088]. Park further explains that a bounding box may be divided by an adjusted grid size to create new partitions or additional partitions. *Id.* This is evidence that a POSITA working with geospatial event data understood grid size and related parameters as ordinary controls on spatial partitioning.

63. U.S. Patent Application No. 2017/0287006 ("Azmoodeh") describes the same operation directly in a geofencing context. It states that the geofence module "divides the region encompassed by the geo-fence into a set of cells," with each cell representing a portion of the region, and that "the number of cells within the region may be defined based on a size of the geo-fence, or based on user input." Ex.1010, ¶[0046]. The disclosure therefore teaches both subdivision of a bounded geographic region and user control over the resulting spatial resolution.

64. Azmoodeh's system defines a geofence from geolocation data and then divides the enclosed region into cells; the later collection of usage data and adjustment of the boundary are separate downstream operations. Because the

subdivision operates on the coordinates and geometry of the enclosed region, it does not depend on whether the cell-level information is later used for advertising, safety monitoring, or another specific purpose. Ex.1010, ¶¶[0015]-[0018], [0043]-[0049].

65. As of March 5, 2019, a POSITA would have understood that subdividing a geofenced area into cells, and allowing the number or the size of those cells to be selected, were well-known design techniques. The arithmetic relationship between the two quantities is elementary. Over a bounded region of fixed total area, the area of each cell equals the total area divided by the number of cells, so specifying either quantity necessarily determines the other. A system that accepts a cell count as its input computes the corresponding per-cell area in order to lay out the grid, and a system that accepts a cell size as its input computes the corresponding number of cells in order to cover the region. Increasing the number of cells decreases the area each cell covers, and decreasing the number of cells increases it. Ex.1016, ¶¶[0082]-[0084]; Ex.1010, ¶[0046]; Ex.1007, 15:46-55.

66. Before March 5, 2019, a POSITA would have regarded the receipt of a resolution input, the determination of the area represented by each resulting cell, and the generation of the corresponding number of cells as the ordinary sequence by which a configurable georeferenced grid is constructed. A POSITA implementing a configurable grid over a geofence before March 5, 2019 would have performed these operations as a matter of routine engineering.

67. Finally, a POSITA would have understood that applying alert generation at the level of an individual grid cell required no new technical concept. As described in subsection C, geofencing systems already generated an alert when a device's position status relative to a stored boundary changed. The same comparison of a reported coordinate against a stored boundary therefore operates identically at the perimeter of a geofence and at the perimeter of a cell within it, and a POSITA would have understood the choice between them to be a choice of granularity rather than of technique.

E. Architecture enabling geofences has varied from server-based systems to device-based systems to hybrids, varying as needed by available resources and use case specifics as well as technology advancements.

68. The architecture of geofencing systems, meaning where the boundary catalog is held, where the enter-or-exit comparison is computed, and which radio supplies the position fix could be server-centric, device-centric, or hybrids of the two.

1. Server-based

69. This architecture relied on a server for primary processing, with the device being primarily utilized for location determination and display. The device would determine or calculate a latitude/longitude, such as GPS, then send it to geofencing-related functionality operating on a central server. The server would then compare the latitude/longitude to stored zones, including circles and polygons or

bounding boxes, and perform comparison calculations, along with rule-based generation of alerts, notifications, and/or commands. The geofence parameters were stored only on the server.

70. A POSITA also understood that geofence information and event processing could be maintained on network infrastructure. Branscomb describes "a server including a processor" and "a geofence database," with a search engine that identifies geofences whose geographic areas overlap a coordinate point. It further explains that geofence boundaries may be published through a fence-delivery network and stored in cellular towers or WiFi access points. Ex.1015, ¶¶[0028], [0020]-[0021]. These disclosures show that storing fence data in server-side or distributed infrastructure for lookup was a known implementation.

71. Zises provides the same client-server background. It describes a "network-based system" with mobile devices, servers, databases, a location-based service application, and a geofence-paging application. It also states that the system may use a client-server architecture and that servers may execute location-based services that interoperate with software on the mobile device. Ex.1014, ¶¶[0033]-[0039], [0043]-[0047]. A POSITA therefore understood that a system could divide location acquisition, geofence storage, and boundary evaluation between a client and one or more servers without changing the underlying geofencing operation.

72. Early implementations, such as Sprint geofencing services, were server-intensive because devices had relatively little processing power and no always-on operating-system location services. Accuracy limitations, particularly before Selective Availability was removed in 2000 (greatly improving the accuracy of GPS-based location systems), also meant that early areas and geofences tended to be large. U.S. Patent No. 6,353,390 (Ex.1018) and U.S. Patent No. 6,721,652 (Ex.1019) likewise assume a network plus a central monitor.

2. Device-based

73. As mobile devices became more capable, particularly following the introduction of the iPhone in 2007 and Android devices in 2008, the evaluation of a device's position against a stored boundary also increasingly was also performed on the device itself. Mobile operating systems and application frameworks came to provide region-monitoring and geofencing interfaces that allowed an application to register a bounded region and to receive enter, exit, and dwell events computed locally, using position fixes fused from GPS, Wi-Fi, and cellular sources.

3. Hybrids

74. Systems also divided the work. An exemplary division performed coarse proximity detection on the device and reserved precise boundary determination for the server, which held the full catalog of zones and evaluated the more complex rules such as dwell conditions and multi-asset logic. A related

division tiered the positioning method itself, using low-power network-based position estimates when a device was far from any boundary and progressively more precise methods as it approached one.

75. Across all three of these architectures, the underlying computation did not change. A geofencing system may obtain a position fix, hold a representation of the boundary, compare the fix against the boundary, and act on the result under a set of rules. A POSITA would therefore have regarded the allocation of the boundary comparison between the client device and the server as an implementation choice rather than a technical constraint, because both arrangements operate on the same two inputs: the reported coordinate and the stored boundary representation. Zises describes a location module that receives location data from a mobile device and determines whether the current location falls within a parent geofence, while Branscomb describes a server querying a geofence database to identify the fences associated with a coordinate point. Ex.1014, ¶[0054]; Ex.1015, ¶¶[0028], [0055]-[0056].

76. A POSITA choosing between those arrangements would have weighed a familiar set of considerations. Server-side comparison was indicated where the position data was already being reported to the server for routing, storage, or notification purposes, because the comparison then consumed an input already present at the point where the notification decision was made. It was also indicated

where the server already maintained the authoritative boundary representation, since the boundary could be changed centrally without reconfiguring devices. It offered a reliability benefit, because an independently computed server-side result could cross-check a device-side determination that was erroneous or that failed to be reported. It accommodated monitoring interfaces and client devices that lacked the processing capacity or memory to evaluate a boundary or pixel map themselves, allowing each such interface to receive a completed result rather than duplicating the calculation. And it conserved energy on the monitored device, because repeatedly comparing successive position fixes against a boundary is a recurring computation on a battery-powered device, whereas server infrastructure is continuously powered.

77. Device-side comparison was correspondingly indicated where continuous reporting of position fixes would have imposed unacceptable network or power cost, or where the system needed to detect a crossing while disconnected. A POSITA in this field would have selected between the two, or divided the work between them, on those ordinary grounds. The ’757 Patent itself reflects the same understanding, stating that one or more steps of the disclosed method may be performed by a server computer and that one or more steps may likewise be performed by a client computer, and separately that the server may be configured to analyze the location data. Ex.1001, 9:60-62, 6:56-59, 26:40-41.

F. Message handling, event processing, and data storage were conventionally implemented as cooperating software components on shared server infrastructure.

78. A further aspect of that architectural practice concerns how the server side of such a system was internally organized. A POSITA building a supervisory location or emergency-response platform before March 5, 2019 would not have built three physically distinct machines to handle communications, processing, and storage. The conventional practice was to implement each of those functions as one or more software components, together with their associated databases, running on shared server infrastructure, and to describe them functionally by the role each played rather than by any distinct hardware identity. Staton, for example, describes its backend control system as an integrated arrangement of gateways, a codec, an asynchronous routing system, routing services, databases, networks, and a web server on the communication side; an operations data processor, configuration utility, and routers on the processing side; and a history recorder, history queue, history database, real-time database, and resources database on the storage side. Ex.1007, 6:66-7:23, 7:30-33, 19:50-20:3. Rauner likewise describes an emergency response computer system comprising a processing unit, an emergency response module containing device communications, processing, response, notification, determination, administration, and mapping modules, and a storage device, and

states expressly that a single server can include those modules. Ex.1009 ¶¶[0053]-[0054], [0097].

79. In my opinion, a POSITA reading such descriptions would have understood the communication, processing, and storage functions to be roles performed by software components and databases within one server environment, and would have understood the assignment of a given function to one component rather than another to be an ordinary matter of software organization.

G. The use of many of the above capabilities was well-known in a variety of industries prior to the Asserted Patents, with various use cases involving specific types and organizations of geofences, grids, and underlying map data.

80. As discussed in subsection C, supervisor configuration of the monitoring terms was a standard element of supervisory location services, and the configuration set routinely included boundary designations, thresholds, and event rules as well as access permissions. The boundary-designation art discussed in subsection C is equally settled, *e.g.*, the Beri patent, with its user-defined bounding boxes configured from map grid coordinates, and the Sanqunetti patent, which used predefined geo-fencing boundaries in a coordinate system. The server-side operations come next: generating the geofence, evaluating supervisee position against it, and issuing a notification. Branscomb and Zises, discussed in subsection E, disclose that arrangement directly, and the ’685 and ’986 Patents discussed in

subsection C disclose the notification that follows from a change in a device's position status relative to a stored boundary.

81. As discussed in subsection D, Staton divides a supervisor-selected area into a grid of smaller rectangles, maps each to a pixel, assigns a geographical area to each pixel, and makes the resolution of that subdivision user-selectable, so that increasing the resolution increases the number of rectangles and decreases the area each covers. Azmoodeh discloses the same subdivision, with the number of cells defined by the size of the geo-fence or by user input, and Park, the Samsung SDS patent, and the IBM patent each describe the same configurable partitioning of a bounded area into georeferenced cells.

82. Finally, as to finer localization, U.S. Patent No. 10,085,117 ("Smith") describes a virtual boundary in three-dimensional space defined by lateral position parameters together with an altitude parameter and explains that altitude-based geofencing can determine whether a user is on a particular floor of a multistory structure. Ex.1011 (Smith). A POSITA would have understood facility plans and building schematics to be the ordinary representation of a position within a structure, and a boundary defined by a building's footprint to be a geofence.

83. Thus, a coordinate overlay places a reference grid across a map so that positions can be labeled and correlated, as Rauner's alphanumeric grid does. Ex.1009 ¶[0094]. For nesting places, a smaller, separately defined boundary is

placed inside a larger one, as Zises describes. Ex.1014 ¶[0033]. Further, structural subdivisions may partition a single bounded area into a set of cells that together make up the whole of that area, each cell carrying its own portion of the area, as Staton, Azmoodeh, and the Samsung SDS and IBM patents describe. These techniques were well known before March 5, 2019, and a POSITA would have understood which was called for by a given design objective.

84. Taken together, not only was each of these capabilities well known before the March 5, 2019 priority date, each had been known and in commercial use for many years before that date, in most instances since the early 2000s or earlier.

VI. THE CHALLENGED PATENTS

A. '757 PATENT

1. Priority

85. The '757 Patent issued on October 11, 2022, from U.S. Application No. 16/810,703, filed March 5, 2020. Ex.1001, cover. The application claims the benefit of Provisional Application No. 62/814,097, filed March 5, 2019. Ex.1002, 30, 70. I have assumed, without conceding, that the challenged claims are entitled to the March 5, 2019 date, and I have applied that date in assessing the prior art and the knowledge of a POSITA.

2. Overview of the '757 Patent

86. The '757 Patent states that a geofence is "a virtual perimeter for a real-world geographical area that is widely used in location-based services." It further

explains that geofences can be "predefined boundaries (such as school zones and/or neighborhood boundaries)" that allow an individual to trigger an alert to multiple users when the individual enters or exits the geofence. These statements describe the same basic virtual-boundary concept discussed in Section V. Ex.1001, 1:13-21.

87. The patent identifies a purported deficiency in "conventional geofencing applications," which "do not allow easy access for a user to create the geofence." Ex.100, 1:22-23. It also identifies examples of factors such as criminal activity and crowd density that, according to the patent, conventional applications did not permit a user to use when creating a geofence. Thus, the asserted problem is ease and flexibility of geofence creation rather than a new kind of geographic boundary. Ex.1001, 1:21-30.

88. The disclosed architecture is described functionally. The communication device receives a parameter and a geographical location from a supervisor device. The processing device analyzes the geographical location based on a security parameter and generates a geofence corresponding to a geographical area. Ex.1001, 11:38-63. The processing device then analyzes supervisee data based on the geofence and generates a supervision-related notification, while the communication device transmits that notification to the supervisor device. *Id.,* 12:1-14.

89. The specification uses generic server terminology for those functions. It states that a server computer may include a processing device for "analyzing, identifying, determining, generating, transforming, calculating, computing" and other ordinary data-processing tasks, a communication device for communicating with external devices, and a storage device for data storage and retrieval. A POSITA would read this passage as describing ordinary server-side software functions and data handling, not specialized hardware architecture. Ex.1001, 6:56-7:10; Ex.1002, 208-209.

90. The patent's parent-child example illustrates the intended use. It describes a supervisor parent receiving a notification when a supervisee child reaches a geofence. Ex.1001, 18:6-23. It also depicts geofence creation using a name, a location, and a radius, with the location selectable on a map by a "drop pin" operation. Those are conventional geofence inputs of the type discussed in Section V. *Id*., 18:52-19:6, Fig. 23.

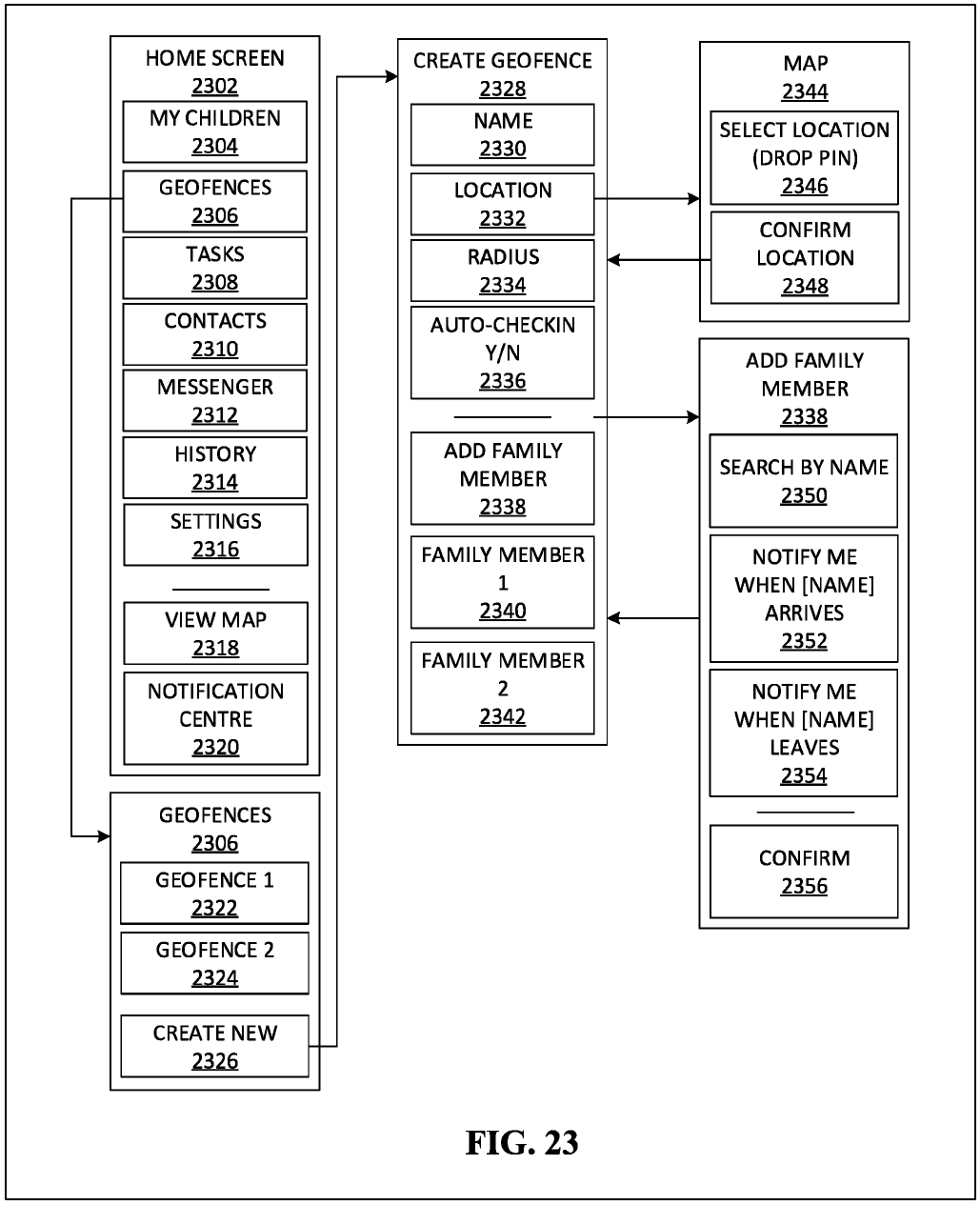


FIG. 23

Ex.1001, Fig. 23.

91. The patent separately describes a grid-based geofence. It states that the geofence may comprise "a plurality of geofence grid boxes associated with the geofence area" and that each grid box is characterized by "a grid box geofence area of the geofence area." Ex.1001, 13:8-22. It further states that the communication

device receives one or more grid parameters from the supervisor device and that the processing device analyzes the parameters, determines the grid-box area, and generates a number of grid boxes. Ex.1001, 13:8-22; see also Fig. 5 and 14:30-45.

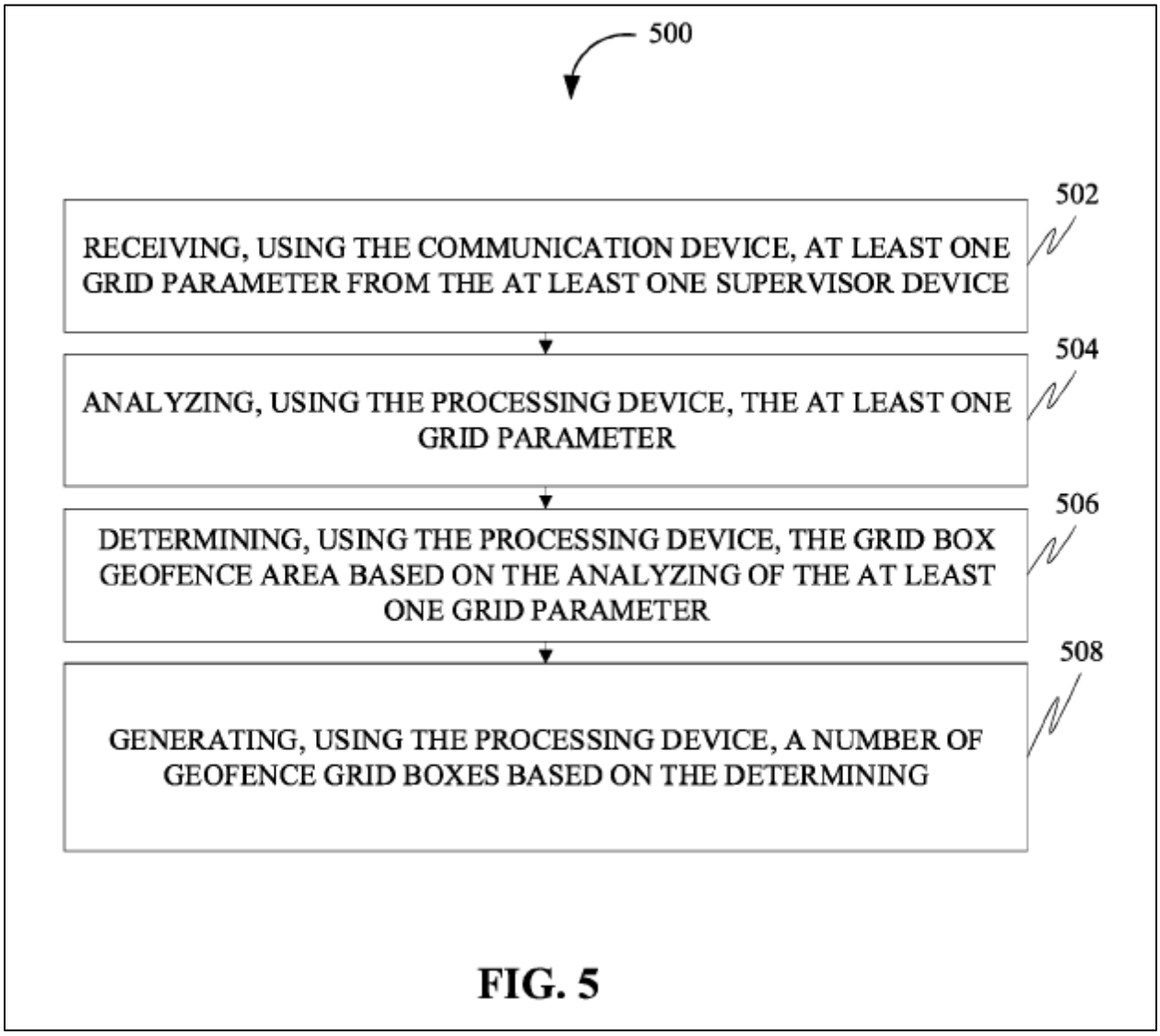


FIG. 5

Ex.1001, Fig. 5.

92. The specification, however, does not identify what quantity the grid parameter expresses. Ex.1001, 13:8-22. It does not state whether the parameter is a cell count, a length, an area, a resolution value, or another quantity; it does not

identify units or an encoding; it does not specify a communication format or interface by which the parameter arrives from the supervisor device; and it does not disclose an algorithm that converts the parameter into a grid-box area or a number of boxes. Ex.1001, 14:30-45. The specification names the parameter and recites analyzing it, but leaves those implementation details unstated. *Id*., Fig. 5. It does not specify whether such grids are uniform, non-uniform, or hybrid. Figure 5, the only figure describing the geofence grid boxes, largely repeats the claim language rather than disclosing any implementation: its boxes recite receiving a grid parameter, analyzing the grid parameter, determining the grid box geofence area, and generating a number of geofence grid boxes, in substantially the same terms used by the claims. Ex.1001, Fig. 5, 13:62-14:6.

93. During prosecution, the Examiner's analysis treated the geofencing prior art as disclosing the supervision system and its ordinary receiving, processing, storage, and notification functions, but identified the grid-box subject matter as the missing feature. The Examiner's statement records that "Claim 19 (now incorporated in claim 11 as amended) is allowable," and the Examiner's amendment added the claim 19 grid-box limitations to the independent claims. Ex.1002, 219-221, 257-259.

94. The reasons for allowance state that the prior art disclosed the supervision system but that "the prior art references do not teach" the claimed

geofence grid boxes, grid-box area, receipt and analysis of a grid parameter, and generation of a number of grid boxes. Ex.1002, 222-223. The Examiner then allowed the other claims because they included subject matter the same as or similar in scope to the allowable claim. In my opinion, that technical conclusion was incorrect. I explain why in Ground 1's Staton's comparison and in the Ground 3 Rauner-Azmoodeh analysis, rather than repeating those analyses here. Ex.1002, 222-224, 260-262; Section IX, Ground 1; Section IX, Ground 3.

95. The later reissue history is also relevant to the procedural record. Reissue Application No. 18/648,671 was filed on April 29, 2024 to address alleged errors in claims 9 and 18. Ex.1012, 46-48, 63-65. The Examiner issued an Office Action rejecting claims 1-18 on June 4, 2026. *Id.*, 23-35. The applicant filed an express abandonment on September 23, 2026. *Id.*, 8-9.

B. '421 Patent

1. Priority

96. The '421 Patent issued on November 26, 2024, from U.S. Application No. 18/045,781, filed October 11, 2022. Ex.1003, cover. It is a continuation-in-part of U.S. Application No. 16/810,703, filed March 5, 2020, which issued as the '757 Patent (Ex.1001), and it also claims the benefit of Provisional Application No. 62/814,097, filed March 5, 2019. Ex.1003, cover.

97. I have assumed, without conceding, that the challenged claims are entitled to the March 5, 2019 date, and I have applied that date in assessing the prior art and the knowledge of a POSITA, exactly as I did for the ’757 Patent. My opinion as to the level of ordinary skill in the art is unchanged.

2. Overview of the ’421 Patent

98. The ’421 Patent largely carries forward the ’757 disclosure, and figures. I therefore incorporate my overview of that shared disclosure from Section [VI.A.2] rather than repeating it, and the observations I made there apply equally to the ’421 Patent. Ex.1003.

99. Relative to the ’757 Patent, the ’421 Patent adds claimed subject matter related to: altitude and building-floor limitations; the supervisee-initiated shake, button, or phrase signal with a geofence-determined emergency number; the per-grid-box stored emergency contact number; and the audio/video, proximity-based sensor-selection, and sensor-handoff features.

100. In the February 1, 2024 Office Action, the Examiner interpreted the “communication device,” “processing device,” and “storage device” limitations under 35 U.S.C. § 112(f), reasoning that “device” is a generic placeholder coupled with functional language without sufficient structure, and that neither “device” nor “unit” is established to represent a proper structure.

101. The Examiner rejected claims 11-25 under § 112(b) because the written description "fails to disclose the corresponding structure, material, or acts for performing the entire claimed function and to clearly link the structure, material, or acts to the function." Applicant agreed that § 112(f) applies and identified the corresponding structure as "standalone functions existing inside of the server computer," in most embodiments "simple programs and databases," and "programs running on a server computer and not standalone devices of any unique structure." Applicant explained that the communication device handles messaging between the server computer and external devices, the processing device receives data from the communication device, and the processing device stores processed data on the storage device. Ex.1004.

102. The Examiner rejected claims 1-8, 10-18, and 20 for nonstatutory double patenting over claims 1-18 of the '757 Patent. Claim 21 was separately rejected over '757 claim 1 in view of Stevenson, U.S. Publication No. 2011/0227730. Applicant filed a terminal disclaimer on June 27, 2024. Ex.1004.The Notice of Allowance issued July 12, 2024, and a Corrected Notice issued August 5, 2024, allowing claims 1-22 and 24-25 after claim 23 was cancelled.

VII. CLAIM CONSTRUCTION

103. I understand that claim terms are given the ordinary and customary meaning they would have to a POSITA in light of the specification and the

prosecution history, under the same standard used by district courts. Because the specifications are largely the same for both patents, the claim terms discussed below apply equally to both the ’757 and ’421 patents.

104. “Geofence.” A POSITA would have understood “geofence,” which appears in all challenged claims, to encompass the virtual geographic boundary as well as associated settings or parameters that trigger an alert upon entry or exit. This construction reflects how the patent and the technical literature use the term: the boundary is the spatial component, while the associated settings determine how the system recognizes and responds to a location event.

105. The intrinsic evidence supports that construction. The specification defines a geofence as “a virtual perimeter for a real-world geographical area” and explains that predefined boundaries can allow an individual to trigger an alert when entering or exiting. The definition is therefore functional, not limited to an abstract line on a map. A boundary by itself does not identify the triggering condition, the event response, or the intended recipient; those functions depend on the settings associated with the boundary. Ex.1001, 1:13-21.

106. The specification also treats configuration inputs as part of the created geofence rather than as unrelated information. Its geofence-creation interface includes a name, a location, and a radius, and the location may include a map with “drop pin” selection. The patent separately describes notification choices for when

a named family member arrives at or leaves the location. These passages show that the patent's geofence is created and used together with settings that define its operational behavior. Ex.1001, 18:52-19:6; Ex.1001, Fig. 23; Ex.1001, 18:6-23.

107. The POSITA understanding is also consistent with the prior art. For example, Branscomb explains that a geofence database includes information associated with a geofence, such as "the owner of the geofence," licensees, a class, and other information, and that the system stores rules and entitlements associated with geofences. It further describes devices receiving metadata and responding according to the geofence's classes and entitlements. Thus, in the relevant art, "geofence" could refer to the boundary together with the rule set and metadata that determine what occurs when a device approaches, enters, exits, or dwells within it. Ex.1015, ¶¶[0043], [0058]-[0064], [0081].

108. Accordingly, I apply "geofence" to include the virtual geographic boundary and the associated settings or parameters that give the boundary operational meaning, including the rules or zone properties used to trigger and direct an alert. This interpretation is consistent with the specification, the prosecution history, and the way a POSITA would have understood the term, and I apply it consistently throughout my analysis.

109. Section 112(f) terms. I have been informed that, during prosecution, the Applicant agreed that §112(f) applies to the "communication device," "processing

device," and "storage device" limitations wherever those terms appear in the challenged claims, because they use a generic placeholder, "device", coupled with functional language without reciting sufficient structure. Ex.1002, 208-209. The Applicant identified the corresponding structure as functions or programs inside a server computer rather than independent hardware devices. Ex.1002, 208-209.

110. For the communication device, the Applicant identified a program or database inside a server computer that "handles messages between the server computer and external devices." *Id.*, 209. For the processing device, the Applicant identified a program inside the server computer that "receives data from the communication device" and stores processed data on the storage device. *Id.* For the storage device, the Applicant identified a program or database inside the server computer that stores the data. *Id.*

111. The '421 file history also states that the structures are "standalone functions existing inside of the server computer," generally "simple programs and databases," and "programs running on a server computer and not standalone devices of any unique structure." Ex.1004, 207-208. The '757 specification likewise describes ordinary server processing, communication, and storage functions. Ex.1001, 8:44-9:10.

112. I apply these §112(f) constructions consistently in every ground addressed below, for both the '757 and the '421 Patents. The grounds cross-reference

this section when identifying the communication, processing, and storage structures in the prior-art systems.

113. In my opinion the term "supervisor" as used in the patents does not require a construction, but for the sake of clarity, I note that the patents describe a broad range of individuals and/or groups filling this role. For example, the Asserted Patents describe parents, nearby first responders, and dispatchers as all being potential supervisors. Ex.1003, 25:4-11, claim 23; Ex.1001, 18:6-23, 26:40-41. In my opinion, a POSITA would have understood that a variety of roles, such as dispatchers, who do not occupy a typical hierarchical "supervisor" role, are supervisors within the claims.

114. All other terms. I have applied the ordinary and customary meaning to every other term in the challenged claims. My opinions would not change under any reasonable alternative construction because the prior art disclosures and the technical reasons for the combinations do not depend on a narrower or specialized meaning of any other term.

VIII. DESCRIPTION OF THE PRIOR ART

A. Staton (Ex.1007)

115. U.S. Patent No. 7,317,927, titled "Method and System to Monitor Persons Utilizing Wireless Media," issued January 8, 2008 to Houston Staton, Torres Mercedes Piso, James Ashley, Sr., James Ashley, Jr., and Patrick Mooney, and

assigned to Wireless Werx International, Inc. I understand that Staton qualifies as prior art under 35 U.S.C. §§102(a)(1) and (2). Ex.1007, cover.

116. Staton concerns monitoring persons, including children, carrying portable wireless devices such as PDAs within defined geographical zones. Ex.1007, Abs., 3:6-18, Fig. 5. It explains that a PDA can determine its position using GPS data, determine its relation to a zone, and transmit an event message when an event such as entering or exiting a zone occurs. Ex.1007, 2:40-65. Staton states that the PDA is event-driven and transmits data when configured exceptions occur, including boundary crossings and other monitored conditions. *Id.,* 3:10-21, 14:1-19.

117. Staton's backend architecture performs several functions. The patent states that PDAs send event information to backend control system 150, which includes gateways 151-154, codec 155, asynchronous routing system 159, routing services 156, database 157, and web server 158. It also identifies operations data processor 173 for defining geographical zones and waypoints, configuration utility 172 for configuring PDA features. Ex.1007, 6:66-7:23.

118. Staton also explains how a zone is represented and configured. A zone may be defined by waypoints, irregular boundaries, and/or a pixilated image. Ex.1007, 14:34-44. In the pixel-map, "each pixel 505 is a square," the squares draw the outline shape 510 of zone 515, and "a geographical area is then mapped to each pixel 505." Ex.1007, 16:47-17:16. Staton further describes an 80-by-80 pixel map

and a position-fix test that determines whether a PDA is inside or outside the zone. *Id.,* 15:4-9.

119. Staton's configuration disclosure is also relevant to resolution. It explains that a user may select a rectangular area, divide it into smaller rectangles, activate selected pixels, and choose the resolution. Ex.1007, 15:27-55. It states that increasing the number of grid rectangles increases resolution because each rectangle covers less geographical area, while reducing rectangle size provides greater detail. *Id.,* 15:46-55.

120. Staton provides event-driven notification through the backend. It states that the backend can reroute an event message from one PDA to another, that the remote notify router formats and encodes messages, and that messages are placed in outbound SMS or SMTP queues for gateway transmission. Ex.1007, 8:19-25, 21:47-51, 22:16-36. It also describes real-time and historical databases used to update and display PDA information.

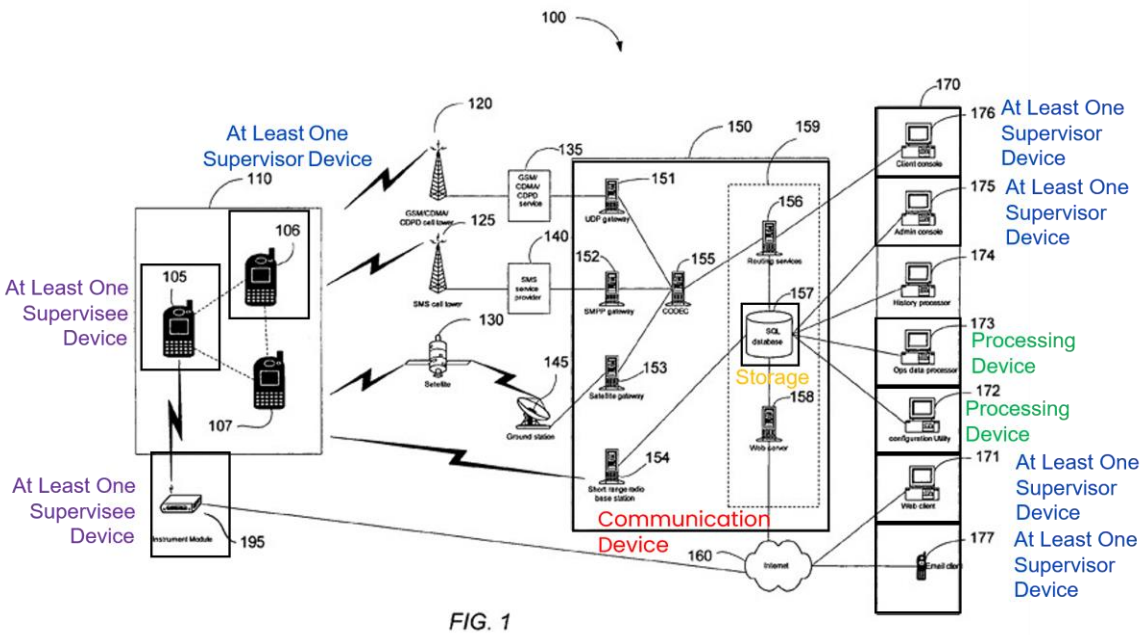


FIG. 1

Ex.1007, Fig. 1 (annotated).

B. Noland (Ex.1008)

121. U.S. Patent Application Publication No. 2018/0158305, titled "System and Method of Automated Gunshot Emergency Response," was published June 7, 2018 to Bryan Lee Noland and Frank Z. Patterson and assigned to OnAlert Guardian Systems, Inc. I understand that Noland qualifies as prior art under 35 U.S.C. §§102(a)(1) and (2). Ex.1008, cover.

122. Noland discloses a threat sensing system 100 with threat sensing devices distributed throughout a school or other facility and a system gateway 110. The threat sensing devices may include acoustic, gas, pressure, and image sensors, and communicate sensor data to the gateway. Noland states that the gateway receives

and processes the data to determine whether it corresponds to a known threat, such as a gunshot. Ex.1008 ¶¶[0015]-[0019].

123. Noland's gateway can analyze a sound waveform to determine whether it is a valid gunshot, determine the general weapon type, and establish the location or room number of the shooter. Ex.1008 ¶¶[0106]-[0108]. It can evaluate subsequent waveforms to determine whether more than one weapon or shooter is involved. *Id*. ¶[0108]. Noland also describes weapon and ammunition classification using lookup information, including caliber categories such as 9 mm, .223, and .308. *Id*. ¶¶[0111], [0127].

124. Noland also integrates facility information into the response. It describes stored floor-plan and building-layout information, alerts that provide the threat location and a diagram of the school, and a displayed map showing the threat highlighted in a particular classroom. Ex.1008 ¶¶[0019], [0025]-[0026], [0095]-[0097]. It further discloses NFC and far-field communication devices that can communicate with nearby portable devices, including RFID integrated into an identification badge. *Id*. ¶[0074].

125. Noland's notification system communicates threat information to first responders, dispatchers, school staff, administrators, and other designated recipients. Noland states that the system gateway sends information about the weapon discharge, including location, acoustic and image signatures, weapon type, and

caliber, to mobile devices and local authorities. Ex.1008 ¶¶[0092]-[0098]. *Id.* ¶¶[0103]-[0109].

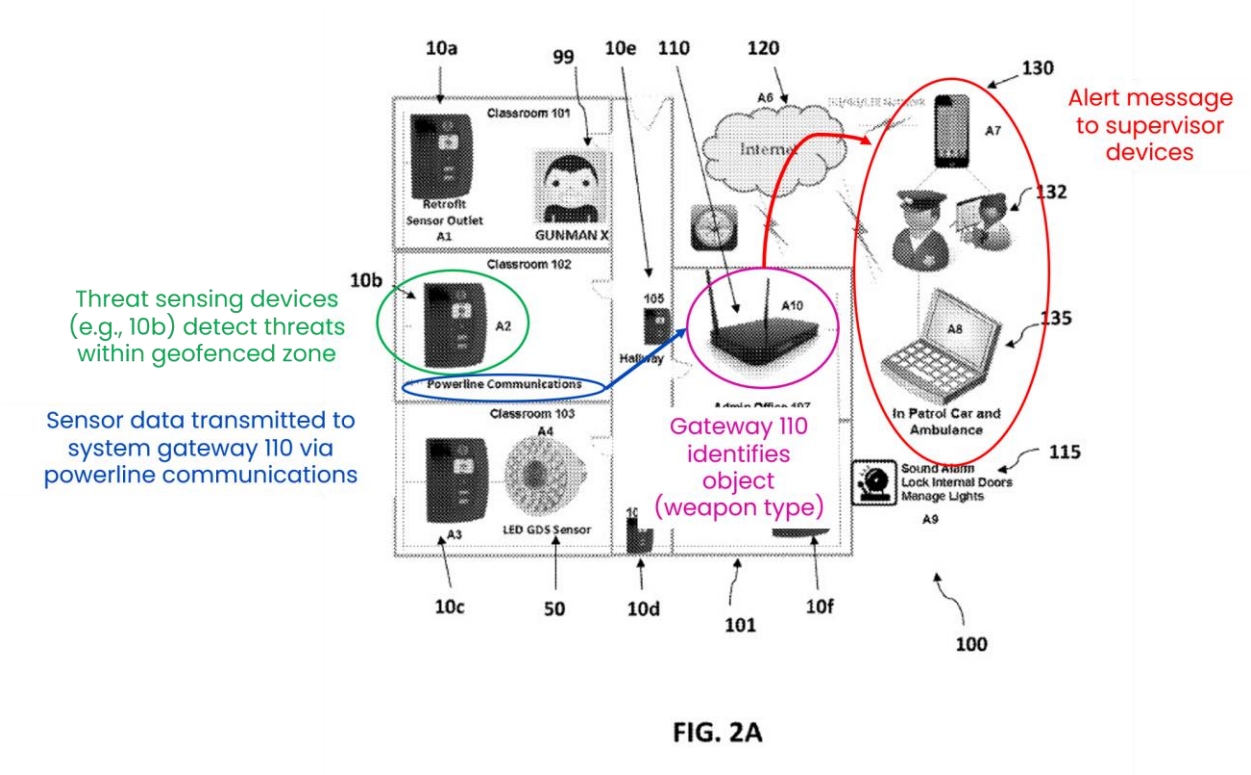


FIG. 2A

Ex.1008, Fig. 2A (annotated).

C. Rauner (Ex.1009)

126. U.S. Patent Application Publication No. 2019/0166480, titled "Emergency Messaging System and Method of Responding to an Emergency," was published May 30, 2019 to Paul A. Rauner and assigned to SirenGPS, LLC. I understand that Rauner qualifies as prior art under §102(a)(2) based on its effective filing date. The application was filed January 7, 2019, is a continuation of Application No. 15/865,245 filed January 8, 2018, and claims a continuation-in-part

relationship to Application No. 14/369,147 filed June 26, 2014, with provisional applications identified on its face. Ex.1009, cover.

127. Rauner describes an emergency response computer system operating with remote computing devices, response units, and a communications network. It uses a cloud computing environment accessed by PSAP computers through a browser. Response computer system 101 includes processing unit 161, emergency response module 150, storage device 162, and modules including device communications module 151, processing module 152, response module 154, notification module 155, determination module 156, administration module 157, and mapping module 158. Ex.1009 ¶¶[0031]-[0034], [0047]-[0059], [0239].

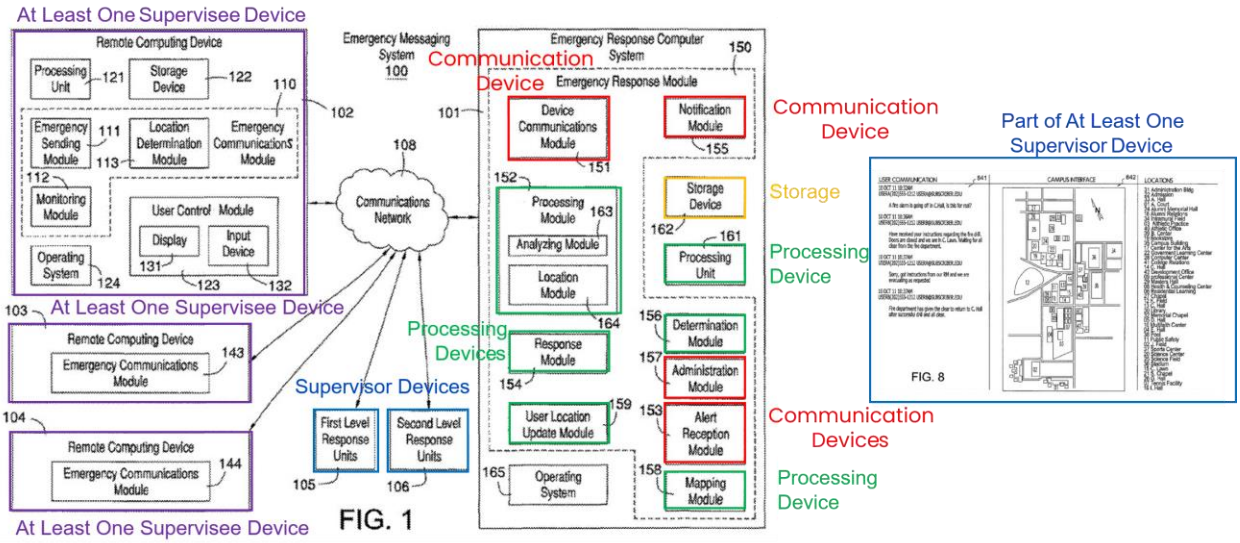
128. Rauner's mapping module loads graphical representations, creates an alphanumeric grid over a map, translates grid coordinates to GPS coordinates, and associates GPS coordinates within a grid box. Ex.1009 ¶¶[0093]-[0095]. The system administrator can select buildings, floors, parks, zones, and other areas through the graphical interface. *Id*. ¶¶[0093]-[0095]. Rauner also describes a geofence defined by the geographic footprint of a building and matching the location of an event to a building schematic. *Id*. ¶¶[0197]-[0199], [0215].

129. Rauner describes two overlapping embodiments. System 100, in paragraphs [0047]-[0095], provides the core architecture and emergency messaging functions. Ex.1009 ¶¶[0047]-[0059]. System 1600, in paragraphs [0157]-[0200],

extends that architecture with additional modules, including structure module 1657, while retaining processing unit 161, storage device 162, device communications module 151, remote computing devices 102-104, and communications network 108. *Id*. ¶¶[0157]-[0166], [0194]-[0200].

130. In my opinion, a POSITA would have understood system 100 and system 1600 as complementary descriptions of a single system, not mutually exclusive alternatives. Both use the same processing unit 161, storage device 162, device communications module 151, remote computing devices 102-104, and communications network 108. Ex.1009 ¶¶[0052]-[0059]. Components that share the processor, storage, communications interface, and client devices are parts of one system because the later embodiment adds modules to the same processing and communications framework. *Id*. ¶¶[0162]-[0166].

131. Rauner stores and processes location and profile information and generates notifications. It describes current and past locations stored in user profiles. Ex.1009 ¶¶[0050], [0098]-[0099]. It also describes emergency messages recorded in an event log, and mass-event warning messages entered into a subscriber message log in storage device 162. *Id*. ¶¶[0070]-[0075], [0080]-[0083]. It also describes location-based determination of response units and transmission of emergency messages to affected devices. *Id*. ¶¶[0098]-[0099].



Ex.1009, Figs. 1 and 8 (annotated).

D. Azmoodeh (Ex.1010)

132. U.S. Patent Application Publication No. 2017/0287006, titled "Mutable Geo-Fencing System," was published October 5, 2017 to Farnaz Azmoodeh, Peter Sellis, and Jinlin Yang and assigned to Snap Inc. I understand that Azmoodeh qualifies as prior art under 35 U.S.C. §§102(a)(1) and (2). Ex.1010, cover.

133. Azmoodeh describes generating a geofence from geolocation data, including a radius around a point or other defined boundaries. Ex.1010 ¶¶[0015]-[0018]. It then describes dividing the first region encompassed by the geofence into a set of cells, with each cell representing a portion of the region and the cells collectively covering the region. *Id.* ¶¶[0022], [0043]-[0046].

134. Azmoodeh states that "the number of cells within the region may be defined based on a size of the geo-fence, or based on user input." It further assigns

usage metrics to cells based on messages and uses those metrics to adjust a geofence boundary. The cell subdivision is prior to and separable from the later metric and boundary-adjustment operations. Ex.1010 ¶¶[0046]-[0049].

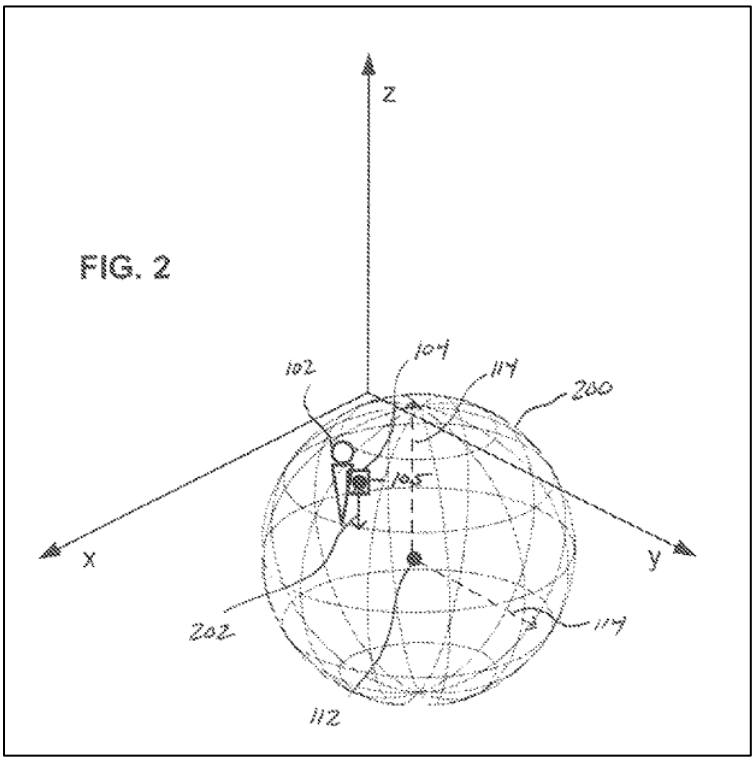
135. In my opinion, Azmoodeh's cell-subdivision technique is a general-purpose geofencing technique rather than one tied to content delivery. Ex.1010 ¶¶[0015]-[0018]. The subdivision operates on geospatial coordinate data describing the fenced region and is indifferent to the purpose for which the resulting cell-level location information is used. The usage metric that Azmoodeh happens to compute is a separate downstream step. A POSITA seeking finer spatial granularity within a geofence for safety monitoring would therefore have recognized the technique as applicable because the same cells can be used to associate locations with any later monitoring or notification function. *Id*. ¶¶[0043]-[0049].

E. Smith (Ex.1011)

136. U.S. Patent No. 10,085,117, titled "Methods and Apparatus for Altitude-Based Geofencing," issued September 25, 2018 to Michael Smith and Manase Xiong and is assigned to DISH Technologies L.L.C. It issued from U.S. Application No. 15/379,779, filed December 15, 2016. I understand that Smith qualifies as prior art under 35 U.S.C. §§102(a)(1) and (2). Ex.1011, cover.

137. Smith concerns geofencing that incorporates altitude data and is therefore three-dimensional. Smith identifies the two-dimensional character of then-

existing geofencing as a shortcoming, stating that such techniques "are generally two-dimensional (*i.e.*, are defined within a planar map) and thus do not comprehend an altitude, height, or 'z-axis' attribute," so that they cannot determine "whether a user has changed floors within a home." Ex.1011, 1:27-36.



Ex.1011, Fig. 2.

138. Smith's method defines a virtual boundary in a three-dimensional geographical space including lateral position parameters and an altitude parameter, defines a boundary-related event and an action triggered by the position of a trackable object with respect to that boundary, estimates that position from lateral position values and an altitude value, and performs the action if the event is triggered. *Id.,* Abstract, 4:51-61. Smith adds that the current location of the trackable

object may be "set as the z-distance for a boundary (*e.g.*, first floor, second floor, etc.)." *Id.,* 5:3-6.

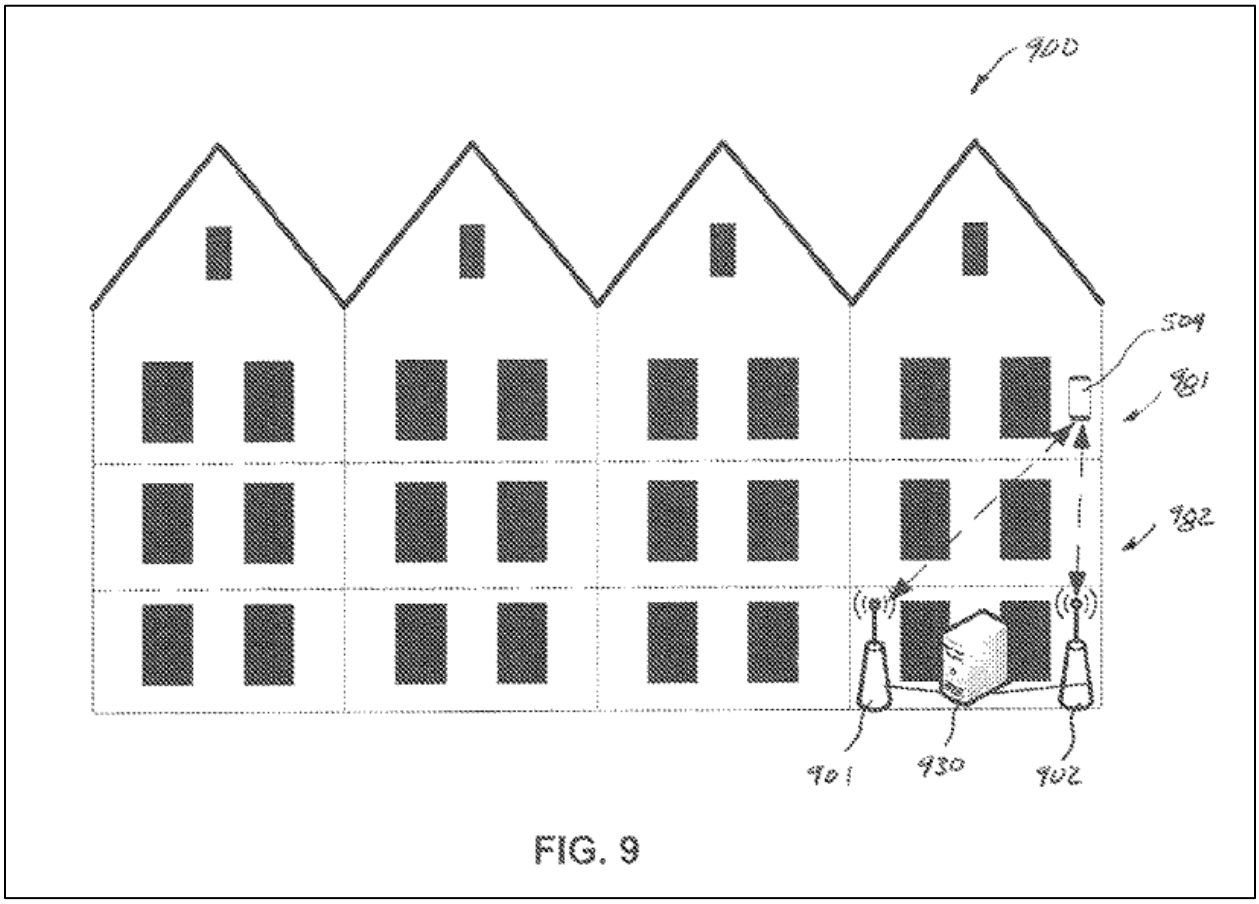


FIG. 9

Ex.1011, Fig. 9.

139. Smith describes several means of estimating altitude using an altitude estimation module. *Id.,* 4:37-50. Smith applies the result to resolve position to a floor, describing a structure that "includes multiple (*i.e.*, 3) stories, or 'floors'," a system that determines "whether a trackable object 504 . . . is on the third floor 981 or 982, and act[s] accordingly," and the use of altitude data by "first responders . . .

to determine which floor (*e.g.*, 981 or 982) the user is on during an emergency situation, such as during a fire." *Id.,* 5:30-50, 5:62-65.

IX. INVALIDITY OF '757 PATENT CLAIMS 1-18 UNDER 35 U.S.C. § 103

140. In my opinion the '757 patent is invalid based on the following grounds:

Ground	Claims	Reference(s)
1	1-4, 6, 8, 10-13, 15, 17	Staton + knowledge of a POSITA
2	5, 7, 9, 14, 16, 18	Staton + Noland + knowledge of a POSITA
3	1-4, 6-8, 10-13, 15-17	Rauner + Azmoodeh + knowledge of a POSITA
4	5, 9, 14, 18	Rauner + Azmoodeh + Noland + knowledge of a POSITA

A. Ground 1: Claims 1-4, 6, 8, 10-13, 15, 17 are Rendered Obvious By Staton + Knowledge of a POSITA

1. Relevant Architecture

a. Architecture of Staton

141. In my opinion, Staton's backend control system 150 is a unified server infrastructure containing communication, processing, and storage components and applications that correspond to the claimed devices.

RAVE/MSI, EX1005, p. 88

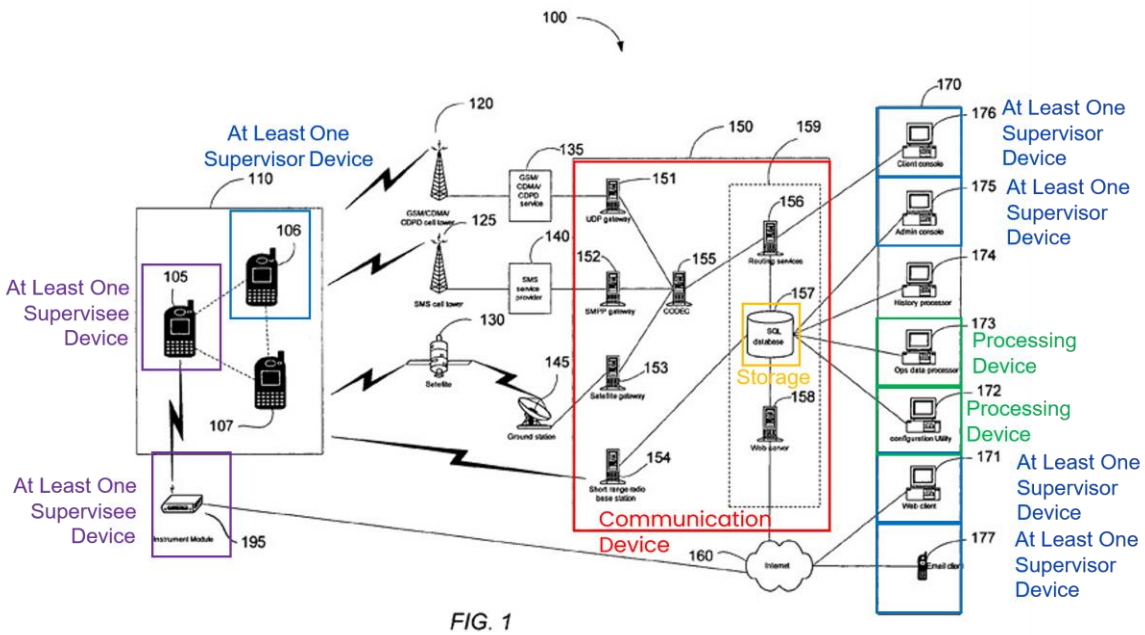


FIG. 1

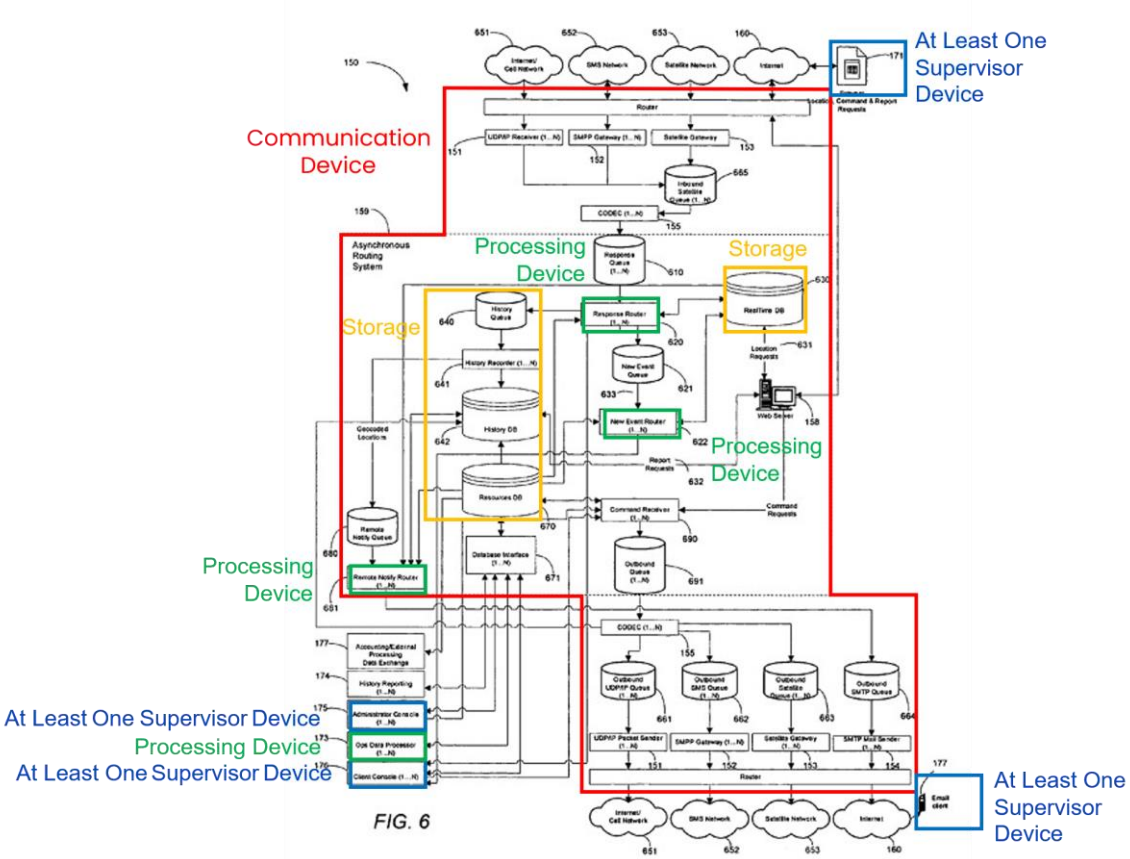


FIG. 6

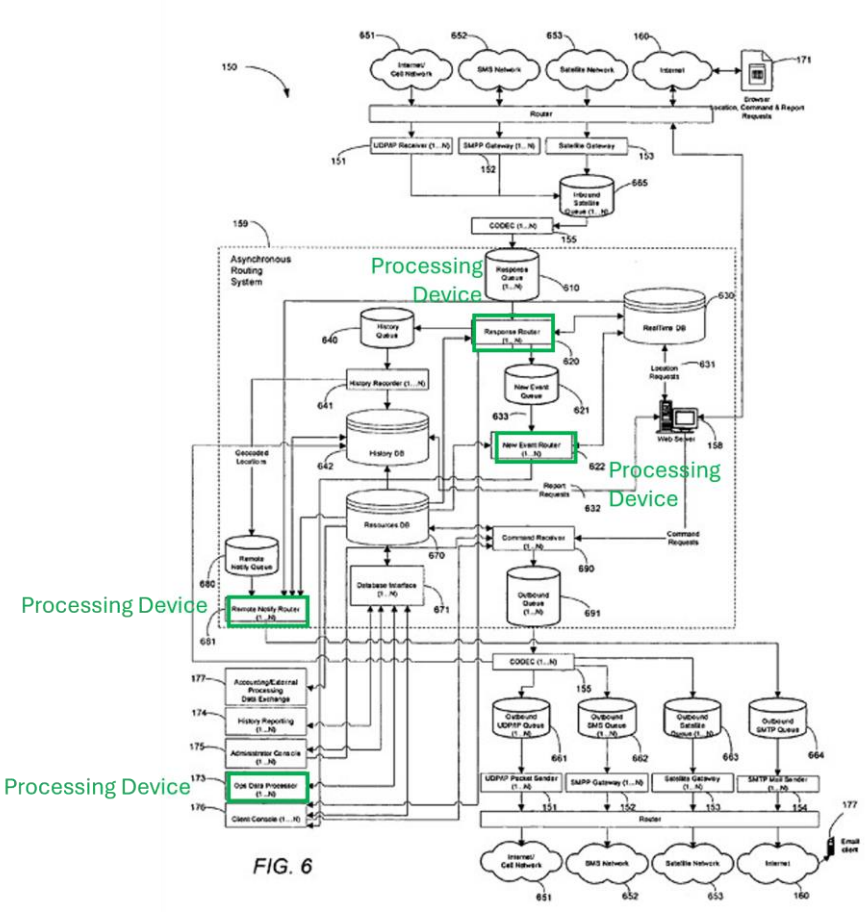
Ex.1007, Figs. 1 and 6 (annotated).

142. As shown in the figure above, Staton includes a communication device, storage device, and processing device.

143. I describe these devices in Staton further in by limitation-by-limitation mapping below.

144. FIG. 6 and Staton's description at 6:66-7:23 show an integrated arrangement of gateway systems 151-154, codec 155, asynchronous routing system 159, routing services, databases, networks, and a web server. Staton explains: "The codec 155 is the central codifier and decodifier of the backend control system 150 and allows the backend control system to adapt and communicate with any communications network." Ex.1007, 7:6-9. This disclosure identifies the codec as the component that converts communications into a form the backend can process and into a form suitable for transmission, which is why it performs part of the claimed receiving and transmitting functions. Staton further states: "The backend control system 150 also includes an asynchronous routing system 159 that allows incoming and outgoing communications to be handled asynchronously and efficiently. In one embodiment, the asynchronous routing system 159 includes a plurality of routing services 156, at least one database 157 and a web server 158." *Id.,* 7:12-17. The routing system, routing services, database, and web server therefore provide the internal paths and message-handling functions through which

the backend receives inputs, processes destinations, and sends outputs to the relevant devices. Ex.1007, 7:6-17.



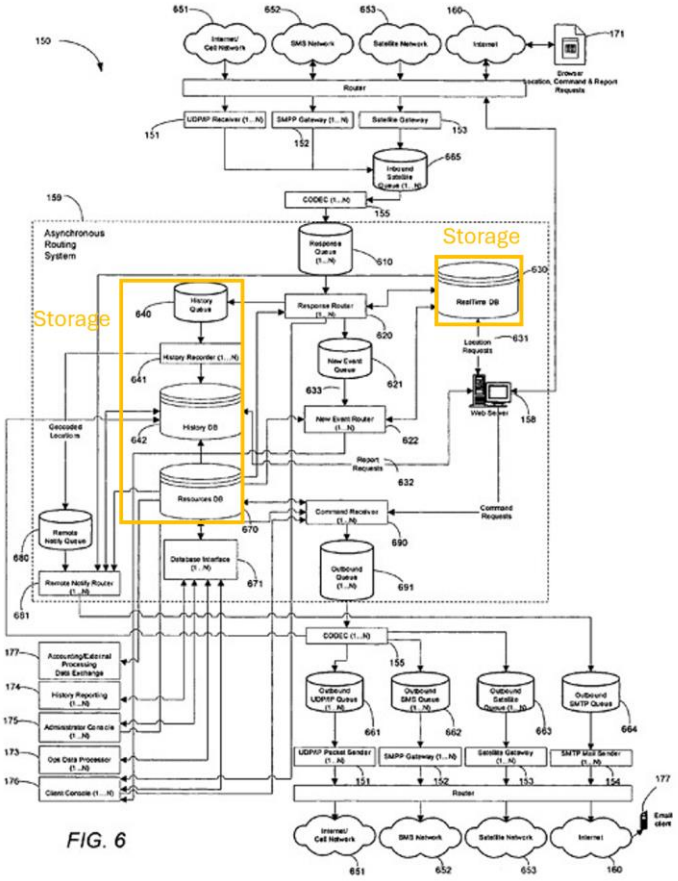
Ex.1007, Fig. 6 (annotated).

145. The processing components are likewise part of that server-side infrastructure. Staton states: "An operations data processor 173 permits an operator to define geographical zones and waypoints for operation of the PDA 105. A configuration utility 172 permits operators to easily configure PDA 105, features and functionality." Ex.1007, 7:30-33. Defining zones and waypoints and configuring

the PDA are the substantive operations that the claim assigns to the processing device when it analyzes supervisor inputs and generates a geofence.

146. The response router 620, new event router 622, and remote notify router 681 perform additional server-side routing and event processing relevant to claim functions that analyze supervisee data and generate or route notifications. *Id.,* 21:47-22:33. First, the remote notify router 681 is the basis of what I have termed "the remote notify router theory" in which the remote notify router 681 determines that a remote notification is required, retrieves the relevant contact information and formats and encodes the required message. Ex.1007, 22:18-35. Remote notifications "can be received by a member having permissions to receive such notification" and "can be an email, SMS message, an instant message, a voice message, a network popup, and alphanumeric page, etc." *Id.*, 25:29-40. Second, response router 620 is the basis of what I have termed "the response router theory" in which the response router 620 determines that client console 176 is tracking the supervisee PDA and routes "the incoming message to the appropriate client console 176." Ex.1007, 21:47-51.

RAVE/MSI, EX1005, p. 92



Ex.1007, Fig. 6 (annotated).

147. The storage components are also expressly within the backend control system. Staton states: "the real time database 630 can maintain records of the most recent information from a PDA such as location, speed, direction, associated instruments, associated geographical zones, etc." Ex. 1007, 19:52-55. This database contributes the current supervisee information used for monitoring. Staton further states: "The history database 642 maintains records of all events and transactions that were received and sent from the asynchronous routing system 159." *Id.*, 19:55-58. This database contributes the record of inbound supervisee data and outbound

supervision notifications. Finally, Staton states: "the resources database 670 keeps records of all the instrument modules and PDAs that are part of the system." *Id.,* 19:58-60. The resources database contributes the device and configuration information used to identify devices and determine how received events should be handled. Together, these databases perform the claimed storing function for the data, messages, and supporting records used by the system. Ex.1007, 19:50-20:3.

b. ***A POSITA's Understanding of the Architecture***

148. In my opinion, a POSITA would have understood these communication, processing, and storage components to work together as a single server architecture because the gateways feed the asynchronous routing system, the routing system uses the databases and routers, and the databases supply information back to the processing and communication components. Staton does not merely permit a single-computer implementation; it encourages and motivates implementing these parts of backend control system 150 on a single computer system, and a POSITA would have had a reasonable expectation of success in doing so. Staton expressly states that "[t]he backend control system 150 can be configured to run on any combination of computer servers," including the configuration in which its communication gateways "run on a common computer system." Ex.1007, 19:61-66; Fig. 6. Those statements confirm that the described functions are server-

hosted functions whose precise physical distribution can easily vary without changing the functions of the components.

149. Accordingly, it would at least have been obvious to implement the communication, processing, and storage functions in a single server system. Staton expressly permits different server arrangements, and the precise distribution of software services and databases was an ordinary implementation choice because the components already communicate through defined queues, routers, gateways, and shared databases; placing those cooperating services on one server would reduce inter-server traffic while preserving the same message interfaces and processing sequence. Ex.1007, 19:61-66, 20:1-8, 21:18-22:3.

150. Regarding the disclosed configuration utility and operations data processors, I also note that Staton further states: "[o]perations data processors 173 connect to the resources database 670 in order to retrieve configuration information for a specific user, PDA 105, or instrument module 195" and "[m]ultiple applications may connect to the central database 157 to provide further system functionality….An operations data processor 173 permits an operator to define geographical zones and waypoints for operation of the PDA 105. A configuration utility 172 permits operators to easily configure PDA 105, features and functionality." Each application is described as reaching internal queues, routers,

RAVE/MSI, EX1005, p. 95

and databases of the backend system and is described as a server-hosted application or service. *Id.,* 24:12-25, 7:24-33.

151. Staton also says that "the computing device is a home computer and the user is the PDA 105 user who configures the different geographical zones on his computer. The home computer connects to the configuration utility through a direct secure connection via an application installed on the home computer. Alternatively, the home computer can be connected through the Internet using a web browser." 1007, 7:18-23, 15:17-22; FIG. 6. Similarly, Staton says "[t]he schedule times, area boundaries, speed limits, and acceleration parameters are determined by the parents and can be changed at any time through the internet/cellular system." *Id.* 27:66-28:2. And, as stated above, the operations data processor is the application that Staton describes as "permit[ting] an operator to define geographical zones and waypoints for operation of the PDA 105" and the configuration utility is the application that Staton describes as "permit[ting] operators to easily configure PDA 105, features and functionality." *Id.* 7:30-33.

152. These descriptions of parents configuring the geofences through a remote network like the internet/cellular system reinforces the understanding that these are server hosted applications or services that are exposed through communication interfaces rather than distinct remote client machines.

153. Below I provide my analysis of the Challenged Claims in view of Staton.

2. Claim 1

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

154. Staton states that "[t]his disclosure relates to systems and methods for monitoring persons, such as children within a specific … geographical zone." Ex.1007, 1:20-22, 26:24-26; *id.* 8:11-14, 1:64-67. This establishes that Staton monitors persons in relation to a defined geographical zone, which is the claimed supervision context. Staton also states: "[a] user can monitor an individual carrying a PDA 105 in relation to a geographical zone." *Id.,* 26:24-26. This identifies the monitored PDA user as the individual being supervised and ties the monitoring to the geographical zone.

155. Staton provides the parent-monitoring-daughter relationship in FIG. 8B. It states: "In one embodiment, through the use of the PDA 106 a parent can, monitor the location, movement, and vehicle conditions of his daughter carrying PDA 105." Ex.1007, 8:11-14. This supplies both sides of the supervisory relationship: the parent using PDA 106 is the supervisor, and the daughter carrying PDA 105 is the supervisee. Staton also explains that "where a family of multiple members (*e.g.*, father, mother, son, and daughter) each have a PDA, a parent can

own a PDA 106 which monitors all of the other PDAs," and that "[t]he monitoring individual (*e.g.* the parent) can also be provided with a portable device that is networked with the portable device of the monitored person (*e.g.*, the child)." *Id.,* 27:11-15, 1:64-67. The first family disclosure confirms that one supervisor device can monitor multiple supervisee devices, while the second confirms the networked supervisor-device/supervisee-device arrangement. PDA 105, carried by the monitored individual, is the supervisee device, while PDA 106 is the supervisor device. *Id*., FIG. 8B.

156. Staton also expressly discloses the general supervision function and geofencing events. It states: "[v]arious events can be configured based on 'geofencing' events." Ex.1007, 13:65-66. Staton further explains: "Geofencing entails creating configurable boundaries or geographical zones in which a PDA 105 operates," and "the entering or leaving a geographical area that has been geofenced can be an event itself." Ex.1007, 13:66-14:4. Staton further explains that an event related to a geographical zone can trigger communication from one PDA to another. *Id.,* 14:12-13.

157. Regarding FIG. 8B, Staton states that "[t]he daughter's PDA 108 could include the geographical area for an unsafe neighborhood and event alarms indicating that the unsafe neighborhood has been entered along with instructions on how to leave the dangerous neighborhood." Ex.1007, 28:58-59. This disclosure

shows a supervisee device carrying a zone-specific rule that produces an alarm when the supervisee enters a designated unsafe area, which is supervision based on a geofence in operation. *Id.* 27:11-15, 27:52-54. The preamble is disclosed.

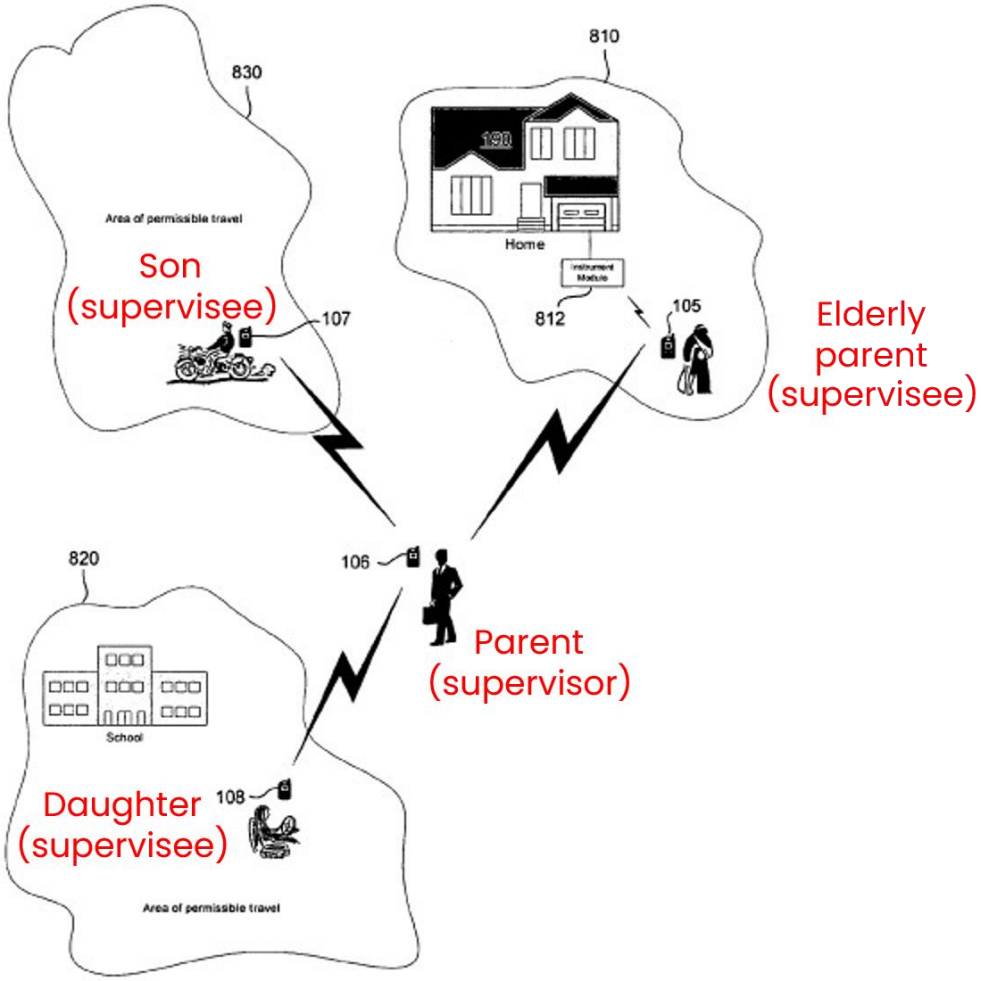


FIG. 8B

Ex.1007, Fig. 8B (annotated).

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;"***

158. For limitation 1[a], the communication device = the communication components of Staton's backend control system 150, including the functions,

including programs, middleware, and software, running in the gateways 151-154, codec 155, asynchronous routing system 159, routing services 156, database 157, and web server 158 that handle communications between the server-side system and client devices. Ex.1007, 6:44-48, 6:66-7:23, 7:6-15, 19:62-67, Fig. 6; *see* Section [IX.A.1.b]. The at least one supervisor device = PDA 106, the home computer, web client 171, client console 176, and administrator console 175. Ex.1007, 7:25-33; 15:17-22; 17:26-33; 24:12-25. In my opinion, Staton discloses "receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor," for example, because the identified supervisor devices provide the configuration inputs and the backend communication components receive and communicate those inputs. Ex.1007, 6:66-7:23.

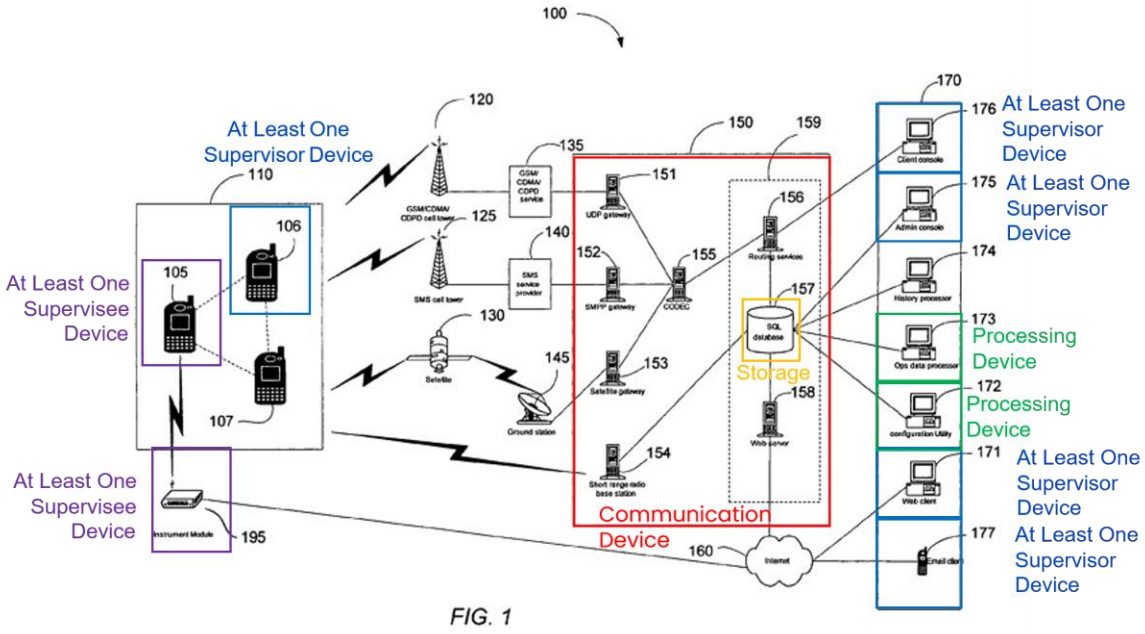


FIG. 1

Ex.1007, Fig. 1 (annotated).

159. The at least one security parameter = Staton's properties and rules associated with Staton's geographical area. Staton states: "[t]he properties of a zone include a name, description and a flag determining if the zone is an off-limits zone or an enclosed zone." Ex.1007, 14:53-55. The off-limits or enclosed flag is a supervisor-set configuration value that governs whether the monitored person is treated as being in a restricted area or within a contained area, so it governs how the system supervises the person relative to the zone. Staton also states that zone-related parameters include "speed threshold of the entity, flagged as a 'no-fly zone,' color coded in order of danger or security threat, communication enabled or disabled, etc." *Id.,* 16:13-17. Each threshold, flag, color, and communication setting changes the security-related monitoring behavior associated with the zone, for example, by identifying a prohibited area, expressing a danger level, or controlling whether communications are enabled. Staton further states: "[e]xemplary events can be configured 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 event rules determine which movements or timing conditions produce monitoring events and therefore govern whether and how the supervisee is supervised. A POSITA would have understood these supervisor-set properties, thresholds, flags, and event rules to be security parameters because they are configuration values that control security-related monitoring of a person in a geographical zone.

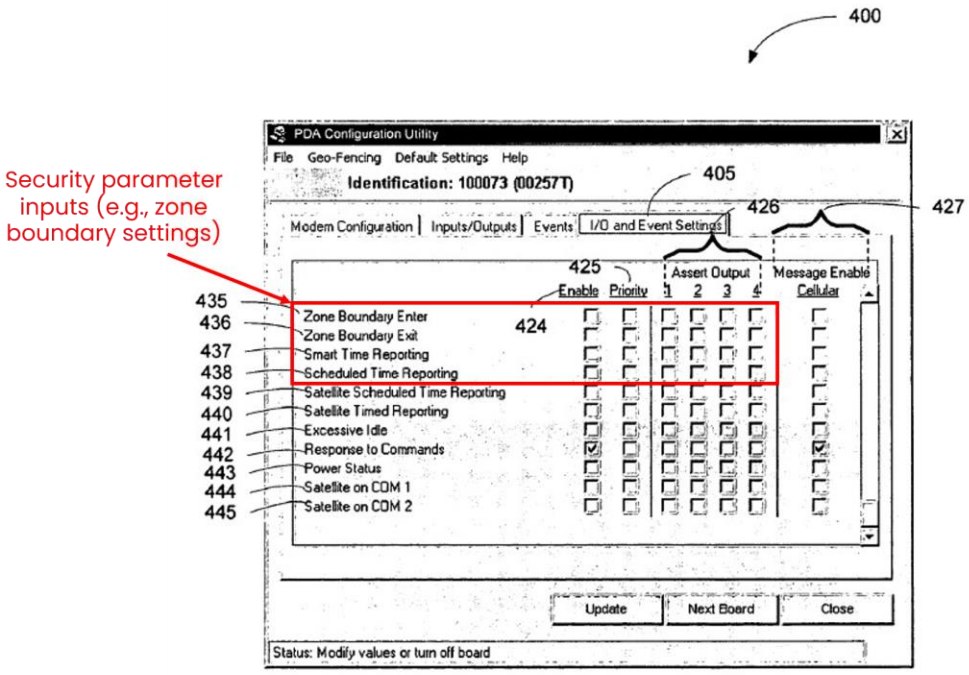


FIG. 4

Ex.1007, Fig. 4 (annotated).

160. Staton explains that "the configuration of devices is entered through the backend control system 150 or any other portal host." When a supervisor uses a home computer or console to set zone properties, event rules, or thresholds, those parameters necessarily travel through the backend's communication components to the internal configuration utility that processes them. Ex.1007, 11:27-50, 25:60-62, 27:66-28:2.

161. Staton also discloses that "the computing device is a home computer and the user is the PDA 105 user who configures the different geographical zones on his computer. The home computer connects to the configuration utility through a

direct secure connection via an application installed on the home computer. Alternatively, the home computer can be connected through the Internet using a web browser." Ex.1007, 15:17-23. In this example, the home computer is a supervisor device setting configurations and security parameters for the supervisee PDA device via the configuration utility. Because the backend control system supplies the communication components between that supervisor device and the configuration utility, the security parameters are "receiv[ed], using a communication device ... from the at least one supervisor device." Thus, limitation 1[a], "receiving ... at least one security parameter from at least one supervisor device," is disclosed.

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

162. For limitation 1[b], the communication device has the mapping stated above, and the geographical location = the coordinates and user-selected geographical areas used to create Staton's zones. Staton states: "In one embodiment, a geographical zone may be created by selecting a plurality of coordinates and downloading the coordinates to the PDA 105. The plurality of coordinates may be in the Mercator system." Ex.1007, 14:56-59. These coordinates identify a real-world area selected for monitoring, and the system receives them as the geographic input from which the zone is created. Because the claim requires receipt of a geographical location, not a particular coordinate format, Mercator coordinates satisfy the

limitation. *Id.* 15:27-30.; *see also* 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.").

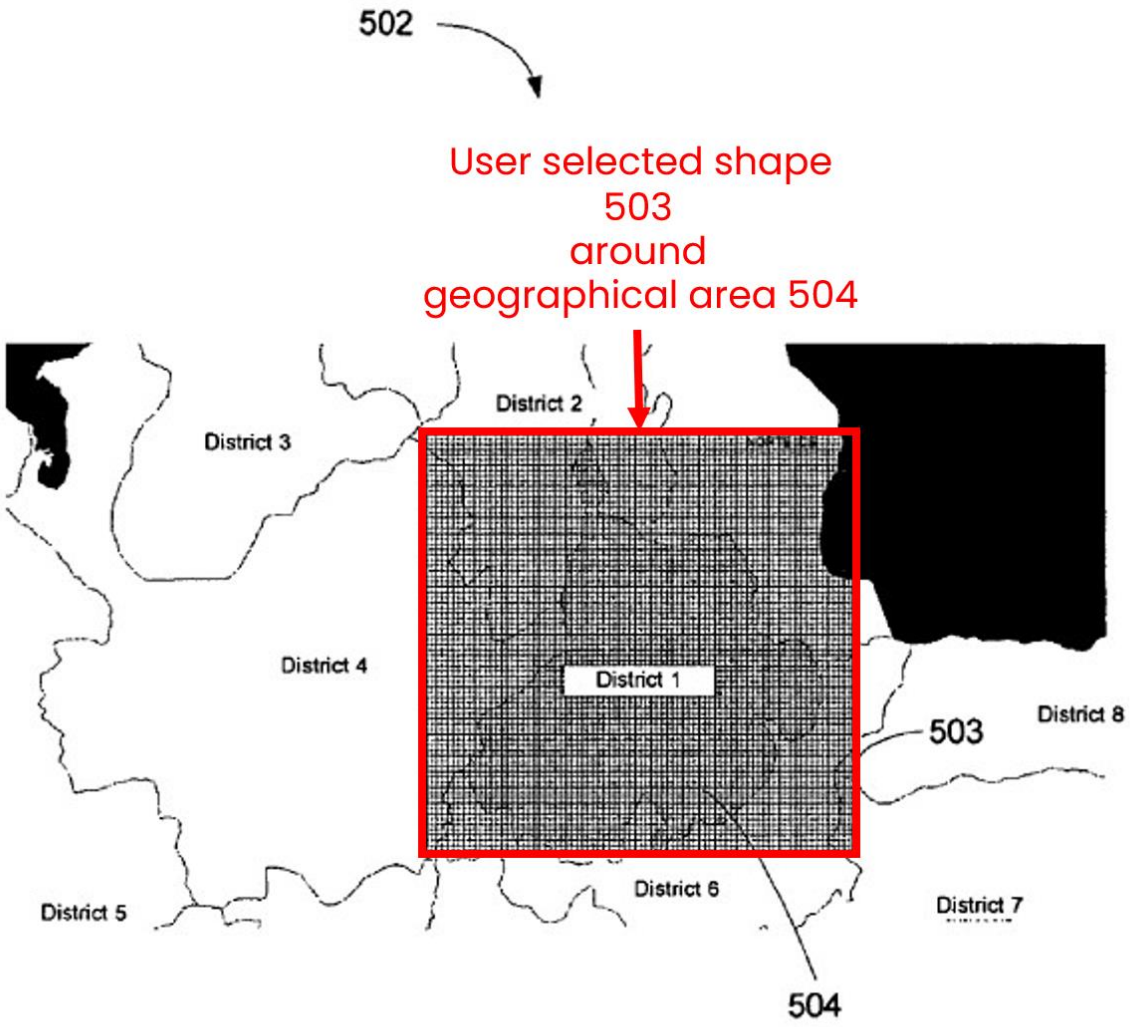


FIG. 5A

RAVE/MSI, EX1005, p. 105

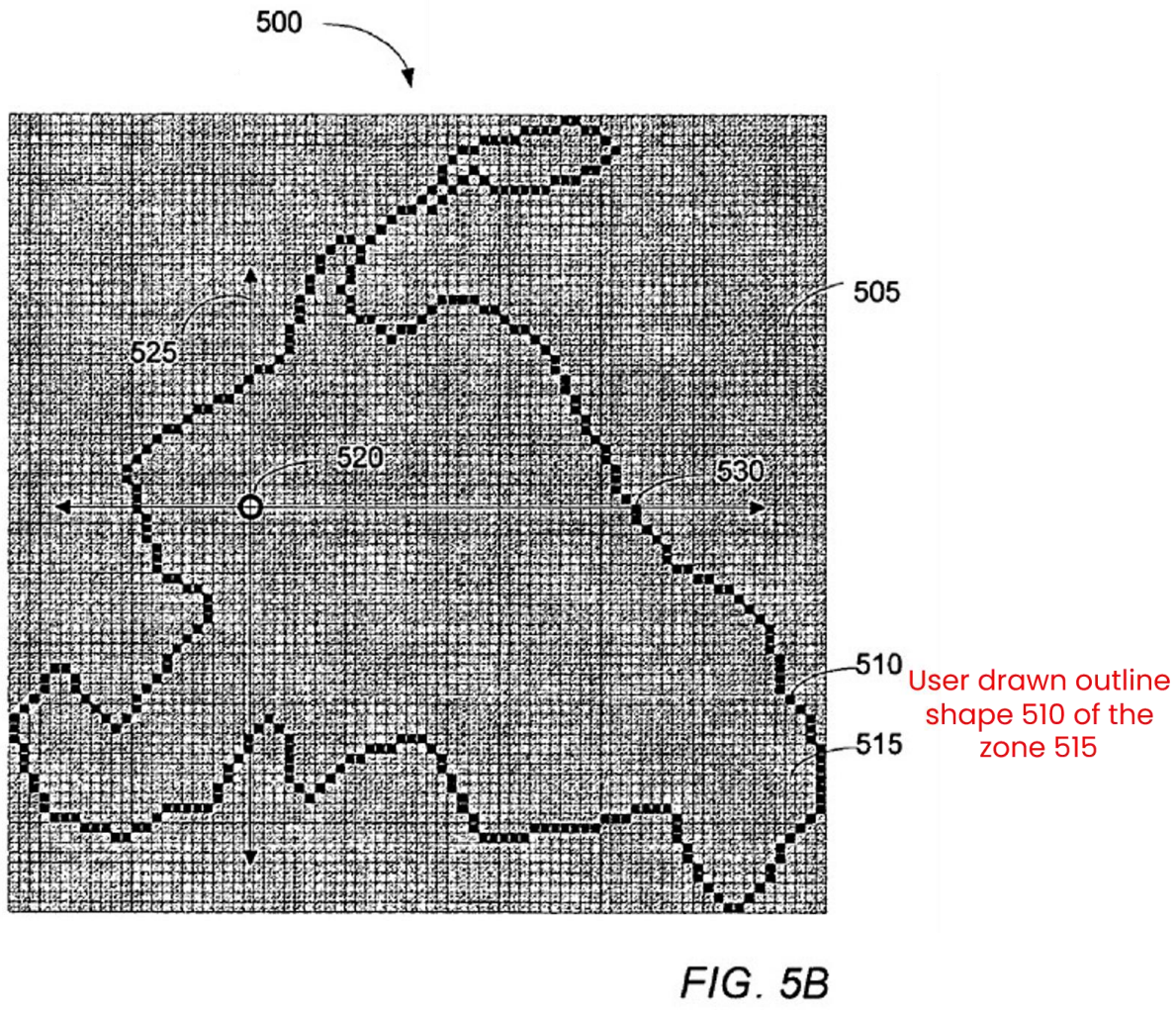


FIG. 5B

Ex.1007, Figs. 5A, 5B (annotated).

163. Staton also describes the supervisor selecting a rectangular shape: "The configuration application displays a map on which the user selects a rectangular shape 503 around the geographical area 504 that the user desires to define." Ex.1007, 15:27-30. The selected shape identifies the real-world area that the supervisor wants the system to monitor, so it is another form of geographical location received from the supervisor device. Staton further states: "The geographical zone can be a home environment, a work environment, a state, a city, a commercial neighborhood, a

residential neighborhood, or a school zone." *Id.,* 2:48-52. Staton also states: "Configurable boundaries or geographical zones can also be used and are configurable to any shape the user desires." *Id.,* 6:14-22. The claim does not limit the format of a geographical location, so a map selection, coordinates, or another user-selected boundary each meets the claimed receipt of a geographical location. As with limitation 1[a], when the supervisor makes that selection through a home computer or console, the data travels through the communication components of backend control system 150 to configuration utility 172. *Id.*, 15:17-23, 25:60-62, 27:26-27, 27:52-54, 27:66-28:2. This is "receiving, using the communication device, a geographical location from the at least one supervisor device," and limitation 1[b] is disclosed.

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

164. For limitation 1[c], the processing device = Staton's processing components including operations data processor 173 and configuration utility 172, and response, notification, and event routers. Staton states: "An operations data processor 173 permits an operator to define geographical zones and waypoints for operation of the PDA 105. A configuration utility 172 permits operators to easily configure PDA 105, features and functionality." Ex.1007, 7:30-33; *see id.*, 15:4-9, 11:48:50, 15:25-31; *see also* Section [IX.A.1.b]. In my opinion, Staton discloses

"analyzing ... the geographical location based on the at least one security parameter" because the operations data processor and configuration utility process the user-selected geographical area in light of, and as shaped by, the supervisor's security-related inputs to define and build the geographical zone. Ex.1007, 7:30-33. *Id.,* 15:4-9.

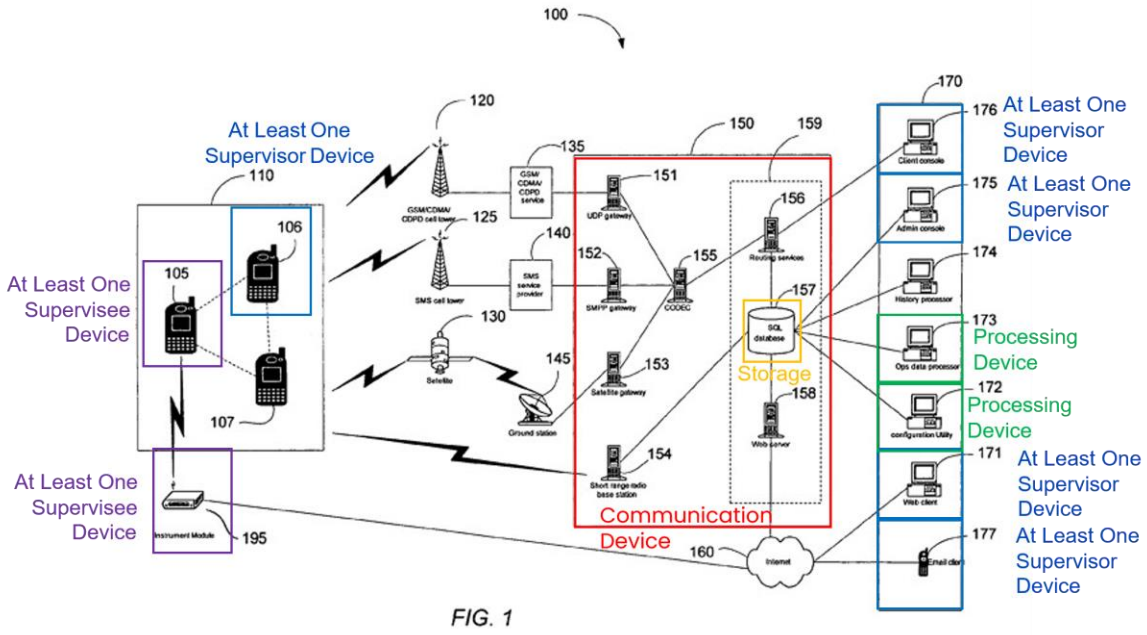


FIG. 1

Ex.1007, Fig. 1 (annotated).

165. In my opinion, Staton's processing components track the "processing device" of the '757 Patent. The '757 Patent specification describes its processing device as one or more computing devices that may be implemented in hardware, in software, or in a combination of the two, and it does not require any particular hardware embodiment. Ex.1001, 6:28-29, 28:59-29:14. Staton's operations data processor 173, configuration utility 172, and the server-side routers identified above

are likewise programs and functions executing on the backend server. Ex.1007, 7:30-33, 19:62-65.

166. In Staton, the security parameters directly influence how the geographical location is analyzed and what kind of geofence is generated. Staton states: "[t]he properties of a zone include a name, description and a flag determining if the zone is an off-limits zone or an enclosed zone." Ex.1007, 14:53-55. The off-limits or enclosed flag determines the character of the zone being created from the selected geographical area, designating it either as a restricted area or a contained area. Staton also states: "[t]he parent may utilize the configuration software to delineate specific areas where the son can travel, and areas where the son cannot travel. For example, an area of non-permissible travel can be outside of city limits, or a particular area where there is known gang activity." *Id.,* 27:52-54. In other words, the security assessment of a geographical area drives which geographical locations may be designated as geofences and how they are configured, so the geographical location is analyzed based on security-related determinations and parameters. Staton further states that zones may be "color coded in order of danger or security threat." *Id.,* 16:14-15. Here, the geographical area is selected and configured because of the security determination about that area; the security parameter, danger or threat level, is therefore the basis on which the system analyzes and configures the geographical location. Finally, Staton states: "[t]he daughter's

PDA 108 could include the geographical area for an unsafe neighborhood and event alarms indicating that the unsafe neighborhood has been entered along with instructions on how to leave the dangerous neighborhood." *Id.,* 28:55-57. This example shows the selected geographical area being configured as a security-related zone because it is unsafe, with the resulting zone controlling the monitoring response.

167. Staton further states: "[e]vents may be based on rules using a combination of the GPS position and one other factor such as time or speed." Ex.1007, 5:43-45; *see also id*., 11:59-67. This combination of position, which supplies the geographical location, and speed or time thresholds, which supply security parameters, in a rule-based framework confirms that the system analyzes geographical locations based on security parameters because the two are evaluated together. Staton also explains: "The schedule times, area boundaries, speed limits, and acceleration parameters are determined by the parents and can be changed at any time through the internet/cellular system." *Id.,* 27:66-28:2. These are supervisor-set values that alter how the selected area and the supervisee's operation within it are evaluated. As further support, Staton states: "[T]he PDA may detect geographical boundaries crossings, route and schedule adherence of a individual or host vehicle, reporting of position, speed, mileage, direction of travel, acceleration and altitude of the PDA, an individual or a host vehicle." *Id.,* 5:10-14. This shows the system using

location together with movement and threshold information in its monitoring rules. A POSITA would understand the combined zone-building and security/event-configuration teachings to perform that analysis because the same operations data processor and configuration utility evaluate the selected area together with the security-related inputs in order to produce the zone and its operational rules. The operations data processor therefore uses both the geographical location and these security parameters together to build the zone, thereby "analyzing ... the geographical location based on the at least one security parameter." Limitation 1[c] is disclosed.

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

168. For limitation 1[d], the processing is the same as 1[c], and the geofence corresponding to a geographical area = the outline shape 510 of zone 515 as represented in pixel map 500, including the associated settings and parameters relating to that boundary. Ex.1007, 2:53-65, 16:43-52, 14:1-3; 15:31-34. Staton states: "Waypoints and zones are built by the operations data processor 173. These loads are loaded on to the PDAs with the configuration utility 172." Ex.1007, 15:4-9, *see also* 16:53-56. This identifies the operations data processor and configuration utility as the processing components that perform the claimed generating.

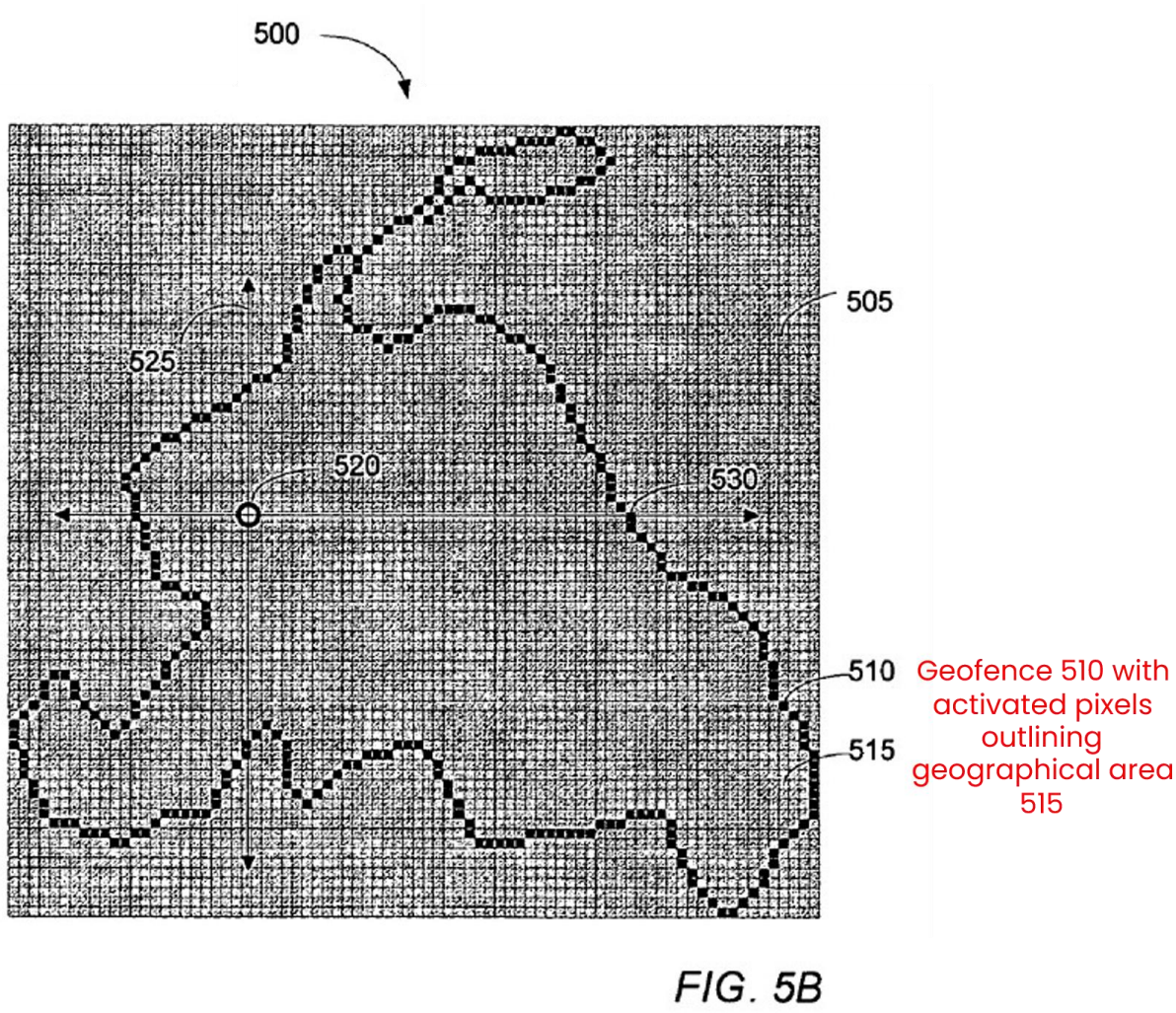


FIG. 5B

Ex.1007, Fig. 5B (annotated).

169. The configuration application displays a map, the user selects rectangular shape 503 around geographical area 504, and Staton states: "The rectangular shape is then divided into smaller rectangles such that the area of the rectangle is divided into a grid. Each pixel in the grid can be activated to be part of the geographical zone." Ex.1007, 15:31-34. The square or rectangular boundary first bounds the selected geographical area, the division creates the grid, and activation of pixels defines which portions form the zone boundary.

170. The generation is based on the analyzing because the operations data processor and configuration utility use the supervisor-selected geographical area together with the zone properties, event rules, thresholds, and other security parameters discussed for limitation 1[c]. Staton states: "A configurable boundary or geographical zone may be constructed through a combination of waypoints and/or zones," and "Geofences can be waypoints, zones, routes, or a collection of waypoints, a collection of zones, a collocation or routes, or any combination thereof." Ex.1007, 14:22-24, 26:39-41. The processing device can construct the boundary from the processed geographic inputs.

171. More specifically, Staton explains: "[t]he pixel map 500 is created by first drawing a square around the entire area of the zone. The square is then divided into an 80/80-pixel map. Each pixel 505 is a square. These squares are then used to draw the outline shape 510 of the zone 515. A geographical area is then mapped to each pixel 505 of the pixel map 500." Ex.1007, 16:47-52. In this example, the square supplies bounds, the 80/80 division supplies a grid, the square pixels supply selectable portions of the area, and the mapping of geographical area to each pixel means the outline shape and zone correspond to a real-world geographical area. Staton also describes the coordinate-mapping operation: "[T]he data representative of each geographical zone is a plurality of coordinates.... Mapping the coordinates on a pixelated image so as to assign one pixel to each coordinate ... connecting the

plurality of assigned pixels with lines forming a contiguous and connected line that encloses an area in the pixelated image, and activating the pixels that lie on the lines in order to form a contiguous array of pixels that enclose a shape in the pixilated image." *Id.,* 2:53-65. Finally, Staton states that "the entering or leaving a geographical area that has been geofenced can be an event itself." *Id.,* 14:1-3. That confirms that the generated boundary is used as an operative geofence for monitoring movement relative to the geographical area. Because the same processing device builds the zone from the supervisor-selected area as shaped by the security parameters analyzed under limitation 1[c], the geofence is generated "based on the analyzing." Thus, Staton meets "generating, using the processing device, a geofence corresponding to a geographical area based on the analyzing," and limitation 1[d] is disclosed.

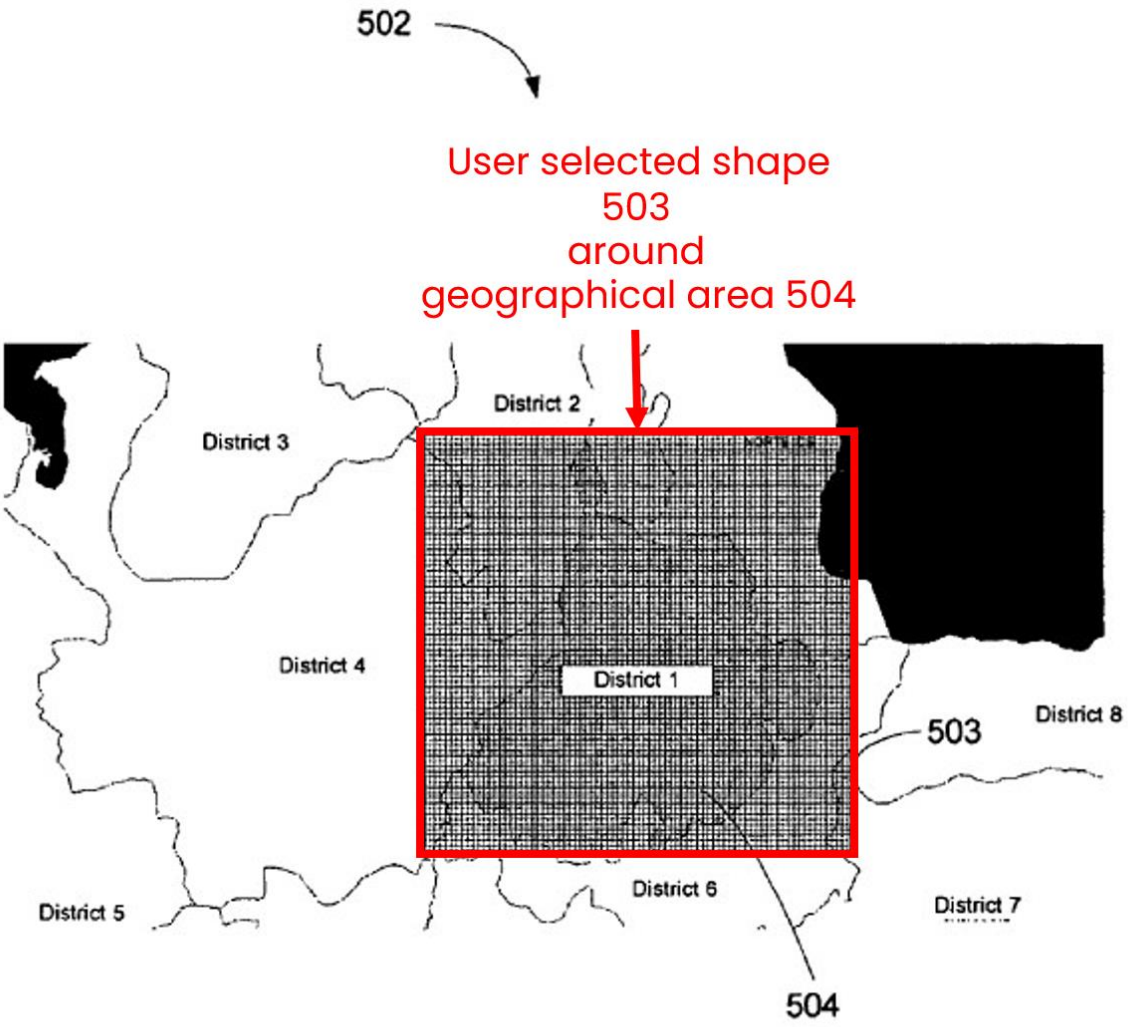


FIG. 5A

RAVE/MSI, EX1005, p. 115

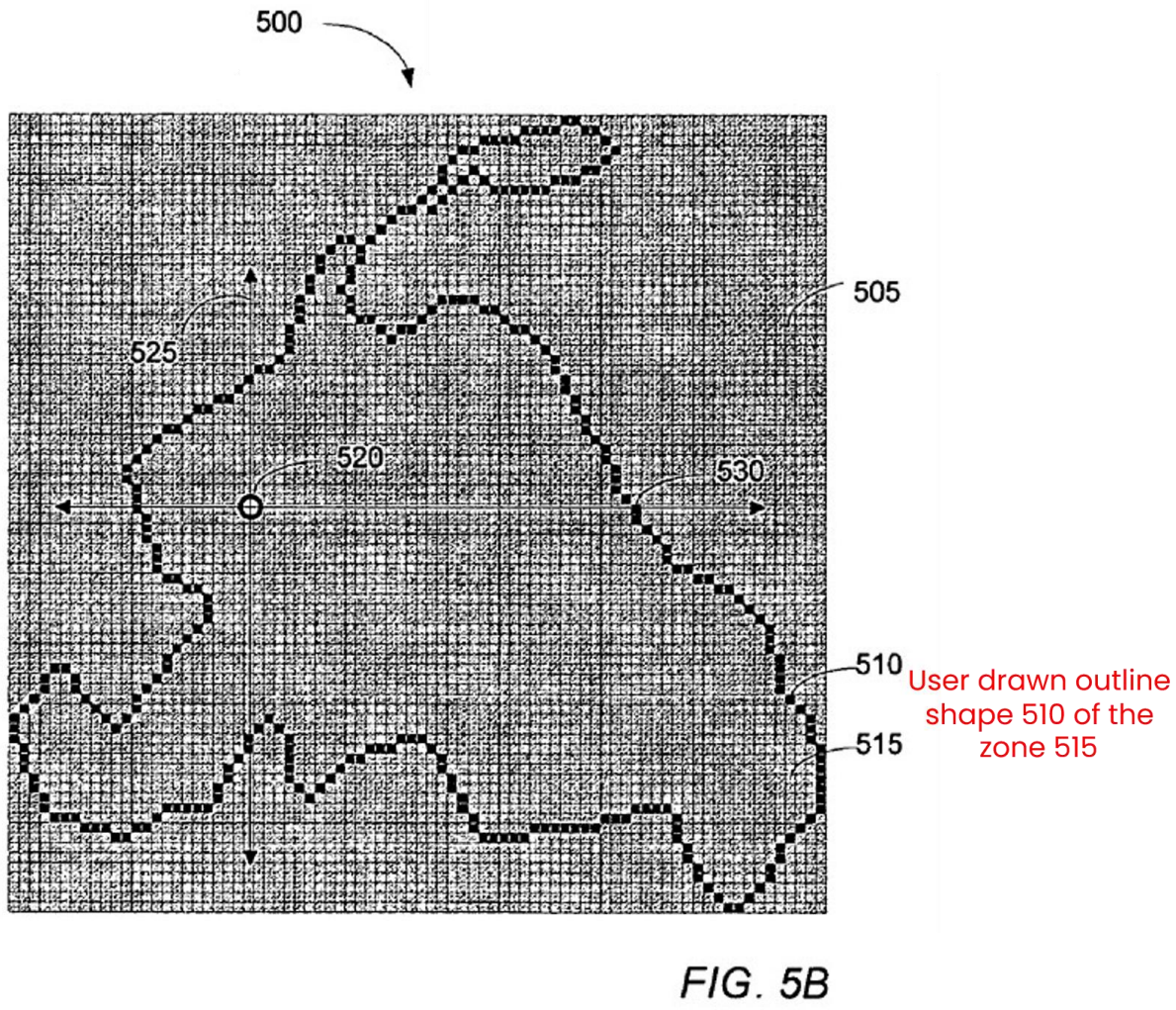


FIG. 5B

Ex.1007, Figs. 5A, 5B (annotated).

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

172. For limitation 1[e], the communication device is the same as limitation 1[a], and the supervisee device = the device carried by/associated with the monitored individual (the supervisee), e.g., PDA 105, with PDA 108 included in the family example. The at least one supervisee data = the geocoded location and event messages and other information transmitted from the supervisee device to the

communication device. For example, because PDA 105 is carried by the monitored individual, that location and event information is data associated with the supervisee. Staton states: "PDAs 105, 106 and 107 send event information to backend control system 150 and respond to commands sent to each of the PDAs by the backend control system 150 through the communications network." Ex.1007, 7:1-7. This identifies the communication path from the supervisee device to the backend and shows that the backend receives event information generated by the monitored devices. The data comes from the device carried by the monitored individual and describes that individual's monitored events.

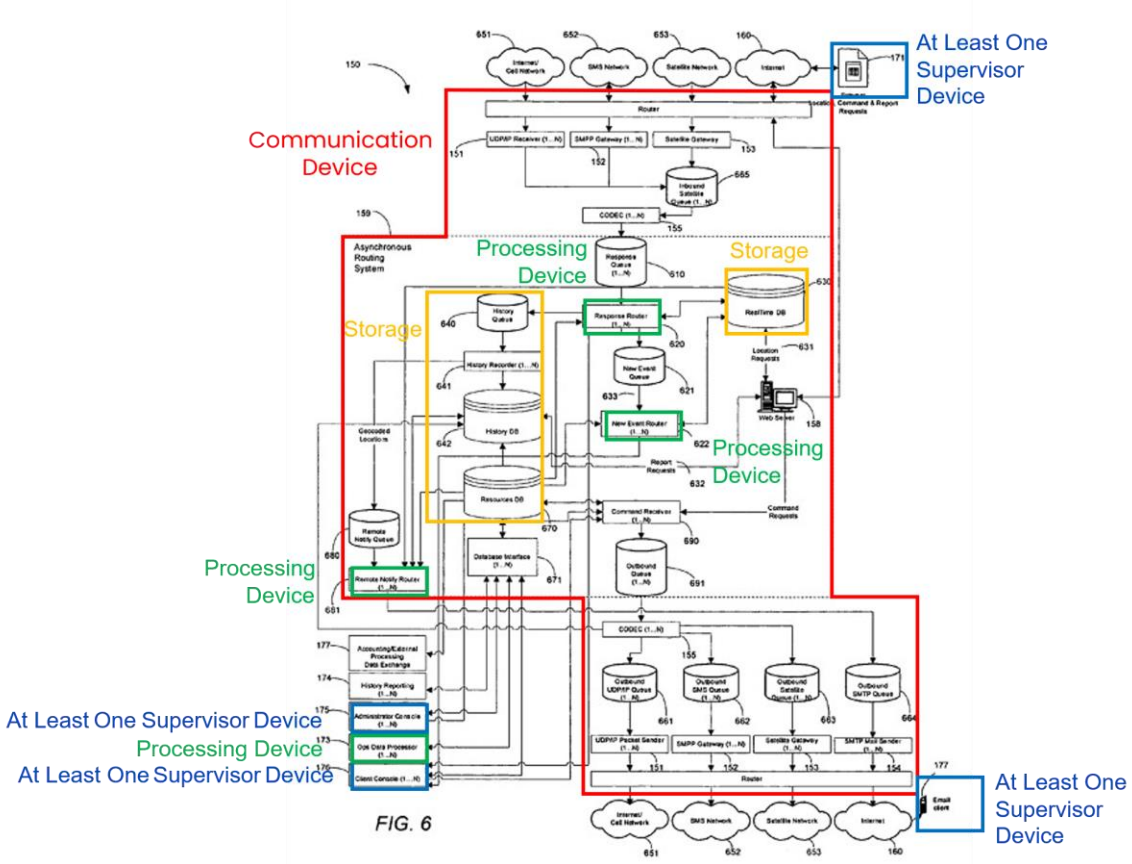
173. Staton states: "The PDA 105 communicates with the one of a plurality of base stations 120, which in turn communicates with the service provider 135. The backend control system 150 receives the communication signals from the service provider 135 and maps the correct destination if any." Ex.1007, 8:14-19. This shows the backend receiving the supervisee device's transmission through the communications network. Staton further states that event messages "can include latitude, longitude, speed, direction, time, state of the inputs, odometer, event reason or source, and any other relevant information." *Id.,* 16:18-23. Latitude and longitude identify the monitored individual's location; speed and direction describe movement; and time, input state, odometer, and event reason describe the

individual's circumstances and the event that prompted the transmission. These are therefore data associated with the supervisee.

174. Staton states: "PDA 106 can receive information related to PDA 105 if PDA 106 is listed as a monitored PDA. The backend control system 150 reroutes an event message, text message or any other information originating from PDA 105 to PDA 106." Ex.1007, 8:19-25. This disclosure confirms that the backend receives information originating from PDA 105 before the information is rerouted to the supervisor device. Functionally, the backend receives the monitored individual's location and event information from the PDA carried by that individual, which is an example of supervisee data associated with a supervisee. Thus, limitation 1[e], "receiving ... at least one supervisee data associated with a supervisee from at least one supervisee device," is disclosed. *Id.,* 16:18-31, 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;"***

175. For limitation 1[f], the processing device is the same as limitation 1[c]. I provide two independent theories for how Staton analyzes supervisee data based on the geofence, followed by an alternative obviousness analysis.



Ex.1007, Fig. 6 (annotated).

176. (1) Under the remote notify router 681 theory, history recorder 641 geocodes packets with valid latitude and longitude and places the geocoded locations and event-message information in remote notify queue 680. Staton states: "the history recorder 641 also transmits the geocoded locations and event message information to remote notify routers 681 by placing the geocoded locations in a remote notify queue 680. The remote notify router 681 that receives the geocoded location and event information queries the resources database 670 to find out if the configuration information or event information received requires a notification to a PDA 105, the instrument module 195 or communications device 177." Ex.1007,

22:18-35. The input is thus the supervisee's geocoded location and event information. The router then evaluates that input against the stored configuration and event information and determines whether the result requires a notification, which is an analysis rather than mere message forwarding.

177. This is analysis "based on the geofence." Staton states: "[v]arious events can be configured based on 'geofencing' events." Ex.1007, 13:65-66. This identifies the incoming event information as information generated under a geofence-based event rule. Staton further states: "Geofencing entails creating configurable boundaries or geographical zones in which a PDA 105 operates," and "the entering or leaving a geographical area that has been geofenced can be an event itself." *Id.* 13:66-14:4. The incoming event information is therefore geofence-originated when it records entry into or exit from the geofenced area. Staton also states that "[a]n event related to a geographical zone can trigger communication from one PDA to another." Ex.1007, 14:12-13. This confirms that the router's notification inquiry is tied to the geographical-zone event. Remote notify router 681 evaluates that geocode and event information against the configuration information and event rules stored in the backend, which are among the settings and parameters included in the geofence under the construction applied here. Thus, the router analyzes supervisee data based on the geofence, and limitation 1[f] is disclosed under theory (1). *Id.,* 22:18-35.

178. (2) Under the response router 620 theory, response queue 610 feeds packets to response router 620. Staton states: "The response queue 610 feeds the packets to the response router 620. The response router 620 determines if a client console 176 is tracking PDA 105 or the instrument module 195 associated with the incoming message. If so, the response router 620 routes the incoming message to the appropriate client console 176. Thus, the client console 176 receives the message before any other process in the asynchronous routing system 159. If no client console 176 is tracking the PDA 105 or the instrument module 195 associated with the incoming message, the response router 620 places the incoming message into a new event queue 621." Ex.1007, 21:45-60. The response queue supplies the incoming supervisee message, response router 620 performs the tracking determination, and the router either sends the message to the tracking console or places it in the new-event queue. The decision whether to route the message depends on the console's monitoring relationship to the incoming supervisee PDA.

179. This second pathway is also analysis "based on the geofence." Staton states that client console 176 provides "real-time PDA location mapping, location tracking, PDA control and PDA message/event handling," and that "the client console 176 allows a user to view all PDAs that are within a waypoint" and "allows a user to view all PDAs that are within a geographical zone." Ex.1007, 17:30-33, 17:48-52. The first disclosure identifies the console's tracking function, while the

RAVE/MSI, EX1005, p. 121

second identifies the geographic reference used for that tracking. Accordingly, determining whether the console is tracking the incoming supervisee PDA is a geofence-specific analysis: the console tracks PDAs by waypoint and geographical zone, so the response router's routing decision is made by reference to the geofence. Under theory (2), Staton meets "analyzing, using the processing device, the at least one supervisee data based on the geofence." *Id.,* 21:47-51.

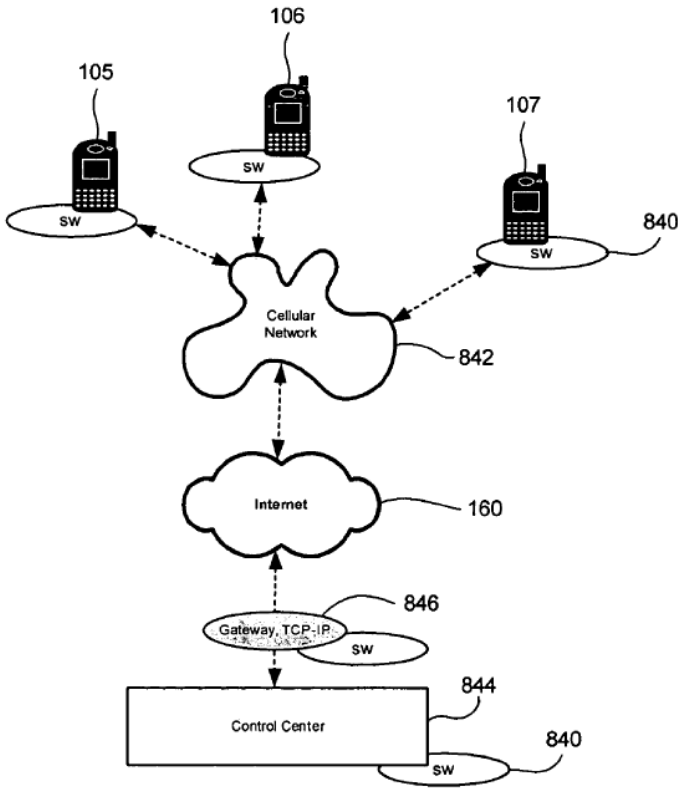


FIG. 8A

Ex.1007, Fig. 8A.

180. To the extent Patent Owner contends that limitation 1[f] requires the processing device to compare the supervisee's real-time location with the geofence boundary, I disagree that is required but have considered that position separately. Staton discloses that PDA 105 performs this comparison: "The PDA 105 can be programmed to determine the position of the entity with a simple calculation of whether the pixel in which the PDA's location falls is activated or deactivated." Ex.1007, 16:6-9. Staton also states: "A geofencing software 840 loaded on the PDA 105, 106 and 107 can be configure[d] to determine whether the PDA is inside or outside a geographical zone or a plurality of geographical zones. The geofencing software utilizes GPS data, geographical zones loaded on the PDA, and preconfigured event data to analyze if a entering or leaving a zone is an event in itself." *Id.,* 26:44-50. Staton discloses the real-time boundary comparison at the PDA, but is silent as to whether the server-side processing components also perform that comparison. It would have been obvious for the server to perform the comparison too.

181. First, a POSITA would have found server-side comparison useful because the supervisee's real-time location information is already reported to backend control system 150. Staton states: "The PDA 105 communicates with the one of a plurality of base stations 120, which in turn communicates with the service provider 135. The backend control system 150 receives the communication signals

from the service provider 135 and maps the correct destination if any." Ex.1007, 8:14-19. The server therefore already receives the location-bearing input; adding a comparison against the stored geofence would use an input already present at the point where routing and notification decisions are made.

182. Second, a POSITA would have found the modification straightforward because the server already possesses the second input required for the comparison: the geofence representation. Geofences are generated through operations data processor 173 and configuration utility 172. Staton states: "Waypoints and zones are built by the operations data processor 173. These loads are loaded on to the PDAs with the configuration utility 172." Ex.1007, 15:4-9. Thus, the server-side processing components have both the supervisee's location data and the geofence representation needed to determine inside-or-outside status, so no new source of either input would be required.

183. Third, a POSITA would have considered server-side comparison a known architectural alternative because Staton's backend already performs processing and analysis of messages at the control center before identifying the final recipient. The backend also maintains real-time location information and performs routing and event processing. Moving the same location-to-zone comparison into that existing processing path would keep the comparison close to the data and

notification decision rather than requiring a separate exchange between the PDA and server. Ex.1007, 26:47-61, 19:50-20:3, 21:47-22:3.

184. Fourth, a POSITA would have expected the modification to succeed because Staton places the same geofencing software 840 at the control center as on the PDAs. Staton identifies "the control center 844 where the geofencing software 840 also exists." Ex.1007, 26:52-61. Staton states: "At the control center, the message is processed and analyzed to find out the final recipient." *Id.,* 26:63-65; FIG. 8A. The first disclosure supplies the existing server-side geofencing capability, and the second identifies the control center as a location where message analysis already occurs. The proposed modification therefore would not require developing a new geofencing algorithm; it would invoke the existing comparison logic at the control center using the location and zone data already available there.

185. Fifth, a POSITA would have recognized a reliability benefit from server-side comparison because an independent comparison could cross-check the PDA's determination using the same coordinate and pixel-map information. That second determination would provide a backend check on an erroneous device result or a failed device-side event determination before the system sends a notification. Ex.1007, 16:6-9, 26:44-50.

186. Sixth, a POSITA would have recognized that server-side comparison would support monitoring interfaces or client devices that lack the processing power

or memory to perform the pixel-map or boundary calculation themselves. Staton already contemplates multiple monitoring interfaces, including websites, applications, client consoles, and other user interfaces, while centralizing routing, databases, and event processing in backend control system 150. Performing the comparison centrally would allow those interfaces to receive a completed location-status result without duplicating the geofence calculation in each interface. Ex.1007, 17:26-33, 26:24-34.

187. Seventh, moving continuous comparison to the server would conserve battery power on PDA 105 because repeated comparison of current GPS positions against a pixel map or boundary is a recurring computation on a portable device, whereas the backend is continuously powered for routing and event processing. Staton states that "environment device information can be presented to an operator through a website or an email by transmitting such information from a web server 158 to a web client 171." Ex.1007, 7:34-45. That disclosure confirms Staton's use of the web server to centralize presentation of device information, making server-side handling of the recurring comparison a predictable extension of the same architecture.

188. Finally, in my opinion, selecting the server, the client, or both to perform the comparison of the supervisee's location with the geofence boundary would have been a routine design choice well understood by a POSITA as of the

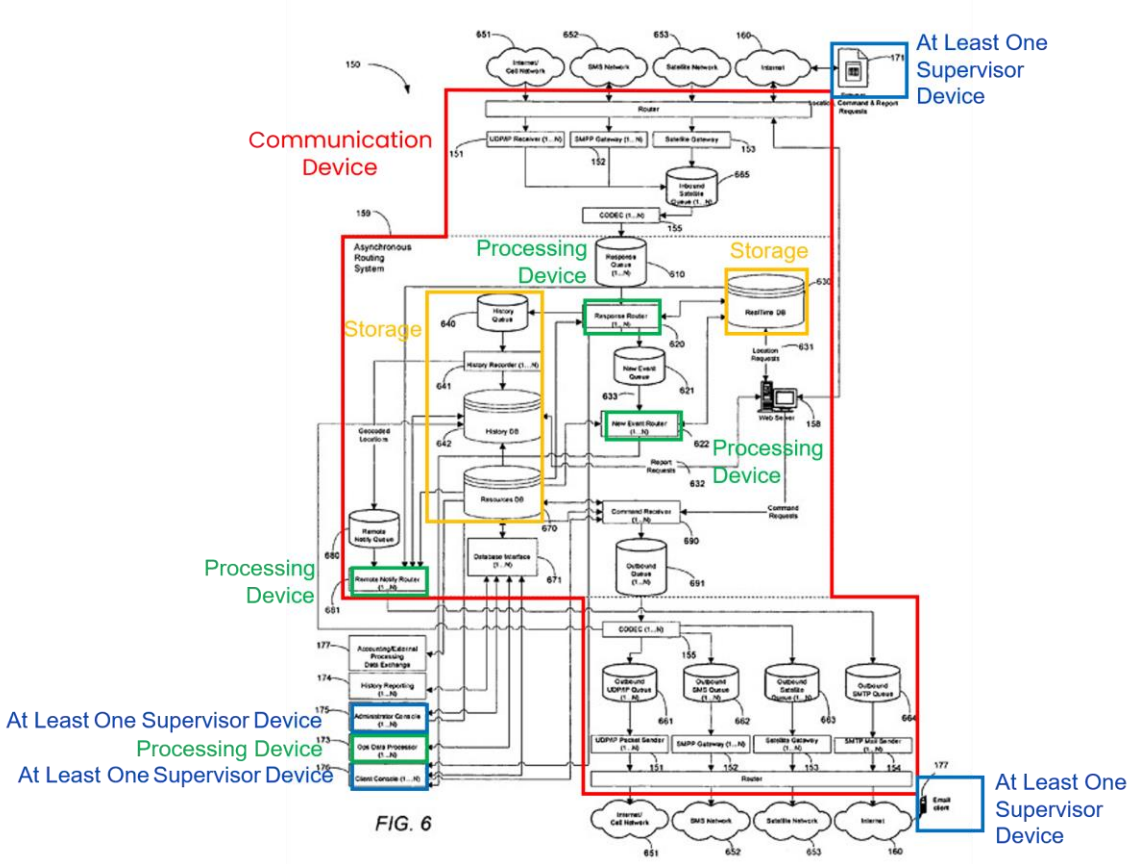
priority date. The '757 Patent itself reflects that allocation: it states that "one or more steps of the method may be performed by a server computer" and that "[s]imilarly, one or more steps of the method may be performed by a client computer." Ex.1001, 9:60-62. It further states that "[t]he server computer may include a processing device configured for performing data processing tasks such as, for example, but not limited to, analyzing, identifying, determining, generating," *id.,* 6:56-59, and, specific to the analysis at issue here, that "the server 4108, in an instance, may be configured to analyze the location data." *Id.,* 26:40-41. A POSITA would therefore have regarded performance of the location-to-geofence comparison at the server, at the client, or at both as an ordinary implementation choice rather than a technical obstacle.

189. I would have expected the modification to succeed because the location information is already reported to backend control system 150, the geofence and its coordinate or pixel-map representation are generated and maintained by the server-side configuration components, and the control center already has geofencing software 840. The modification therefore applies existing comparison logic to inputs already available in the same server architecture. Under this alternative obviousness rationale, the server-side processing device would analyze the supervisee data based on the geofence, and limitation 1[f] is disclosed. Ex.1007, 8:14-25, 15:4-9, 16:43-61, 26:63-65.

190. This server-side comparison rationale applies equally to limitations 1[g] and 1[h] and to the corresponding analysis in claim 2.

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

191. For limitation 1[g], the processing device is the same as 1[c]. (1) Under the remote notify router theory, after determining that notification is required, Staton states: "If a notification is required, the remote notify router 681 retrieves the contact information for the appropriate PDA 105, the instrument module 195 or the communications device 177. The remote notify router 681 then formats and encodes the message sent to the PDA 105, the instrument module 195 or the communications device 177." Ex.1007, 22:18-35. Formatting and encoding a message for a selected recipient generates a new outbound message addressed for that recipient from the inbound supervisee event data. That is "generating ... a supervision notification."



Ex.1007, Fig. 6 (annotated).

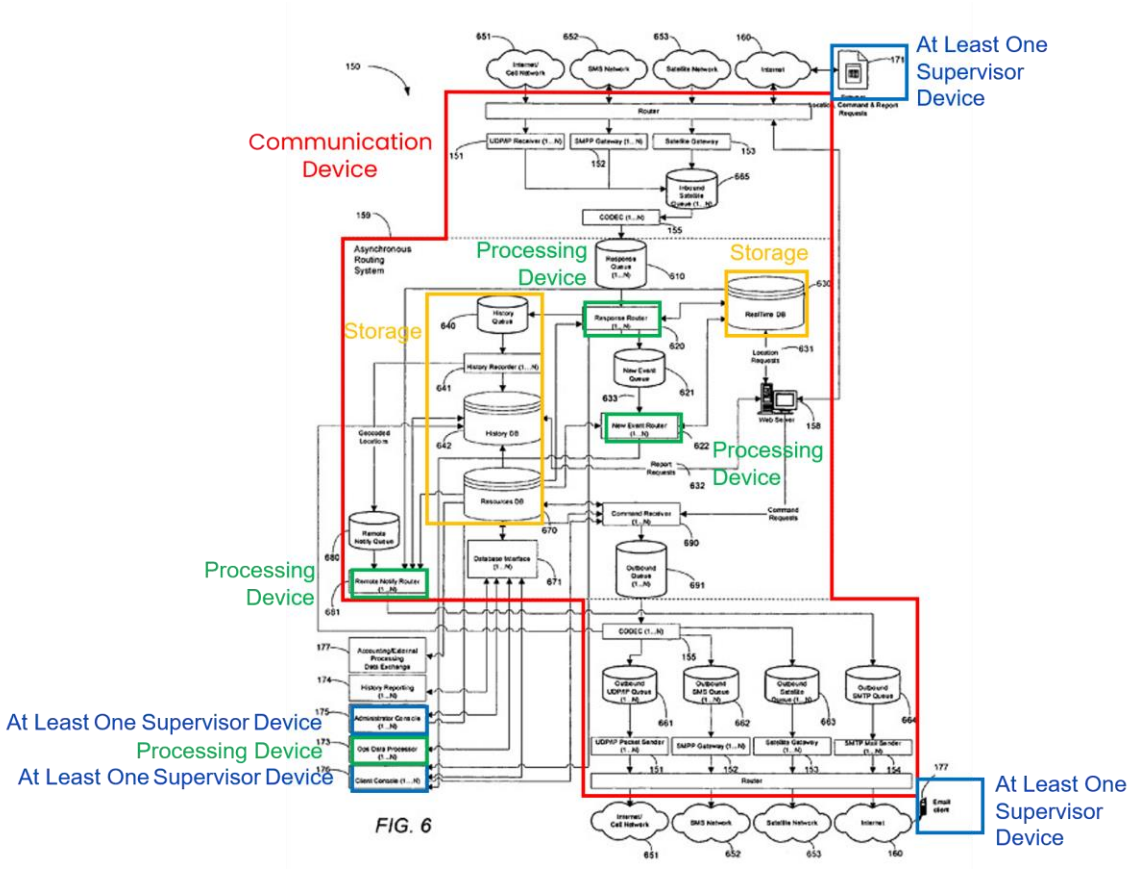
192. The notification is based on the analysis because the remote notify router 681 generates and formats it only after querying resources database 670 to determine whether the received configuration or event information requires a notification. Ex.1007, 22:18-35. Staton further explains that "the control center looks up the correct PDAs to contact in the resources database 670 and any other parties that must be contacted, such as the police or 911." *Id.,* 26:62-27:3. The lookup supplies the recipient and the preceding determination supplies the condition for generating the outbound message.

193. (2) Under the response router theory, after determining that client console 176 is tracking the supervisee PDA, Staton states that "the response router 620 routes the incoming message to the appropriate client console 176." Ex.1007, 21:47-51. The client console receives information enabling "real-time PDA location mapping, location tracking, PDA control and PDA message/event handling," and allows a user to view all PDAs "within a waypoint" or "within a geographical zone." *Id.,* 17:30-33, 17:48-52. The response router's routing decision therefore creates the notification that reaches the supervisor's tracking console: it selects the recipient based on the tracking determination and delivers the event message in the form the console uses for location mapping, tracking, and event handling.

194. This notification is based on the analyzing of supervisee data because, as Staton states, "the response router 620 routes the incoming message to the appropriate client console 176" and "the client console 176 receives the message." Ex.1007, 21:47-53. The router performs that routing only after determining that the console is tracking the incoming supervisee PDA in relation to a waypoint or geographical zone. *Id.,* 17:30-33, 17:48-52. Staton meets "generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data," and limitation 1[g] is disclosed.

i. 1[h]: "transmitting, using the communication device, the supervision notification to the at least one supervisor device; and"

195. For limitation 1[h], the communication device is the same as limitation 1[a]. (1) After remote notify router 681 generates the notification, Staton states: "The message is placed in the outbound SMTP queue 664 to be sent through the SMTP gateway 154. The message can be placed in the outbound SMS queue 662 to be sent through the SMPP gateway 152." Ex.1007, 22:28-36. The gateways are part of the communication device, and transmit the generated message to the selected supervisor device.



Ex.1007, Fig. 6 (annotated).

196. Staton confirms the resulting transmission by stating: "The backend control system 150 reroutes an event message, text message or any other information originating from PDA 105 to PDA 106." Ex.1007, 8:19-25. This confirms that the backend reroutes information originating from the supervisee device to PDA 106, the supervisor device. In the worksite example, "PDA 108 notifies a backend control system 150, which in turn notifies PDA 107 of the arrival." *Id.,* 29:55-57. This likewise confirms that a backend-received event is transmitted onward to another monitoring PDA, so the notification reaches a supervisor device.

197. (2) Under the response router theory, response router 620 transmits the notification using the communication components of backend control system 150 to the appropriate client console 176. Staton states: "Thus, the client console 176 receives the message." Ex.1007, 21:49-51. This is the claimed transmission to a supervisor device because the client console is the supervisor-facing recipient, and the routing is geofence-specific because the console tracks PDAs within a waypoint or geographical zone. Accordingly, Staton meets "transmitting, using the communication device, the supervision notification to the at least one supervisor device," and limitation 1[h] is disclosed under either theory. *Id.,* 17:30-33, 17:48-52.

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

198. For limitation 1[i], the storage device = history recorder 641, history database 642, and associated storage infrastructure (e.g., history queue 640 and resources database 670). Staton states: "[a]synchronously, a history queue 640 receives the inbound and outbound messages for all PDAs 105 and all of the messages from the instrument module 195." Ex.1007, 22:5-7. The inbound messages include the supervisee data received from PDA 105, and the outbound messages include the supervision notifications generated or routed to supervisor devices. Staton further states: "[t]he history recorder 641 geocodes all packets that have a valid latitude and longitude. The geocoded information is saved in a history database 641 to be used later for reporting and statistical analysis." *Id.,* 22:7-12. Geocoding and saving the location-bearing packets preserve the supervisee's geographic data in a form usable for later reporting and analysis. Staton also states: "Furthermore, the history recorder 641 timestamps all the incoming messages and tags them as being from either PDA 105 or the instrument module 195." Ex.1007, 22:12-15. Timestamping and tagging identify the source and timing of the stored data, confirming that the system stores supervisee-specific information.

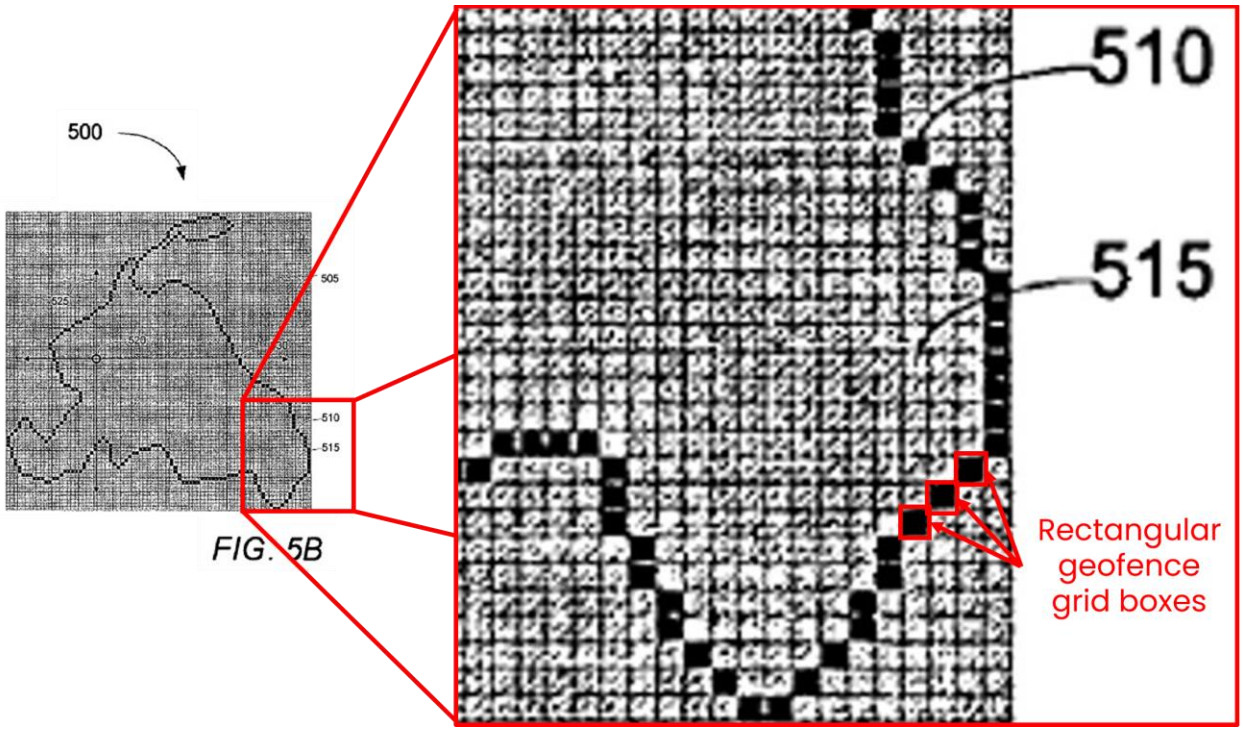
199. The history database 642 maintains records of events and transactions received and sent from asynchronous routing system 159. This stores the inbound

supervisee events and outbound supervision notifications as system transactions. Staton states: "the real time database 630 can maintain records of the most recent information from a PDA such as location, speed, direction, associated instruments, associated geographical zones, etc." Ex.1007, 19:50-20:3. This stores the current supervisee data and its relationship to the relevant zones. Staton further states: "The history database 642 maintains records of all events and transactions that were received and sent from the asynchronous routing system 159." *Id.,* 19:56-59. This independently confirms storage of both directions of message traffic, received supervisee data and sent supervision notifications. Finally, Staton states: "Finally, the resources database 670 keeps records of all the instrument modules and PDAs that are part of the system." *Id.,* 22:5-15. This supports the system's ability to associate the stored messages with the relevant supervisee and supervisor devices. The inbound messages are therefore the stored supervisee data, and the outbound messages are the stored supervision notifications. Staton meets "storing, using a storage device, the at least one supervisee data and the supervision notification," and limitation 1[i] is disclosed.

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:"***

200. For limitation 1[j], the geofence and the geofence area are the same as 1[d]; and the geofence grid boxes = the smaller rectangles into which selected rectangular shape 503 is divided, each mapped to a square pixel 505. Staton states: "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." Ex.1007, 3:10-12. This supplies the geofence area and the act of subdividing it into discrete sections. Staton further states: "[e]ach pixel 505 is a square." *Id.,* 15:27-34. Each square is a discrete grid subdivision that can represent a portion of the bounded geographical area. Staton also states: "These squares are then used to draw the outline shape 510 of the zone 515." *Id.,* 15:27-34. The activated squares collectively define the geofence boundary and therefore are associated with the geofence area. Finally, Staton states: "A geographical area is then mapped to each pixel 505 of the pixel map 500," and "Each pixel in the grid can be activated to be part of the geographical zone." *Id.,* 16:47-52. The first disclosure assigns a portion of the real-world area to each square, and the second identifies how selected/activated squares

form the zone. Each pixel or rectangle a discrete square subdivision of the bounded area to which a portion of the real-world geographical area is assigned.



Ex.1007, Fig. 5B (annotated).

201. Staton also states: "The pixilated computer image can be created by the steps of allowing a user to identify a geometrical zone in a computer map using two coordinate attributes, 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, and associating the at least one section to a pixel in a pixilated computer image such that the pixels selected by the user in the identified geometrical area are identified as being in the geographical zone. The grid can divided into a number of sections so as to achieve a high enough resolution to be able to correctly

delineate the geographical zone." Ex.1007, 3:6-18. This passage confirms the identified geometrical zone supplies the bounded area, the sections supply the discrete grid boxes, the pixel association supplies the digital representation, and the selected/activated sections define the geofence. Staton meets "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," and limitation 1[j] is disclosed.

202. Regarding this limitation, the Examiner erred. The Examiner's reasons for allowance rested on the conclusion that the prior art, including cited Staton '733, failed to disclose a geofence comprising geofence grid boxes. That conclusion was incorrect because the prosecution record did not substantively account for Staton '733's disclosed grid of rectangles and pixels, each representing a portion of the defined geographical area. The grid-box limitations were added to the independent claims by Examiner amendment, and the prosecution record does not show substantive consideration of the grid-box disclosures in Staton '733. Ex.1002, 213-225.

203. Staton '733 states: "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 the resolution of the area." Ex.1013, 13:60-14:8. Staton '733 also states: "Each selected rectangles is then mapped to a pixel." *Id.,* 14:14-16.

204. Staton '733 also states: "the pixilated computer image contains the same number of pixels as the number of sections in the grid." Ex.1013, 14:18-20; *id.,* 14:1-14.

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:"***

205. For limitation 1[j][1], the communication device and supervisor device are the same as 1[a], and the grid parameter = the user-selected "resolution of the area definition." Ex.1007, 15:46-55 ("The home computer connects to the configuration utility….The user can also select the resolution of the area definition…."). Staton receives that input through the same pathway described for limitations 1[a] and 1[b]. Because the resolution is supplied by the user who configures the geographical area, it is a supervisor-supplied value, and because it travels through the backend communication infrastructure to the configuration

functions, it is received using the communication device. Ex.1007, 15:17-23, 15:46-55; see the receiving-pathway discussion for limitations 1[a] and 1[b] above.

206. Staton states: "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 the resolution of the area." Ex.1007, 15:46-55. This disclosure shows that resolution fixes the number of subdivision lines and therefore controls both the number and the size of the resulting grid rectangles. Resolution is therefore a "grid parameter."

207. The resolution is a grid parameter because it determines how many vertical and horizontal lines subdivide the selected area and therefore determines the number and size of the resulting grid rectangles. Staton also states: "A zone can be defined by a plurality of waypoints.... A greater number of waypoints will increase the resolution of how the zone is defined. Thus if two waypoints are used, the resolution can be increased by adding ten extra waypoints that further define the delineation of the city boundary." Ex.1007, 14:34-44. Staton further teaches that the zones are configured by a supervisor, stating "[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. This resolution selection therefore occurs as a part of the supervisor-operated configuration software. Increasing the supervisor-selected detail increases the number of defining subdivisions. Thus, limitation 1[j][1], "receiving ... at least one grid parameter from the at least one supervisor device," is disclosed.

m. ***1[j][2]: "analyzing, using the processing device, the at least one grid parameter;"***

208. For limitation 1[j][2], the processing device is the same as in 1[c]. Those components analyze the grid parameter by applying the selected resolution to the selected geographical area. Staton states: "The rectangular shape is then divided into smaller rectangles such that the area of the rectangle is divided into a grid." Ex.1007, 15:31-34. The processing device evaluates the selected resolution to determine how finely the selected area is subdivided, so this is "analyzing ... the at least one grid parameter."

209. Staton explains the relationship: "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 the resolution of the area." Ex.1007, 15:51-55. This disclosure shows what the processing device does with the parameter: it evaluates

the selected resolution to determine how finely to subdivide the selected area and how much area each resulting rectangle covers. Staton states: "An increased resolution of the area can allow a user, for example, to define the geographical area of a house, where the geographical area covered is much smaller than that for a state. The perimeter around the geographical area of the house can have details that can only be identified by very high resolution. On the other hand, a user who is concerned with roughly knowing that a state has been entered does not need great resolution of the state area. Therefore, the resolution necessitated to define the area of a state can be configured to be low." Ex.1007, 15:56-65. This illustration confirms that the analysis selects finer or coarser subdivision based on the geographic detail needed for the selected area. Limitation 1[j][2], "analyzing ... the at least one grid parameter," is disclosed.

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"***

210. For limitation 1[j][3], the processing device is the same as limitation 1[c].

211. The system performs the disclosed mapping using the processing device by determining how much geographical area each pixel, and thus each grid box, represents. For example, Staton states: "the pixilated computer image contains the same number of pixels as the number of sections in the grid," and "[a]

geographical area is then mapped to each pixel 505 of the pixel map 500." Ex.1007, 15:46-55, 16:2-4, 16:51-52; Ex.1013, 14:18-20, 14:25-27. The first disclosure establishes the one-to-one correspondence between grid sections and pixels, and the second assigns geographical area to each pixel.

212. Staton also makes the box size user-configurable through the selected resolution. Staton states: "A zone can be defined by a plurality of waypoints.... A greater number of waypoints will increase the resolution of how the zone is defined. Thus, if two waypoints are used, the resolution can be increased by adding ten extra waypoints that further define the delineation of the city boundary." Ex.1007, 14:34-44,

213. Staton also states: "The increase in number of rectangles increases the resolution because each rectangle covers less geographical area." Ex.1007, 15:50-55. Therefore, the same selected location can be represented by differing numbers of boxes, with each box covering a different amount of area. Finally, assigning a geographical area to each grid box is required by the pixel-map operation, so the system can determine the area assigned to each box in order to execute that assignment. The configurable grid translates resolution into a usable geographic representation for boundary and location calculations.

214. In arithmetic terms, the grid box geofence area is the total selected geographical area divided by the number of grid sections dictated by the resolution

parameter. A higher resolution means that each rectangle is determined to cover less area, while a lower resolution means that each rectangle is determined to cover more area. Thus, limitation 1[j][3], "determining ... the grid box geofence area based on the analyzing of the at least one grid parameter," is disclosed. Ex.1007, 15:46-55.

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

215. For limitation 1[j][4], the processing device is the same as limitation 1[c]. Staton states: "The rectangular shape is then divided into smaller rectangles such that the area of the rectangle is divided into a grid." Ex.1007, 15:31-34. Dividing the selected shape into those smaller rectangles generates the discrete grid boxes corresponding to the geofence area.

216. For example, Staton divides the map into "an 80/80-pixel map" in which "[e]ach pixel 505 is a square." Ex.1007, 16:48-51. The square is therefore divided into 80 rows and 80 columns of square boxes, yielding 80 × 80 = 6,400 geofence grid boxes. Staton further states that "[t]hese squares are then used to draw the outline shape 510 of the zone 515." *Id.* The squares are the discrete units used to form the geofence boundary.

217. The number of boxes is based on the determining because Staton states: "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." Ex.1007, 15:46-65. Once the area per box is fixed by the resolution, the number of boxes needed to cover the selected area follows: higher resolution produces more rectangles covering less area, while lower resolution produces fewer rectangles covering more area. The processing device therefore generates the number of geofence grid boxes based on its determination of the grid box geofence area, and limitation 1[j][4], "generating ... a number of geofence grid boxes based on the determining," is disclosed.

RAVE/MSI, EX1005, p. 144

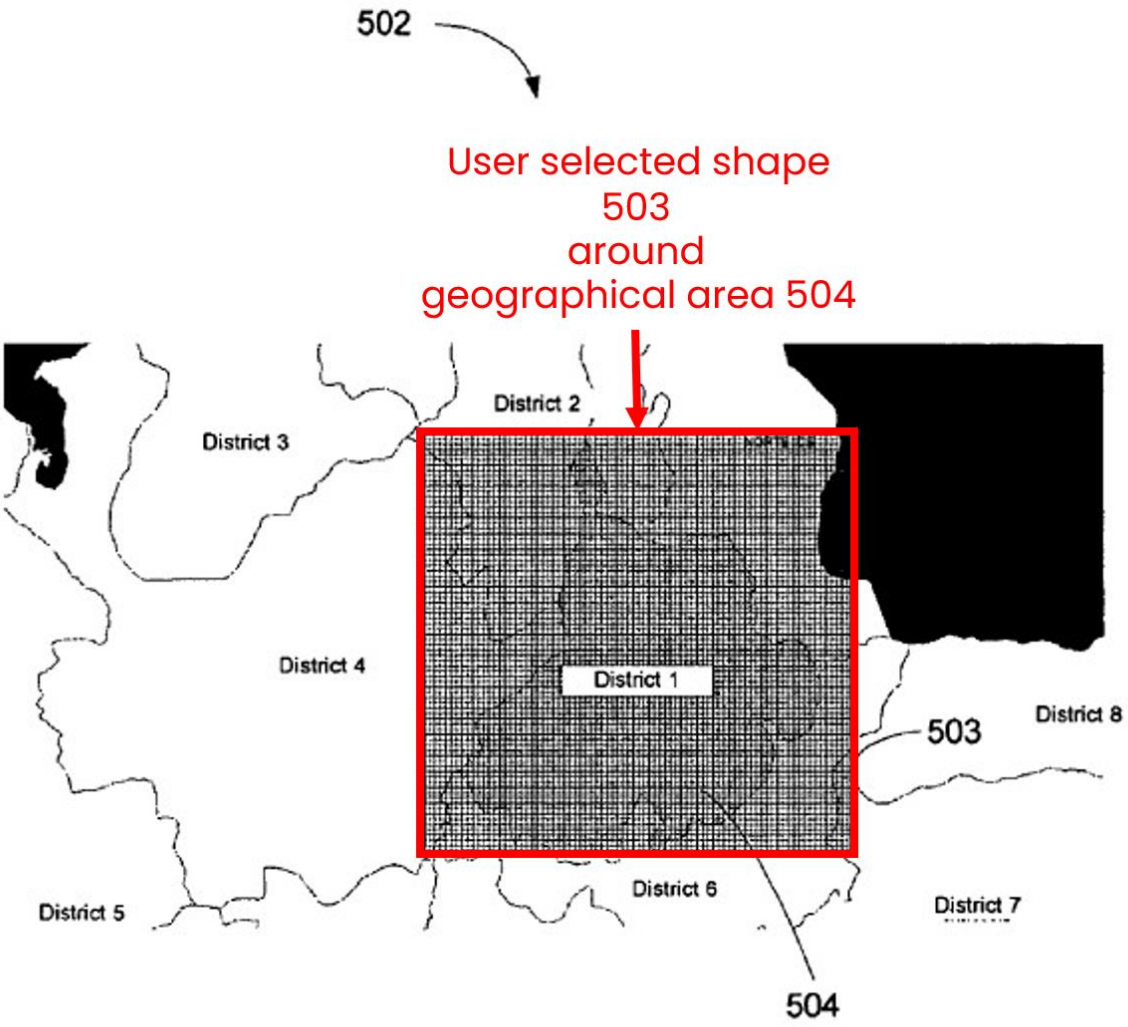


FIG. 5A

RAVE/MSI, EX1005, p. 145

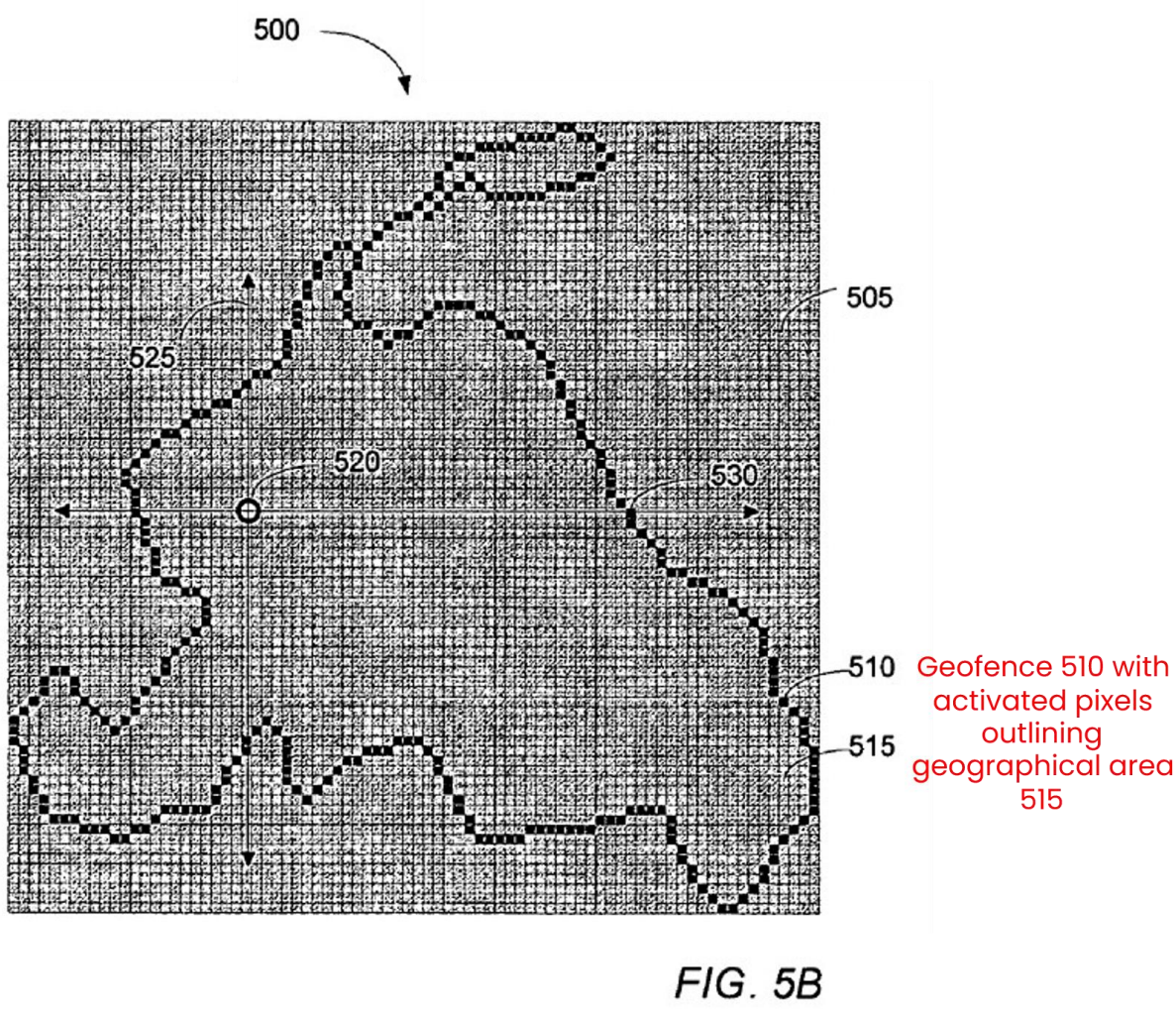


FIG. 5B

Ex.1007, Figs. 5A, 5B.

3. Claim 2

218. Staton discloses claim 2 for the reasons below. Ex.1007, 6:66-7:23, 15:4-9, 22:16-36.

a. ***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;"***

219. For limitation 2[a], I map the claimed "location indication associated with the geographical area" to the specific locations and areas that the supervisor designates within or associated with the broader geofenced area through Staton's configuration software. First, Staton explains that "[t]he parent may utilize the configuration software to delineate specific areas where the son can travel, and areas where the son cannot travel. For example, an area of non-permissible travel can be outside of city limits, or a particular area where there is known gang activity." Ex.1007, 27:52-57, *see also* 27:26-32, 28:52–56. This disclosure identifies both permissible and non-permissible locations selected by the supervisor. Each designated area is a specific location or set of locations within or related to the broader geographical area established in claim 1, and therefore is a "location indication associated with the geographical area." Second, Staton states that "[t]he daughter's PDA 108 could include the geographical area for an unsafe neighborhood and event alarms indicating that the unsafe neighborhood has been entered along with instructions on how to leave the dangerous neighborhood." *Id.,* 28:55-57. The unsafe neighborhood is another supervisor-designated location associated with the broader geofenced area, and the alarm rule confirms that the location is used for supervision. Third, Staton discloses that a "parent may configure regular paths of

travel from home to school and back" and that "if daughter's PDA 108 deviates from such predefined paths, PDA 108 sends a signal to PDA 106 indicating a warning of path deviation." *Id.,* 28:52-57. A predefined path is a set of locations associated with the same geographical area, so it likewise constitutes a "location indication associated with the geographical area."

220. Receiving occurs for the same reasons I described for limitation 1[a]. Staton states that "[t]he configuration of devices is entered through the backend control system 150 or any other portal host." Ex.1007, 25:60-62. Staton further states: "The schedule times, area boundaries, speed limits, and acceleration parameters are determined by the parents and can be changed at any time through the internet/cellular system." Ex.1007, 27:66-28:2; *see also id.,* 15:20-45. Thus, the backend communication components receive the permissible and non-permissible areas, unsafe-neighborhood designation, and predefined path from a supervisor device. The limitation requiring "receiving ... at least one location indication associated with the geographical area from the at least one supervisor device" is disclosed. Ex.1007, 25:60-62, 27:66-28:2.

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

221. For limitation 2[b], I map "identifying, using the processing device, at least one location corresponding to the at least one location indication" to the server-

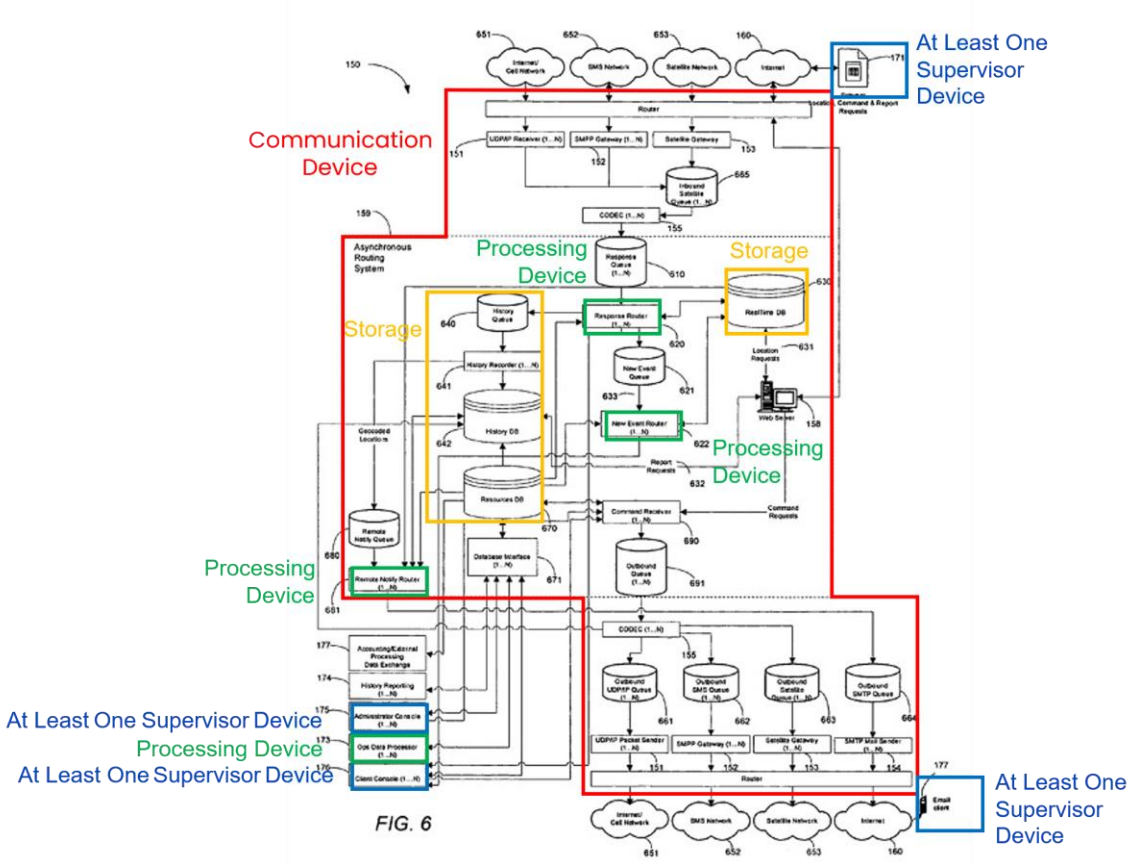
side translation of each supervisor designation into geographic data. Staton states: "Waypoints and zones are built by the operations data processor 173" and "[t]hese loads are loaded on to the PDAs with the configuration utility 172." Ex.1007, 15:4-9. The operations data processor therefore builds the corresponding zone, and the configuration utility receives the supervisor designated areas and prepares the location data for use by the devices. *Id.* 15:4-16:17. When the supervisor designates a non-permissible area or unsafe neighborhood, the processing device builds the corresponding zone with its coordinate data and pixel-map representation. When the supervisor configures a predefined path, the processing device identifies the route coordinates corresponding to that path. In each instance, the processing device translates the supervisor's designation into specific geographical coordinates or a corresponding zone representation that the system can use for monitoring. That translation is the claimed "identifying ... at least one location corresponding to the at least one location indication," and limitation 2[b] is disclosed. 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"***

222. For limitation 2[c], I address two theories, consistent with my analysis of limitation 1[f]. (1) Under the remote notify router 681 theory, Staton states: "When the PDA 105 enters or exits waypoints and zones, an event message can be

transmitted indicating what reference point or zone has been entered or exited." Ex.1007, 16:18-23. This event message is supervisee data generated by the supervisee's position relative to the identified location. Staton also states that, "if daughter's PDA 108 deviates from such predefined paths, PDA 108 sends a signal to PDA 106 indicating a warning of path deviation." *Id.,* 27:22-32. That signal is likewise generated from the supervisee's position relative to the identified path. The remote notify router then "queries the resources database 670 to find out if the configuration information or event information received requires a notification to a PDA 105, the instrument module 195 or communications device 177." *Id.,* 22:18-35. The event data is generated by the supervisee's position relative to the specific designated location, and the router evaluates that data to determine notification requirements. This is analysis of supervisee data "based on the at least one location."

RAVE/MSI, EX1005, p. 150



Ex.1007, Fig. 6 (annotated).

223. (2) Under the response router 620 theory, Staton states that the response router "determines if a client console 176 is tracking PDA 105 or the instrument module 195 associated with the incoming message." Ex.1007, 21:47-51. This determination analyzes the incoming supervisee data in relation to the location or zone being monitored by the client console. Staton further explains that the client console allows a user to view "all PDAs that are within a waypoint" or "that are within a geographical zone." Ex.1007, 17:48-52. The console's tracking relationship is therefore location-based, and the response router uses that relationship when deciding how to handle the incoming message. The message is evaluated against the

designated waypoint or zone that the console is tracking. Thus, under either theory, the processing device analyzes the supervisee data based on the identified location. Ex.1007, 17:48-52, 21:47-51.

224. If Patent Owner contends that limitation 2[c] requires the processing device on the server to specifically compare the supervisee's real-time location to the designated location, I reach the same conclusion stated for limitation 1[f]. Staton already supplies the supervisee's location data to backend control system 150, the operations data processor builds the designated locations, and geofencing software 840 exists at the control center as well as on the PDAs. A POSITA would have found it straightforward to apply that existing comparison logic at the backend, where the location data, designated locations, and event-processing infrastructure are already available; doing so would permit independent verification and would conserve processing and battery resources on the portable device. Thus, even under the narrower direct-comparison reading, the processing device analyzes the supervisee data based on the at least one location, and limitation 2[c] is disclosed. Ex.1007, 8:14-19, 15:4-9, 26:44-50.

RAVE/MSI, EX1005, p. 152

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."***

225. For limitation 2[d], I map "a location anomaly" to a path deviation or entry into a prohibited or unsafe area relative to the supervisor-designated locations. First, Staton discloses path deviation: "if daughter's PDA 108 deviates from such predefined paths, PDA 108 sends a signal to PDA 106 indicating a warning of path deviation." Ex.1007, 27:29-32. Departure from a predefined path is a location anomaly because the supervisee's location has departed from the expected locations indicated by that path. Second, Staton discloses entry into a prohibited or unsafe area: "[t]he daughter's PDA 108 could include the geographical area for an unsafe neighborhood and event alarms indicating that the unsafe neighborhood has been entered." *Id.,* 28:55-57. Presence in a designated area that the supervisee is not supposed to enter is anomalous relative to the supervisor's expectations. Third, Staton discloses departure from an area where the supervisee is supposed to remain. Staton explains that "[t]he properties of a zone include a name, description and a flag determining if the zone is an off-limits zone or an enclosed zone." *Id.,* 14:53-55. An enclosed-zone flag identifies an area in which the supervisee is expected to remain. Staton also states that "[e]xemplary events can be configured such as Zone Boundary Enter 435, Zone Boundary Exit 436, and Smart Time reporting 437 or

Scheduled Time reporting 438." *Id.,* 11:49-52. The Zone Boundary Exit event identifies the supervisee's departure from that enclosed or permissible area. In addition, Staton describes a PDA 105 "configured with a geographical zone 810 around the perimeter of the house 190, effectively geofencing the house. If PDA 105 leaves the area, an event is immediately sent to PDA 106 reporting that presumably the elderly parent has exited the premises of the house and is wandering in the neighborhood." *Id.,* 28:8-17. Exiting a designated safe area is a location anomaly because the supervisee has departed from the area in which the supervisor expects the supervisee to remain.

226. Further, "the generating of the supervision notification is based on the determining." Staton states that the remote notify router "then formats and encodes the message sent to the PDA 105, the instrument module 195 or the communications device 177" after evaluating the received location and event information. Ex.1007, 22:28-36. The formatting and encoding occur after the system determines that the event requires notification, so the anomaly determination supplies the trigger for generating the notification. Staton separately states that the response router routes the incoming message to the appropriate client console when the console is tracking the relevant PDA. Ex.1007, 21:47-51. That routing is likewise performed after the location-based event is evaluated. The detection of path deviation, prohibited-area entry, or safe-area exit therefore triggers notification generation through the same

remote-notify and response-router pathways established for limitations 1[g] and 1[h]. The limitation requiring "determining ... a location anomaly" with notification generation "based on the determining" is disclosed. Ex.1007, 21:47-51, 22:28-36.

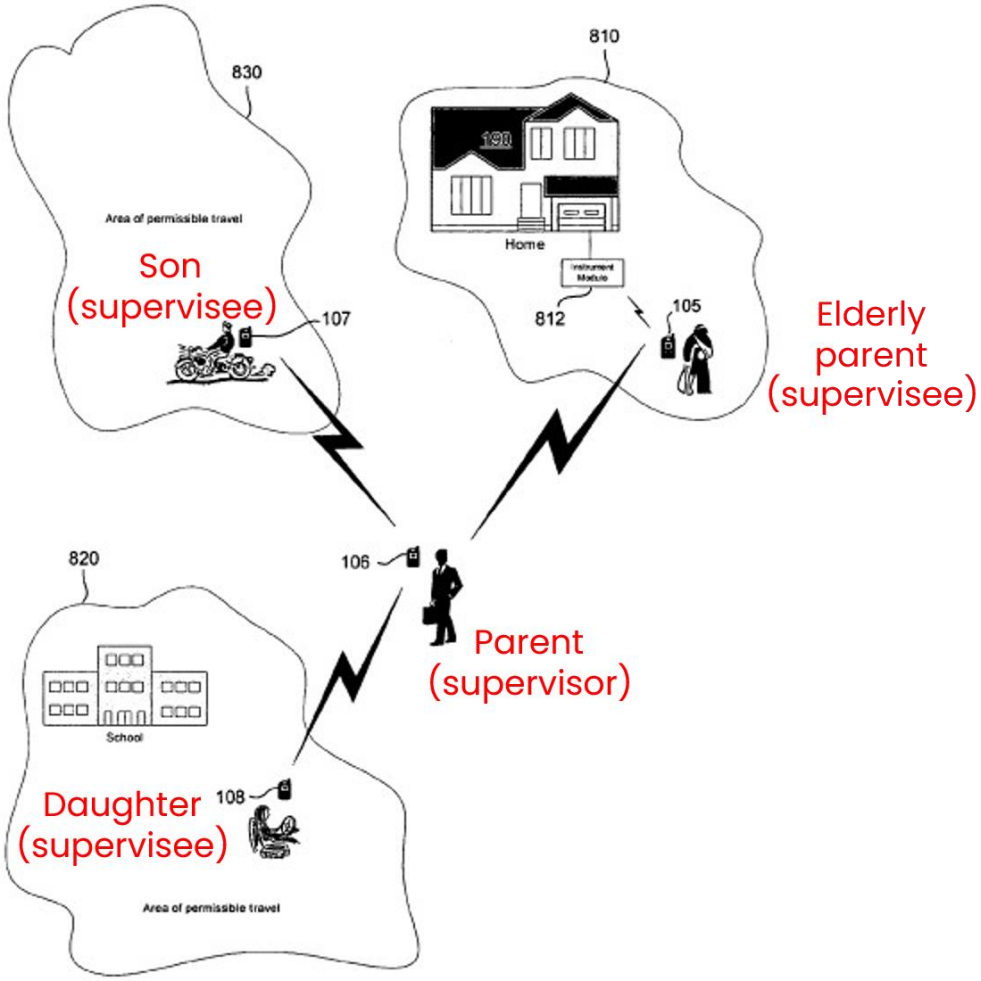


FIG. 8B

Ex.1007, Fig. 8B.

4. Claim 3

a. ***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:"***

227. For limitation 3[a], the supervision notification comprises event information generated by the supervisee device. Staton states that an event message can include "latitude, longitude, speed, direction, time, state of the inputs, odometer, event reason or source, and any other relevant information." Ex.1007, 16:18-23. Because those contents describe the supervisee's location, movement, device state, and event, the supervision notification comprises at least one "supervisee event." Staton also states that "[t]he waypoint and zone events are configurable to take one or more actions." Ex.1007, 16:31-33. This associates the event with a responsive action. Staton gives examples of those actions as "making a telephone call, reporting to a control center, starting an alarm." *Id*., 3:19-21. These disclosures show that the event is tied to configurable system conduct. Thus, the supervision notification "comprises at least one supervisee event" that "is associated with at least one action."

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

228. For limitation 3[b], I map "determining ... the at least one action based on the supervision notification" to the processing device's lookup of the recipients and responsive action. Staton states that the control center "looks up the correct

PDAs to contact in the resources database 670 and any other parties that must be contacted, such as the police or 911." Ex.1007, 26:65-27:3. This lookup uses the received event notification to select the parties and communications response required for that event. Similarly, the remote notify router "queries the resources database 670 to find out if the configuration information or event information received requires a notification to a PDA 105, the instrument module 195 or communications device 177." *Id.,* 22:18-35. That query evaluates the supervision notification against stored rules and contact data to determine the action the event calls for. Each lookup therefore is a determination of the action based on the supervision notification, and the limitation is disclosed.

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."***

229. For limitation 3[c], I map "performing, using the processing device, the at least one action based on the determining" to the processing device's processing of the event, identifying the recipient, formatting and encoding the message, and placing it in the outbound queue for transmission through the appropriate gateways. *See* Ex.1007, 22:28-36, 26:51-61 (message is "processed and analyzed to find out the final recipient. Then the message gets routed back through the gateway 846, to the Internet 160, through the cellular network 842 and to the PDA 106"), 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"). That rerouting and transmission establishes a messaging communication session between the PDA 105 (supervisee) and PDA 106 (supervisor). In addition to establishing a messaging communication session, Staton discloses that, after path deviation, "[t]he parents can then immediately call her to find out about the unexpected event." Ex.1007, 23:57-60, *see also* 8:21-25. The resulting telephone call between PDA 106 as the supervisor device and PDA 108 as the supervisee device is also "an establishment of a communication session." Staton explains that PDA-to-PDA communication is mediated by the backend: "At the control center, the message is processed and analyzed to find out the final recipient." *Id.,* 25:9-15. Staton also states that "[c]ommands can also be from PDA to PDA and are transmitted and received after a screening process through the back end control system 150." *Id.,* 26:52-61. These passages show that the backend processing device determines and mediates the PDA-to-PDA communication. More specifically, the remote notify router "then formats and encodes the message" and places it in the outbound queue for transmission through the appropriate gateway, using contact information maintained in the resources database. Routing the notification to PDA 106 thereby prompts the supervisor to call the supervisee PDA. If the PO argues that the parent's call is not itself performed or initiated by the server-side processing device, in my opinion, a

POSITA would nonetheless understand the backend's mediated routing and screening of the PDA-to-PDA communication to be the processing device performing the establishment of the communication session, because the backend processes the event, identifies the final recipient, encodes and routes the communication, and enables the supervisor and supervisee devices to communicate. Staton also states: "Therefore, a PDA 105 can be configured with a calling number for the monitoring PDA 106, such that when an event occurs, PDA 105 automatically dials monitoring PDA 106." *Id.,* 25:9-12; *see also id.* 3:19-21 ("[T]he method further comprises executing a pre-programmed operation such as making a telephone call…."). This confirms that Staton's event-handling system establishes a communication session between the supervisor and supervisee. Thus, the action comprises "an establishment of a communication session between the at least one supervisor device and the at least one supervisee device," and limitation 3[c] is disclosed.

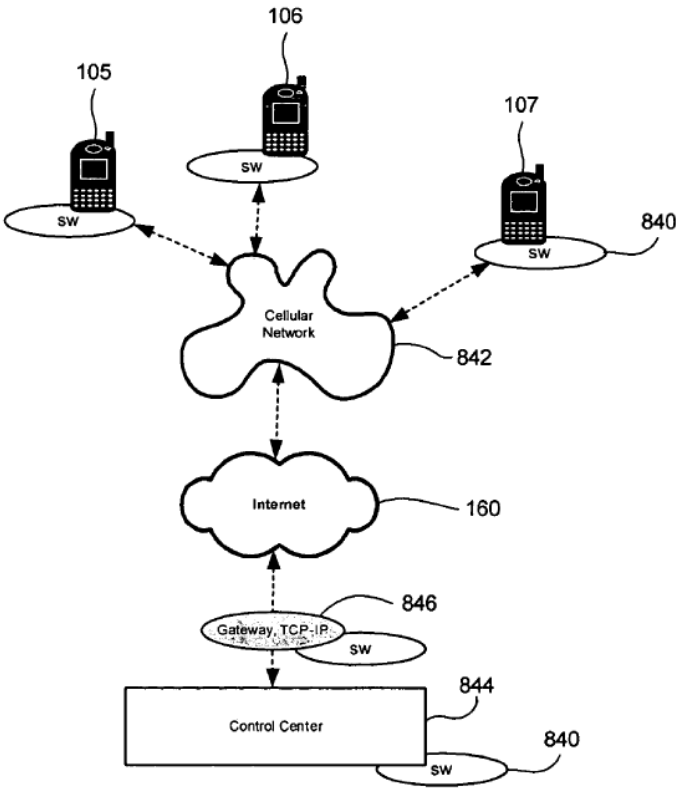


FIG. 8A

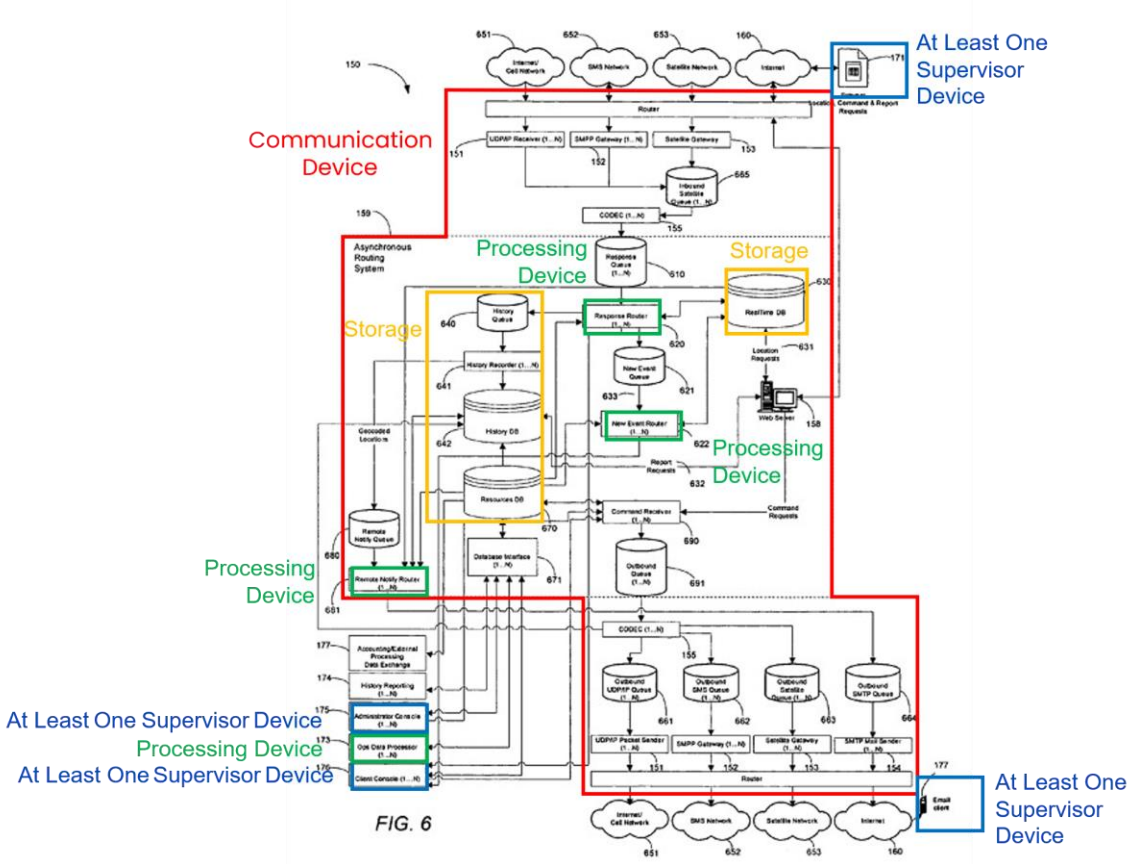
Ex.1007, Fig. 8A.

5. Claim 4

230. In my opinion, claim 4 is disclosed by Staton.

a. 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"

231. For limitation 4[a], I rely on Staton's disclosure that the response router 620 "determines if a client console 176 is tracking PDA 105 or the instrument module 195 associated with the incoming message." Ex.1007, 21:47-50.



Ex.1007, Fig. 6 (annotated).

232. Resolving which PDA the incoming message belongs to identifies the specific supervisee associated with that PDA. Staton also discloses that the command receiver 690 tags an outbound message with the correct PDA 105 address by "searching the resources database 670 and retrieving the address information." *Id.,* 24:58-62. This per-PDA resolution identifies the supervisee to whom the message relates. The remote notify router likewise makes a PDA-specific inquiry when it "queries the resources database 670 to find out if the configuration information or event information received requires a notification." *Id.,* 22:18-35. Finally, Staton explains that "when the backend control system 150 processes a

received message by one PDA, the backend control system 150 can relay the data in the message to the correct PDA." *Id.,* 23:58-24:5.These disclosures show that the processing device determines which supervisee sent the event data by analyzing the incoming message's PDA identification, geocoded location, and event information. Thus, the processing device is "identifying ... the supervisee based on the analyzing of the at least one supervisee data," and limitation 4[a] is disclosed.

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."***

233. For limitation 4[b], I map "supervisee profile data associated with the supervisee" to the relational information of members and accounts stored in resources database 670. Staton states that the resources database stores "relational information of members and accounts ... [and] which PDAs are associated with which PDAs." Ex.1007, 24:12-16. This information identifies the supervisee's account and the relationship between the supervisee PDA and the supervisor PDA. Staton also states that "[o]perations data processors 173 connect to the resources database 670 in order to retrieve configuration information for a specific user, PDA 105, or instrument module 195." *Id.,* 24:56-64. This is profile and configuration data associated with the identified supervisee. The dependency is satisfied because the remote notify router "retrieves the contact information for the appropriate PDA 105, the instrument module 195 or the communications device 177" before formatting

and encoding the message. *Id.,* 22:25-33. Without retrieving the member, account, PDA-association, configuration, and contact information, the system would not know whether or to whom to send the notification. Thus, "the generating of the supervision notification is based on the retrieving," and limitation 4[b] is disclosed.

6. Claim 6

234. In my opinion, claim 6 is disclosed by Staton.

a. ***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;"***

235. For limitation 6[a], I map the environment data to measurements from instrument module 195's environment-condition sensors. Staton identifies measuring instruments that measure "the levels of carbon monoxide, chlorine, smoke, smog, oxygen in the air, or temperature." Ex.1007, 3:35-37; *id.* 5:15-18. These measured levels are data about environmental conditions. Staton also explains that the PDA "can also monitor and analyze hazardous environmental conditions, including the detection of Oxygen, Carbon Monoxide, Chlorine, Natural Gas, Smog and Smoke concentrations." *Id.,* 5:66-6:2. This confirms that the measurements are environmental data used in the supervision system. The data is associated with the geofenced area because the PDA can "adapt to the new one by loading a specific configuration for that zone such that it interacts with zone-specific instruments through the instrument module 195 that operates in that zone." *Id.,* 7:65-8:8. The

instruments operate in and have configurations associated with the particular zone, so their measurements are associated with the geographical area corresponding to the geofence. The communication device receives that data: the instrument module "can also be connected to the internet 160 in order to have connectivity with the web server 158 and the backend control system 150" and "reports such information through the internet 160 to the backend control system 150 and to the PDA 105." *Id.,* 14:4-11. In the smoke example, the instrument module connects to the backend, which "would in turn receive the event message and relay the message to the PDA 105." *Id.,* 19:60-20:6. Thus, Staton meets "receiving ... at least one environment data associated [with] the geographical area corresponding to the geofence."

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."***

236. For limitation 6[b], once the backend receives the environment event data, the same framework described for claim 1 applies. The history recorder places incoming event information, including environment-related event messages, into the remote notify queue. Ex.1007, 19:48-52. Staton states that the remote notify router "receives the geocoded location and event information" and "queries the resources database 670 to find out if the configuration information or event information received requires a notification to a PDA 105, the instrument module 195 or

communications device 177." *Id.*, 22:16-36. Evaluating the reported hazardous condition against the stored configuration and event rules is "analyzing ... the at least one environment data." It also determines "at least one threat" because an event message reporting dangerous smoke, carbon monoxide, or another hazardous condition is a threat determination: the system evaluates whether the reported condition warrants notifying the supervisor. Staton also states that "an emergency from a measurement from an instrument 140 would be a priority message which would be the first message transmitted when the connection is re-established." Ex.1007, 19:15-19. The generation of the supervision notification is based on that determination because, if notification is required, the remote notify router "retrieves the contact information for the appropriate PDA 105, the instrument module 195 or the communications device 177" and "formats and encodes the message" for transmission through the outbound queues. *Id.*, 22:27-30.

237. Staton discloses that the initial determination that sensor data reflects a hazardous condition occurs on the device side: 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 to the PDA 105," and PDA 105 in turn reports that event to backend control system 150. Ex.1007, 12:14-18, 7:65-8:8. But the backend remote notify router also determines a threat when it receives the event information and determines whether the reported

condition requires a supervisor notification. *Id.,* 22:16-36. To the extent Patent Owner contends that the initial determination of a hazardous event must occur at the backend server, it would in my opinion have been obvious to perform that determination at the server in addition or as an alternative to device-side processing, for the same reasons I give for limitation 1[f]: redundancy, compatibility with lower-power client devices, and conservation of PDA battery power. The control center already receives the same measurement, has the geofencing software and event-processing infrastructure to analyze messages before identifying the final recipient, and already applies configuration rules to decide whether a notification is required, so a POSITA would have found it straightforward to move or duplicate that threshold comparison at the server and would have had a reasonable expectation of success in doing so; server-side processing would also centralize the hazard rules and allow the same threshold logic to be applied consistently across zones and supervisor devices. Thus, even under the narrower reading, Staton renders obvious the processing device analyzing the environment data and determining the threat, and the generating of the supervisor notification is based on that determination. *Id.,* 19:60-20:6, 26:52-61.

7. Claim 8

a. *8[a]: "The method of claim 1, wherein the at least one supervisee device comprises at least one sensor"*

238. Staton discloses that the instrument module 195 "can be packaged separately from the PDA 105, or alternatively, an instrument module 195 can be in the same housing." Ex.1007, 8:44-46; *see also* 10:33-35, 8:38-40. When the instrument module is housed within PDA 105, the instrument module and its connected sensors are part of the supervisee device. Staton identifies the connected health-monitoring instruments as "a heart monitor, an insulin level reader, blood pressure monitor, etc." *Id*. Thus, the supervisee device comprises at least one sensor.

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

239. The heart monitor, insulin level reader, and blood pressure monitor detect physiological signals originating in the monitored person's own biological processes, such as heartbeat, blood glucose, and blood pressure. A physiological signal originating in the supervisee's body is a signal made by the supervisee. Staton's claims state: a "poor health condition of the individual carrying the first portable device as measured by an instrument associated by the individual." Ex.1007, 8:46-48. By treating the measured health condition as a condition of the individual, Staton links the detected physiological condition to the individual carrying the device. My opinion is therefore that the health-monitoring sensors detect a signal made by the supervisee. *Id.,* claim 3.

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

240. Staton states that "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 to the PDA 105." Ex.1007, 12:14-20. The event message is supervisee data generated based on detecting the physiological signal and its threshold condition. That data then flows through the same supervisee-data and notification framework established for limitations 1[e] through 1[h]: it is received through backend control system 150, processed by the server-side routing and notification components, and transmitted to the supervisor device. *Id.,* 16:18-23, 22:5-15. Thus, the sensor is "configured for generating the at least one supervisee data based on the detecting," and limitation 8[c] is disclosed.

8. Claim 10

a. ***10[pre]: "A system for facilitating supervision of individuals based on geofencing, the system comprising:"***

241. In my opinion, claim 10 is the system counterpart to method claim 1. It recites a communication device, processing device, and storage device "configured for" the same functions recited as method steps in claim 1, and it incorporates the same grid-parameter limitations in 1[j] through 1[j][4].

b. ***10[a]: "a communication device configured for:"***

242. For limitation 10[a], Applicant argued that the "communication device configured for" receiving and transmitting is a 35 U.S.C. § 112(f) term whose corresponding structure is a program or database inside a server computer that handles messages between the server computer and external devices. Staton discloses that structure as described for 1[a]. Ex.1007, 8:14-25.

c. ***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;"***

243. For limitation 10[a][1], the communication device performs the claim 1 function of limitation 1[a]. As explained for 1[a], Staton meets "receiving ... at least one security parameter from at least one supervisor device associated with at least one supervisor." Ex.1007, 11:27-50, 25:60-62, 27:66-28:2.

d. ***10[a][2]: "receiving, using the communication device, a geographical location from the at least one supervisor device;"***

244. For limitation 10[a][2], the communication device performs the claim 1 function of limitation 1[b]. As described for 1[b], Staton meets "receiving, using the communication device, a geographical location from the at least one supervisor device." Ex.1007, 14:56-59, 15:17-23, 15:27-30.

e. ***10[a][3]: "receiving at least one supervisor data associated with a supervisee from at least one supervisee device; and"***

245. For limitation 10[a][3], the claim as issued recites "supervisor data associated with a supervisee from at least one supervisee device." Based on the antecedent basis in the remainder of claim 10, I understand this wording to refer to the supervisee data of limitation 1[e], and the analysis is identical to 1[e]: the backend communication components receive PDA 105's location and event information and route it to supervisor devices, so it includes data provided for or concerning the supervisor. Thus, under either reading, the communication device performs the claimed receiving function. Ex.1007, 7:1-7, 8:14-25, 16:18-23.

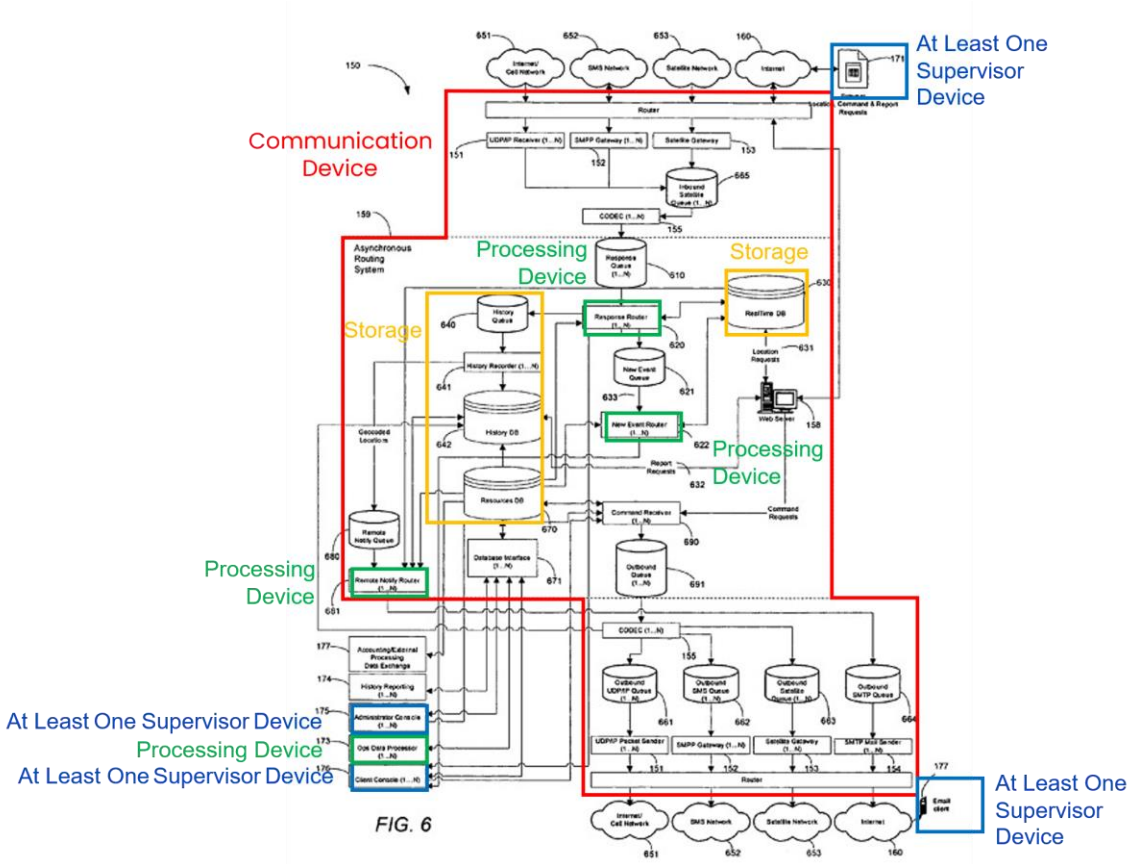
f. ***10[a][4]: "transmitting a supervision notification to the at least one supervisor device;"***

246. For limitation 10[a][4], the communication device performs the claim 1 function of limitation 1[h]. As described for 1[h], Staton meets "transmitting a supervision notification to the at least one supervisor device." Ex.1007, 8:19-25, 21:47-51, 22:28-36.

g. ***10[b]: "a processing device configured for:"***

247. For limitation 10[b], Applicant argued that the "processing device configured for" analyzing, generating, and related functions is a § 112(f) term corresponding to a program or database inside the server computer that receives data

from the communication device and stores processed data on the storage device. Staton discloses that structure as described for 1[c].



Ex.1007, Fig. 6 (annotated).

248. These are server-side programs and processing services that receive communications, build and analyze zones, evaluate incoming event information, and generate or route notifications. Ex.1007, 7:30-33, 21:47-22:33.

h. ***10[b][1]: "analyzing the geographical location based on the at least one security parameter;"***

249. For limitation 10[b][1], the processing device performs the claim 1 function of limitation 1[c]. As described for 1[c], Staton therefore meets "analyzing

the geographical location based on the at least one security parameter." Ex.1007, 14:53-55, 15:4-9, 27:52-57.

i. ***10[b][2]: "generating a geofence corresponding to a geographical area based on the analyzing;"***

250. For limitation 10[b][2], the processing device performs the claim 1 function of limitation 1[d]. As described for 1[d], Staton therefore meets "generating a geofence corresponding to a geographical area based on the analyzing." Ex.1007, 15:4-9, 15:31-34, 16:47-52.

j. ***10[b][3]: "analyzing the at least one supervisee data based on the geofence; and"***

251. For limitation 10[b][3], the processing device performs the claim 1 function of limitation 1[f]. As described for 1[f], Staton therefore meets "analyzing the at least one supervisee data based on the geofence." Ex.1007, 13:65-14:19, 17:48-52, 21:47-51, 22:18-35.

k. ***10[b][4]: "generating the supervision notification based on the analyzing of the at least one supervisee data; and"***

252. For limitation 10[b][4], the processing device performs the claim 1 function of limitation 1[g]. As described for 1[g], Staton therefore meets "generating the supervision notification based on the analyzing of the at least one supervisee data." Ex.1007, 17:30-33, 17:48-52, 22:18-35.

l. ***10[c]: "a storage device configured for storing the at least one supervisee data and the supervision notification, wherein:"***

253. For limitation 10[c], Applicant identified a program or database inside the server computer that stores the data as the corresponding § 112(f) structure. Staton discloses that structure, as described for 1[i]. As explained for limitation 1[i], Staton also meets "storing the at least one supervisee data and the supervision notification." Ex.1007, 19:50-59, 22:5-15.

m. ***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,"***

254. For limitation 10[d], the geofence and grid-based limitations are the system counterparts to limitations 1[j] through 1[j][4]. The communication device's receipt of the grid parameter and the processing device's grid functions are therefore the same as analyzed for claim 1. Ex.1007, 15:31-34, 15:46-55.

n. ***10[d][1]: "wherein the communication device is further configured for receiving at least one grid parameter from the at least one supervisor device"***

255. For limitation 10[d][1], as described for 1[j][1], this limitation is disclosed. Ex.1007, 15:46-55.

o. ***10[d][2]: "wherein the processing device is further configured for: analyzing the at least one grid parameter;"***

256. For limitation 10[d][2], the processing device performs the claim 1 function of limitation 1[j][2], as I described above. Ex.1007, 15:46-55.

p. ***10[d][3]: "determining the grid box geofence area based on the analyzing of the at least one grid parameter; and"***

257. For limitation 10[d][3], the processing device performs the claim 1 function of limitation 1[j][3], as I described above. Ex.1007, 15:50-59.

q. ***10[d][4]: "generating a number of geofence grid boxes based on the determining."***

258. For limitation 10[d][4], the processing device performs the claim 1 function of limitation 1[j][4], as I described above. Ex.1007, 15:48-50, 16:48-51.

259. Each element of claim 10 requires only that the components be "configured for" the recited functions. Because my claim 1 analysis shows that Staton's backend control system 150 and its components perform the corresponding functions, the system is configured for doing so. .

9. Claim 11: "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: identifying at least one location corresponding to the at least one location indication; analyzing the at least one supervisee data based on the at least one location; and 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."

260. Claim 11 is the system counterpart to claim 2. The communication device of claim 10 performs the receiving function in 11[a], and the processing device of claim 10 performs the functions in 11[b]-[d]: 11[a] corresponds to claim 2[a], 11[b] corresponds to claim 2[b], 11[c] corresponds to claim 2[c], and 11[d] corresponds to claim 2[d]. Because the claim 10 devices are configured for the claim 2 functions, claim 11 is invalid for the same reasons as claims 2 and 10. Ex.1007, 15:4-9, 21:47-51, 22:18-35.

10. Claim 12: "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: determining the at least one action based on the supervision notification; and 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."

261. Claim 12 is the system counterpart to claim 3. The processing device of claim 10 performs the claim 12 functions: 12[a] corresponds to claim 3[a], 12[b] corresponds to claim 3[b], and 12[c] corresponds to claim 3[c]. Claim 12 is therefore invalid for the same reasons as claims 3 and 10, and the claim 10 processing device is configured for each recited function. Ex.1007, 23:58-60, 26:52-61, 25:9-12.

11. Claim 13: "*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, 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.*"

262. Claim 13 corresponds to claim 4. Claim 13[a] corresponds to claim 4[a]: the processing device of claim 10 performs the function. Claim 13[b] corresponds to claim 4[b]: the storage device of claim 10 performs function. Because the claim 10 devices are configured for those functions, claim 13 is invalid for the same reasons as claims 4 and 10. Ex.1007, 21:47-51, 22:18-35, 24:12-16, 24:56-64.

12. Claim 15: "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: 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."

263. Claim 15 corresponds to claim 6. The communication device of claim 10 performs the function corresponding to claim 6[a], and the processing device of claim 10 performs the functions corresponding to claim 6[b]. Claim 15 is therefore invalid for the same reasons as claims 6 and 10, and the claim 10 devices are configured for each recited function. Ex.1007, 3:35-37, 7:65-8:8, 22:16-36.

13. Claim 17: "*The system of claim 10, wherein the at least one supervisee device comprises at least one sensor, wherein the at least one sensor is configured for detecting at least one signal made by the supervisee, wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting*."

264. Claim 17 corresponds to claim 8: 17[a] corresponds to 8[a], 17[b] corresponds to 8[b], and 17[c] corresponds to 8[c]. Claim 17 is invalid for the same reasons as claims 8 and 10, and the claim 10 system is configured for the recited functions. Ex.1007, 8:46-48, 10:26-27, 12:14-18.

B. Ground 2: Obviousness of Claims 5, 7, 9, 14, 16, and 18 over Staton In View Of Noland + Knowledge Of A POSITA

265. Claims 5, 7, and 9 depend from claim 1, and claims 14, 16, and 18 depend from claim 10. In my opinion, claims 1 and 10 are disclosed by Staton as set

out in the Ground 1 analysis, including limitations 1[pre] through 1[j][4] and 10[pre] through 10[d][4], respectively. The additional limitations of these six dependent claims are rendered obvious by Staton in view of Noland.

266. Noland discloses a threat sensing system 100 for automated gunshot detection and emergency response. Noland explains that the system combines sensors and software to detect and report gunshot events, provide emergency notifications, and provide first responders with information about the threat and its location. Ex.1008 ¶¶[0015]-[0019]. This disclosure supplies the threat-sensing functions used below in combination with Staton's geofence-based supervision architecture.

1. A POSITA Would Have Combined Staton with Noland

267. A POSITA would have been motivated to combine Staton with Noland, with a reasonable expectation of success. Staton is in the same field of endeavor as the '757 Patent: facilitating supervision of individuals based on geofencing. Ex.1001, 1:7-10. Staton states that "[v]arious events can be configured based on 'geofencing' events" and that "[g]eofencing entails creating configurable boundaries or geographical zones in which a PDA 105 operates." Ex.1007, 13:65-66. Staton further explains that "the entering or leaving a geographical area that has been geofenced can be an event itself" and that "[a]n event related to a geographical zone can trigger communication from one PDA to another." Ex.1007, 13:66-14:13. These

statements describe geofencing-based supervision of persons within configurable geographical zones with event-based notifications.

268. Noland likewise teaches geofencing for monitoring persons within a defined area. Noland states that "a geo-fence (a virtual perimeter) can be dynamically generated to define a predefined boundary, such as a school attendance zone or a specific building boundary that can be monitored." Ex.1008 ¶[0148]. This disclosure describes monitoring people and events within a defined geographical area, including a school or building boundary.

269. Both disclosures are directed to the same field of endeavor as the '757 Patent: facilitating supervision of individuals based on geofencing. Ex.1001, 1:7-10. The '757 Patent describes geofencing as a virtual perimeter for a real-world geographical area and identifies school zones and neighborhood boundaries as examples. It also describes a supervisee device disposed in the geographical area corresponding to the geofence and supervision notifications sent to a supervisor. Ex.1001, 1:13-29, 12:45-14:6. The specification and file history further describe retrieving a blueprint for a facility such as a school or hostel and determining the supervisee's location on that blueprint. Ex.1001, 12:45-14:6; Ex.1002, 23, 29, 58.

270. The references are also reasonably pertinent to the particular problem faced by the inventor: supervising individuals within a geofenced area and delivering threat information to a supervisor. Staton addresses that problem by monitoring a

RAVE/MSI, EX1005, p. 179

person's location and events relative to a geographical zone and relaying event information to a monitoring device. Noland addresses the same problem in a facility setting by detecting a threat, locating it within the facility, and transmitting actionable threat information to designated recipients. Thus, both Staton and Noland are analogous art to the '757 Patent.

271. A POSITA would have recognized the benefit of incorporating three specific Noland capabilities into Staton's geofence-based supervision framework: weapon detection and classification, facility blueprint access, and near field communication (NFC) identification. Adding those capabilities would improve the information available to supervisors and first responders while using Staton's existing geofence, event, routing, and notification functions.

272. For weapon detection, adding weapon-type identification and lethality assessment would improve the quality and urgency of notifications transmitted to supervisors, enabling more informed responses to threats within supervised zones. Staton itself recognizes notification urgency. Staton explains that an instrument module may report a measurement to the backend "in case of an extreme urgency." Ex.1007, 19:23-26. This shows that Staton already prioritizes prompt transmission when an event is urgent, so a POSITA would have recognized that sharpening the threat information conveyed in that notification would improve the same system's response.

273. Noland expressly identifies the operational benefit of that added information: the threat sensing system "can also advise 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 (*e.g.*, the level of body armor that might be required) and necessary tactics." Ex.1008 ¶[0156]. This passage explains why weapon classification matters: the weapon type informs the level of protection and response tactics. The motivation therefore comes from the references' stated operational benefits, rather than from hindsight.

274. For facility blueprints, pinpointing a threat on a floor plan would enhance the location functionality Staton already provides. Staton locates a supervisee within a zone and communicates that event to a supervisor, but a facility schematic supplies finer room-level location information. That added detail would allow a supervisor or responder to distinguish a location within a school or other building rather than receiving only a zone-level location.

275. For NFC, near-field identification would enhance the identification functionality Staton already performs by hardware-address lookup. It would provide a proximity-based indication of which supervisee device is present in the geofenced area and would allow the backend to associate that indication with the corresponding monitored person.

RAVE/MSI, EX1005, p. 181

276. The combination also would have yielded predictable results and would have been technically feasible. Staton expressly contemplates expandable external sensors. Staton states that "[a]n instrument module can be mounted, attached, manufactured, or otherwise included upon/in various articles or electrical devices" and that the instrument module can "report a specific event or occurrence related to any of the environment devices associated with the instrument module." Ex.1007, 6:34-8:8. This architecture was designed to accept event information from external devices rather than being limited to one fixed sensor. Thus, in my opinion, a POSITA would have understood that Noland's threat sensing devices could be integrated 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].

277. Staton further states that the instrument module "can also be connected to the internet 160 in order to have connectivity with the web server 158 and the backend control system 150" and "reports such information through the internet 160 to the backend control system 150 and to the PDA 105." Ex.1007, 8:2-8. This communication path provides a ready ingress path for Noland's sensor output into Staton's backend.

278. For NFC, Noland teaches identifying persons through NFC/RFID identifiers linked to employee and student IDs. Ex.1008, ¶¶[0034], [0074], [0148].

And Staton's instrument module 195 already communicates with PDA 105 over "WiFi, Bluetooth, [or] wireless USB" and reports "through the internet 160 to the backend control system 150." Ex.1007, 7:60-8:8, 10:28-42. In my opinion, a POSITA would have added an NFC reader to instrument module 195 to confirm who is present in a zone. This would have been a routine addition to the existing short-range instrument module hub. Indeed, Staton discloses that the instrument module and PDA interact "through a wireless link of a known protocol such as Bluetooth, short-range radio, etc.," and a POSITA would have understood that NFC is a short-range radio technology. Ex.1007, 8:40-42.

279. A POSITA would have had a reasonable expectation of success. The relevant data types are the same kind of georeferenced event data; the ingress path through the instrument module, internet or cellular network, and backend already exists; and Staton's backend already performs the receive-analyze-notify sequence required by the combined functionality. A POSITA therefore could have implemented a straightforward modification to route Noland's threat, blueprint, and NFC data to the communication components of Staton's backend control system and process that data using Noland's system gateway 110 logic integrated with Staton's processing components.

RAVE/MSI, EX1005, p. 183

2. Claim 5

280. Claim 5 is disclosed by Staton for the reasons set out in the Ground 1 analysis for claim 1 and for the reasons discussed below.

a. ***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"***

281. For limitation 5[a], I map "at least one object associated with the supervisee" to the weapon that Noland's system identifies within the supervisee's geofenced zone. Noland states that the system gateway 110 analyzes sound waveform data "to determine whether the sound waveform indicates a valid gunshot or gunshots and, if so, to further determine the general type of weapon (*e.g.*, shotgun, handgun, long rifle) that could have produced that sound waveform, and establish the location or room number of the shooter(s)." Ex.1008 ¶[0107]. This identifies an object, the weapon, and also determines its location. Because the identified weapon is located within the supervisee's geofenced zone and is detected by the threat sensing device integrated with the supervisee device, it is an object associated with the supervisee.

282. Noland further states that the gateway "determines not only the validity of a suspect gunshot waveform and determines, from the waveform, the type of weapon involved and location of the waveform, but also independently evaluates each subsequent sound waveform to determine if more than one weapon is being

used and/or more than one shooter is involved." Ex.1008 ¶[0108]. This identification therefore extends beyond a single generic gunshot determination to the number of weapons as well as the type of weapon.

283. The identification is performed by Noland's system gateway 110 as part of the same server-side processing device in Staton's backend control system 150 in Ground 1. It is "based on the analyzing of the at least one supervisee data" because the acoustic and location data analyzed by the gateway are part of the supervisee data in the combination, as described in the preceding section on obviousness.

284. Further, the detected and identified weapon is an "object associated with the supervisee" because the processing device identifies the weapon and determines that its location is within the supervisee's geofenced zone and it is detected by the supervisee device. Thus, the limitation "identifying, using the processing device, at least one object associated with the supervisee based on the analyzing of the at least one supervisee data" is rendered obvious.

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."***

285. For limitation 5[b], Noland's gateway (integrated into the processing device in the combination) determines weapon type and caliber and relates those determinations to the level of threat posed to human life. Noland states that the system "can also advise 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 (*e.g.*, the level of body armor that might be required) and necessary tactics." Ex.1008 ¶[0156]. Determining the level of threat a weapon poses, including the body armor required to withstand it, is a determination of the weapon's lethality.

286. A long rifle firing .308 caliber rounds versus a handgun firing 9 mm rounds requires a different level of body armor and different response tactics. That differentiation is a determination of lethality based on identifying the weapon and its ammunition characteristics. Noland supports the classification by describing lookup tables for firearms and bullets and classification by "caliber (*e.g.*, 9 mm, 40 S&W, 45 ACP, 0.223, 0.308, etc.)." Ex.1008 ¶¶[0111], [0127].

287. Noland states that "information regarding the Gunman X 99 and the weapon discharge (*e.g.*, location of weapon discharge, acoustic signature, image signature, determined weapon type, determined caliber, etc.) is sent via the Internet 120 to designated mobile devices 130 and local authorities 132." Ex.1008 ¶[0096]. Because the determined weapon type and caliber are content of the alert, the generation of the notification is based on the determining.

288. In the combined system, this lethality information is carried in the supervision notification transmitted to the supervisor device through the same notification pathways established in Ground 1 for limitations 1[g] and 1[h]. A POSITA would have incorporated the determined weapon type and caliber into

Staton's formatted and encoded notification because Staton already formats event messages for the appropriate recipient after analyzing incoming event information. That modification would have been obvious because it adds content to an existing server-generated message without changing the established routing path. The limitation "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" is rendered obvious.

3. Claim 7

289. Claim 7 is disclosed by Staton in view of Noland for the reasons set out for claim 1 in the Ground 1 analysis and for the reasons set out below.

a. *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;"*

290. In my opinion, Noland's facility schematics are a "blueprint." First, the '757 Patent describes the blueprint function as retrieving a blueprint associated with the geographical area corresponding to the geofence, analyzing the blueprint and supervisee data, and determining the supervisee's location on the blueprint. It separately explains that the geographical area may include a facility such as a school or hostel. The file history likewise reproduces the same functional claim language and describes retrieving a blueprint associated with a building and locating the

supervised device on it. Ex.1001, 12:45-14:6; Ex.1002, 39, 45, 74. Thus, the '757 Patent does not apply any special meaning to the term "blueprint."

291. Second, in my opinion, a POSITA in 2019 would have understood facility floor plans, building layouts, and facility schematics to be blueprints in ordinary technical usage. Noland's choice of "schematic" rather than "blueprint" is a difference in nomenclature, not substance, because both denote a plan of the structure's interior layout used to locate an event or person within that structure.

292. Noland discloses that "[r]ecorded information may also advantageously include building location, proximity information of floor plans, aerial maps, building layouts and other structural data (*e.g.*, uploaded to and resident in the physical digital storage medium)." Ex.1008 ¶[0034]. This states that floor plans and building layouts are pre-loaded into system storage. Noland also states that the geometry and location of each room in which a threat sensing device is installed "is entered into the system" and "integrated into the schematics of the facility for dissemination to first responders." *Id*. ¶[0113]. The first passage shows storage of the facility plan; the second ties the plan to the monitored facility.

293. In the combined system, the facility monitored by Noland is the geographical area corresponding to Staton's geofence, and the schematic for that facility is the blueprint associated with that area. Noland further states that the event messaging handler "accesses the user and hardware databases" to "create and format

the alert message content," including "a schematic of the school overlaid by icons showing shooter location." Ex.1008 ¶[0179], Fig. 2A, Fig. 2B. This shows retrieval of the stored schematic as part of alert generation, and the schematic that is shown for example in Figs. 2A and 2B is a floorplan.

294. In the combined system, these schematics are stored in and retrieved from the storage device mapped in limitation 1[i]. The retrieval is therefore performed using the storage device. The limitation "retrieving, using the storage device, a blueprint associated with the geographical area corresponding to the geofence" is rendered obvious.

b. ***7[b]: "analyzing, using the processing device, the blueprint and the at least one supervisee data; and"***

295. Noland's system gateway 110, integrated with Staton's processing device, jointly analyzes the stored schematic and incoming event data. Noland states that the gateway analyzes the sound waveform to determine the weapon type and "establish the location or room number of the shooter(s)." Ex.1008 ¶[0107]. Establishing the location or room number references the facility layout and room geometry on the schematic.

296. Noland also explains that the system gateway determines the sensor closest to the gunshot and correlates the "known location of the threat sensing device 10 closest to the location of the gunshot" with the facility information. Ex.1008 ¶¶[0111], [0113]. Correlating sensor-derived event data with the pre-stored room

geometry and facility schematic is analysis of the blueprint and the supervisee data together.

297. The system gateway processes the incoming supervisee data against the stored plan to determine the location and corresponding room, and the integrated gateway is the processing device mapped to Staton's server-side processing components. The limitation "analyzing, using the processing device, the blueprint and the at least one supervisee data" is rendered obvious.

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."***

298. Noland states that the alert content comprises "a schematic of the school overlaid by icons showing shooter location, text giving the name and address of the school, and color-coded information representing the path of the shooter, location of injuries, and status of lockdown by rooms within the school." Ex.1008 ¶[0179]. Noland also describes tracking "where injured persons are located inside the school" and otherwise "track[s] a location of, or presence of" person at the facility. *Id.* ¶¶[0148], [0155]. Plotting a location as an icon on the schematic is a determination of a location on the blueprint.

299. For example, Noland states: "a phone 130 is shown having displayed thereon the map of FIG. 2B, with the threat (*i.e.*, Gunman X 99) highlighted as being

in classroom 101." This description and figure confirms that the system fixes the threat location to a particular classroom on the facility plan, rather than merely reporting a general geographical zone. Ex.1008 ¶[0097]. Although it is not shown in the figure below, it would have been obvious to a POSITA to plot other supervisees' GPS locations on the facility plan because it would be done using the same overlay technique and also inform supervisors and responders as to the location of others relative to the threat.

300. Further, the alert message incorporates the determined location on the facility schematic. In the combined system, the resulting supervision data is generated based on that determination and delivered through the notification framework established in Ground 1 for limitations 1[g] and 1[h]. The claim uses "supervision data" rather than "supervision notification," but the analysis is the same under either reading because the determined room location is included in the generated alert data and transmitted to the supervisor device. The limitation "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" is rendered obvious.

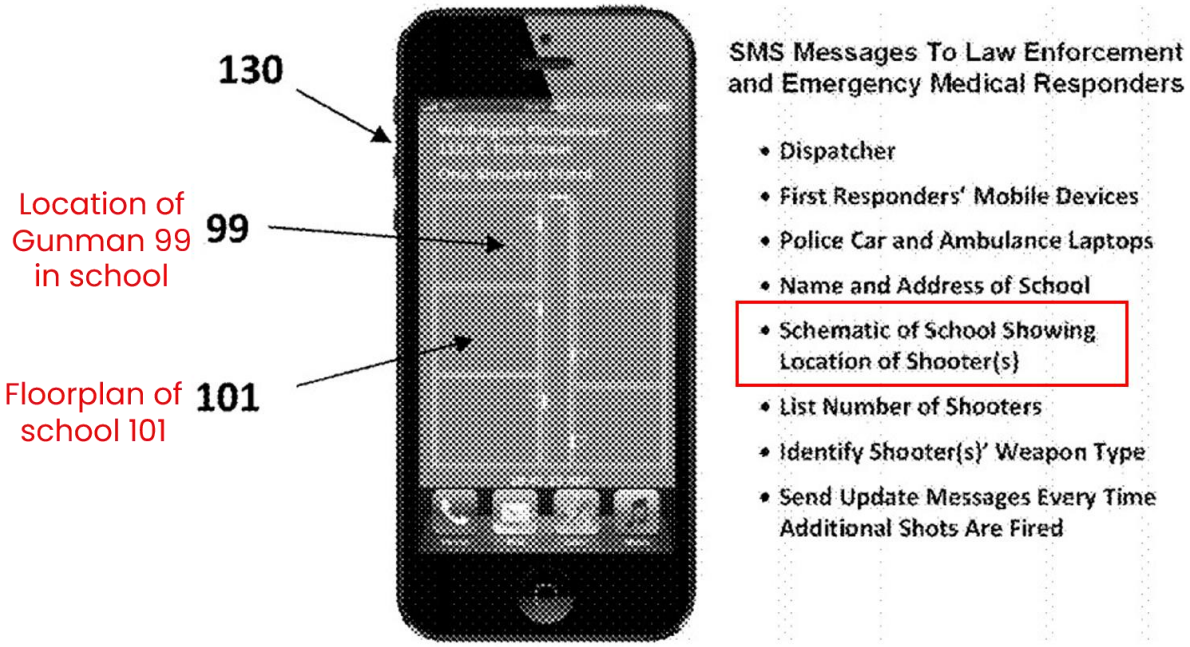


FIG. 2B

Ex.1008, Fig. 2B (annotated).

4. Claim 9

a. ***9[a]: "The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises:"***

301. In the combined system, the supervisee's device is integrated with an NFC identification readable by near-field sensors. Noland states that "[n]ear field sensors could be used to allow the system to identify mobile phones, other mobile devices and the owners of those phones, and monitor the arrival and departure of those device owners from the geo-fenced area." Ex.1008 ¶[0148]. This is an

identification associated with the supervisee, the owner of the identified phone or mobile device, and it operates within a geofenced area. Further, Staton's resource database 670 already "keeps records of all the instrument modules and PDAs" and relates each PDA to its member. Ex.1007, 19:59-61, 24:58-64. A POSITA would have stored the NFC identification there because it is a similar piece of identifying and relational data related to supervisees.

302. Noland also teaches the reading hardware: its threat sensing devices include "a near field communication (NFC) device and/or a far-field communication device (*e.g.*, standard RF, Wi-Fi, etc.), to communicate directly with nearby portable devices (*e.g.*, radio-frequency identification 'RFID' integrated into an ID Badge, etc.)." Ex.1008 ¶[0074]. This supplies a near-field reader capable of reading the NFC identification carried by the supervisee device.

303. The limitation "The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises" is rendered obvious because Noland identifies both the near-field identification and the owner of the identified mobile device within the geofenced area.

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"***

304. Noland's near-field sensor integrated into Staton's instrument module receives the NFC indication from the supervisee device, and the indication reaches the server over the same ingress path established in the obviousness section: a local sensor receives the near-field signal and communicates the resulting event information through the network to the backend. Ex.1008 ¶¶[0074], [0148]. The communication device for this limitation is the same communication components of Staton's backend control system 150 mapped in limitation 1[a]. The receiving is therefore performed using the communication device.

305. Staton already uses short-range wireless protocols for identification and communication between the PDA and instrument module. Staton states that the instrument module communicates with PDA 105 through "a wireless communications protocol such as Wireless USB, WiFi, Bluetooth, etc." and elsewhere identifies "Bluetooth, an infrared signal, a short range radio signal, wireless universal serial bus, or Wi-Fi" as communication signals. Ex.1007, 10:30-32. Ex.1008 ¶¶[0074], [0148]. NFC was a well-known short-range wireless radio

identification protocol and technology as of the priority date, and Noland teaches its application for this purpose within a geofenced area.

306. The limitation "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" is rendered obvious.

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."***

307. Noland teaches that near-field sensors identify "the owners of those phones" based on the detected near-field information. Ex.1008 ¶[0148]. The identification is performed by Noland's gateway logic integrated with Staton's processing components. It also improves Staton's existing per-device identification, which uses each PDA's unique hardware address to associate the device with a specific monitored person and the backend tags an outbound message with the correct PDA 105 address by searching the resources database 670 and retrieving the address information. Ex.1007, 24:56-64. The combined system adds the NFC identifier for that address in the lookup, which would have a reasonable expectation of success because the backend already resolves a device identifier to the monitored person.

308. Once the processing device resolves the NFC indication to a supervisee, it uses the resources database 670 contact lookup established in Ground 1 to select the appropriate supervisor device and generate the supervision notification. Staton states that the remote notify router retrieves contact information and then formats and encodes the message for the selected device. This sequence makes generation of the notification depend on the identification. Ex.1007, 22:18-35; Ex.1008 ¶[0148].

309. The generating of the supervision notification is based on the identifying because the identified supervisee determines which stored contact and supervisor relationship the backend uses to address and route the notification. The notification-generation function is performed through Staton's communication and processing devices from Ground 1, with the NFC identification supplied to that existing path by Noland's system. The limitation "wherein the generating of the supervision notification is based on the identifying" is rendered obvious.

310. Therefore, the limitation "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" is rendered obvious.

RAVE/MSI, EX1005, p. 196

5. Claim 14: "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 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."

311. Claim 14 corresponds to claim 5: 14[a] corresponds to 5[a] and 14[b] corresponds to 5[b]. Claim 14 is invalid for the same reasons as claims 5 and 10, and the claim 10 system is configured for the recited functions.

6. Claim 16: "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, wherein the processing device is further configured for analyzing the blueprint and the at least one supervisee data; and 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."

312. Claim 16 corresponds to claim 7. Claim 16[a] corresponds to claim 7[a]: the storage device of claim 10 performs the function. Claim 16[b] corresponds to claim 7[b]: the processing device of claim 10 performs the function. Claim 16[c] corresponds to claim 7[c]: the same processing device performs the function. Because the claim 10 devices are configured for those functions, claim 16 is invalid for the same reasons as claims 7 and 10.

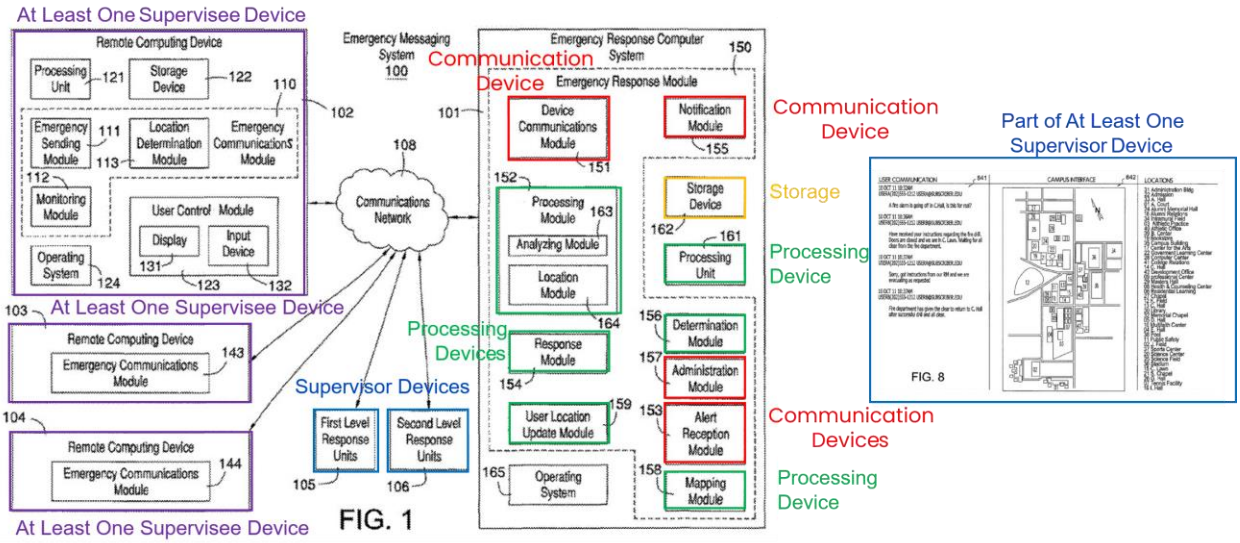
7. Claim 18: "The system of claim 10, wherein the supervisee is associated with at least one near field communication (NFC) identification, wherein the communication device is further configured for receiving at least one NFC indication corresponding to the at least NFC identification from the at least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

313. Claim 18 corresponds to claim 9. Claim 18 expressly recites NFC identification in the first element, while claim 9 uses the broader term "identification"; the claim 9 analysis already maps both the identification and receipt to NFC. Claim 18 omits claim 9's additional requirement that receiving be performed over short-range wireless communication comprising Bluetooth, Zigbee, Ultra-wideband, Wi-Fi, or NFC. That omission removes a limitation, and the claim 9 analysis therefore covers claim 18. Because the combined system performs the corresponding functions, the claim 10 devices are configured for them. Claim 18 is disclosed for the same reasons as claims 9 and 10.

C. Ground 3: Claims 1-4, 6-8, 10-13, and 15-17 Are Rendered Obvious By Rauner In View Of Azmoodeh + Knowledge Of A POSITA

1. Rauner + Azmoodeh Combined Architecture

314. In my opinion Rauner's emergency response computer system includes components corresponding to the claimed communication device, processing device, and storage device.

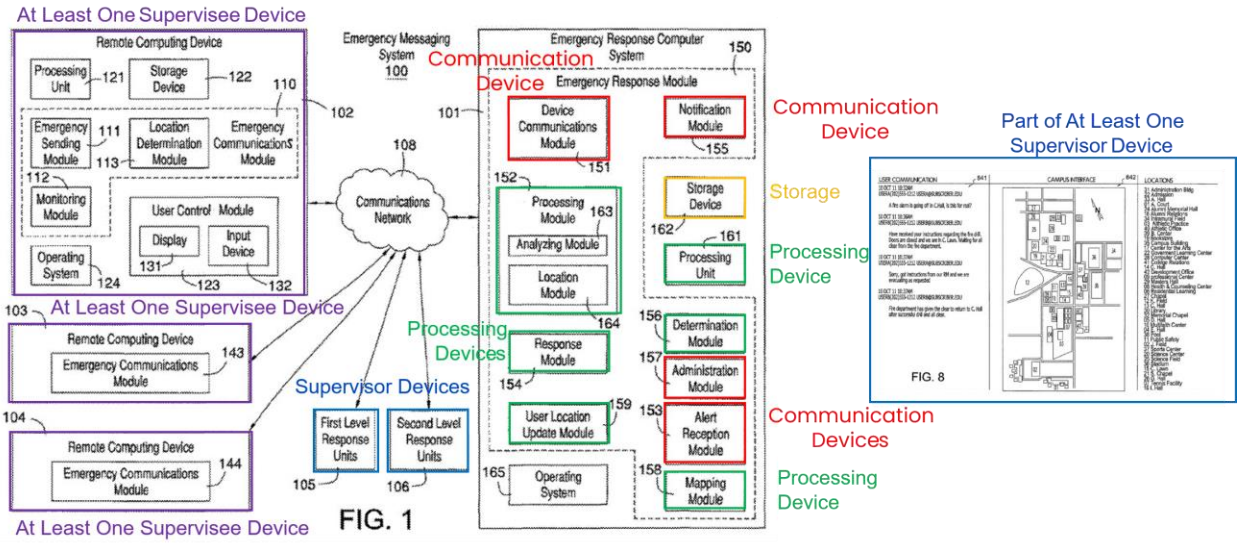


Ex.1009, Figs. 1 and 8 (annotated).

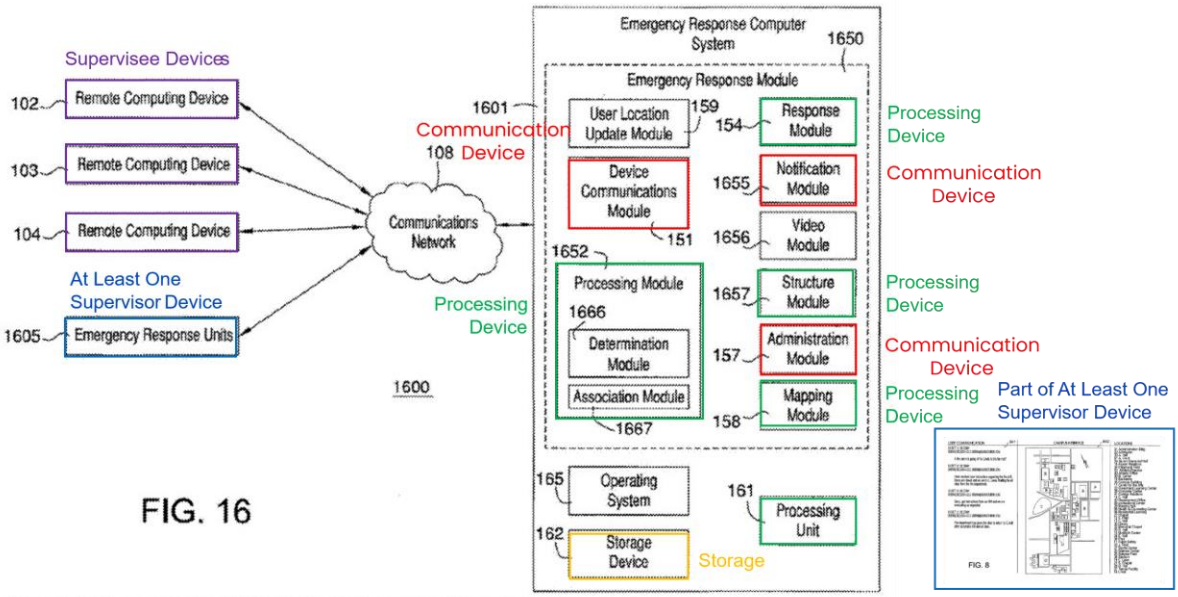
315. I analyze these devices below.

316. Rauner states that emergency response computer system 101 includes "at least one processing unit 161," emergency response module 150 running on processing unit 161, and "a storage device 162," and that emergency response module 150 includes device communications module 151, processing module 152, response module 154, notification module 155, determination module 156, administration module 157, and mapping module 158. Ex.1009 ¶¶[0053]-[0054].

317. Rauner also states that "a single server can include device communications module 151, processing module 152, alert reception module 153, response module 154, notification module 155, determination module 156, administration module 157, mapping module 158, and user location update module 159." Ex.1009 ¶[0097].



Ex.1009, Figs. 1 and 8 (annotated) (first embodiment).



Ex.1009, Figs. 16 and 8 (annotated) (second embodiment).

318. Rauner describes two overlapping embodiments. The first embodiment, emergency messaging system 100, discloses the core architecture. The second embodiment, emergency messaging system 1600, adds modules including structure module 1657. The second embodiment states that response computer system 1601,

remote computing devices 102, 103, and 104, and emergency response units 1605 communicate using communications network 108, that emergency response module 1650 runs on processing unit 161, and that the same storage device 162 is included. Ex.1009 ¶¶[0157], [0162]-[0166].

319. The second embodiment's modules therefore run on the same processing unit 161 and access the same storage device 162, while the two embodiments share device communications module 151, remote computing devices 102-104, and communications network 108. Ex.1009 ¶¶[0162]-[0166]. A POSITA would have understood these as complementary descriptions of a single system, rather than as unrelated systems, because the embodiments use the same processor, the same storage, the same network-facing communications module, and the same client devices. The second embodiment adds functional modules to the architecture already described for system 100.

320. The second embodiment includes modules that already run on processing unit 161 and draw on storage device 162, while device communications module 151 already supplies the shared network interface. The existing processor executes the added modules, and the existing databases supplies the location, association, and schematic information those modules use. I identify the specific module or modules relied upon for each limitation below.

RAVE/MSI, EX1005, p. 201

321. Rauner discloses that the communication, processing, and storage devices are implemented in a single server computer. Rauner expressly discloses that "a single server can include device communications module 151, processing module 152, alert reception module 153, response module 154, notification module 155, determination module 156, administration module 157, mapping module 158, and user location update module 159." Ex.1009 ¶¶[0053]-[0054], [0097]. Rauner also places emergency response module 150 and its modules on processing unit 161, with storage device 162.

2. A POSITA Would Have Been Motivated to Combine Rauner With Azmoodeh

322. Rauner is in the same field of endeavor as the '757 Patent: facilitating supervision of individuals based on geofencing. Ex.1001, 1:7-10. Rauner explains that its emergency messaging system serves target groups within selected geographic areas, including "all students, faculty, staff, etc. at a university or college campus," "all workers at a work location or office building," and users of public spaces. Ex.1009 ¶[0048]. This is facilitating supervision of individuals based on geofencing, across campuses, buildings, and municipalities. Rauner further states that "Geofences are graphic representations of a defined geographic area" that can be created within a Community and shared so organizations can observe emergency events occurring in that location. Ex.1009 ¶[0239].

323. Azmoodeh is in the same field because it teaches a geo-fence system that generates and monitors a real-world geographic area and divides the geo-fenced area into cells. Azmoodeh states that "the mutable geo-fence system divides the geo-fenced area into a grid that comprises a set of cells," with each cell representing a portion of the physical location within the geo-fenced area. Ex.1010 ¶[0022]. Both references therefore concern the same field of endeavor as the '757 Patent: facilitating supervision of individuals based on geofencing. Ex.1001, 1:7-10.

324. The references are also reasonably pertinent to the particular problem faced by the '757 Patent. The '757 Patent describes conventional geofencing applications as not allowing a user to create a geofence easily and identifies criminal activity and crowd density as examples of factors that may inform geofence creation. Ex.1001, 1:22-29. Azmoodeh, for example, addresses the spatial part of that problem by generating a geofence from geolocation data and dividing the region encompassed by the geofence into cells, with the number of cells defined based on the fence size or user input. Ex.1010 ¶¶[0018], [0043]-[0046]. Thus, both Rauner and Azmoodeh are analogous art to the '757 Patent.

325. The combined-architecture is discussed above, and I do not repeat that analysis here.

326. 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. Adding Azmoodeh's cell subdivision would give Rauner's system a structured framework for determining that a device is within a geofence and where within that geofence the device is located with reference to the cells. Azmoodeh explains that usage data can include geolocation data "indicating a location of a device within the geo-fenced area." Ex.1010 ¶[0047]. That added granularity would benefit Rauner's emergency-response system because knowing which part of a campus or building a person occupies can guide the selection of response resources and the information provided to responders.

327. Azmoodeh states that "the mutable geo-fence system adjusts the boundary of the geo-fence to more accurately encompass the location of interest." Ex.1010 ¶[0023]. A POSITA would have applied the cell subdivision to Rauner because assigning locations to smaller, user-defined cells permits the monitored area to be represented with finer spatial precision, while Rauner's existing coordinate and geofence processing can use that finer location information to distinguish where within a campus, building, or other geofenced area a device is located. Ex.1010 ¶¶[0022]-[0023], [0046]-[0047]; Ex.1009 ¶¶[0198], [0244].

328. Rauner serves environments ranging from a university or college campus and office building to a city, county, state, or region served by an emergency-response group. Ex.1009 ¶¶[0048], [0165]. A POSITA would therefore have recognized that a campus or building may benefit from finer resolution, while a metropolitan area may use coarser resolution. A POSITA would have understood that this configurable grid resolution would enable supporting a wide variety of use cases and associated granularity. For example, a campus-wide area would not benefit from the finer resolution required by a building-specific site. Thereby the system resource utilization can be calibrated to reduce loading of unnecessary levels of detail. This would help to reduce system costs by reducing processing, storage, and communications demands, as well as improving processing on any processing devices that may have limited capacity. Thus, this choice is a natural extension of Rauner's administrative interface, through which the administrator configures trigger words, thresholds, maps, and geographic areas. Ex.1009 ¶¶[0089]-[0094].

329. Rauner's range of deployments also supplies an ordinary design incentive for configurability. Because Rauner serves settings ranging from a single building to a metropolitan area, one system with user-configurable resolution can use finer cells where room- or building-level localization matters and coarser cells where area-level monitoring is sufficient, allowing the same system to serve the full range of customer needs and expanding its usefulness to users with diverse

geolocating needs. A POSITA would have adopted that configurable resolution for the reason that it preserves the same coordinate-processing framework while changing only the granularity of the spatial partition, an ordinary design incentive that supports obviousness. Ex.1009 ¶¶[0048], [0165]; Ex.1010 ¶[0046].

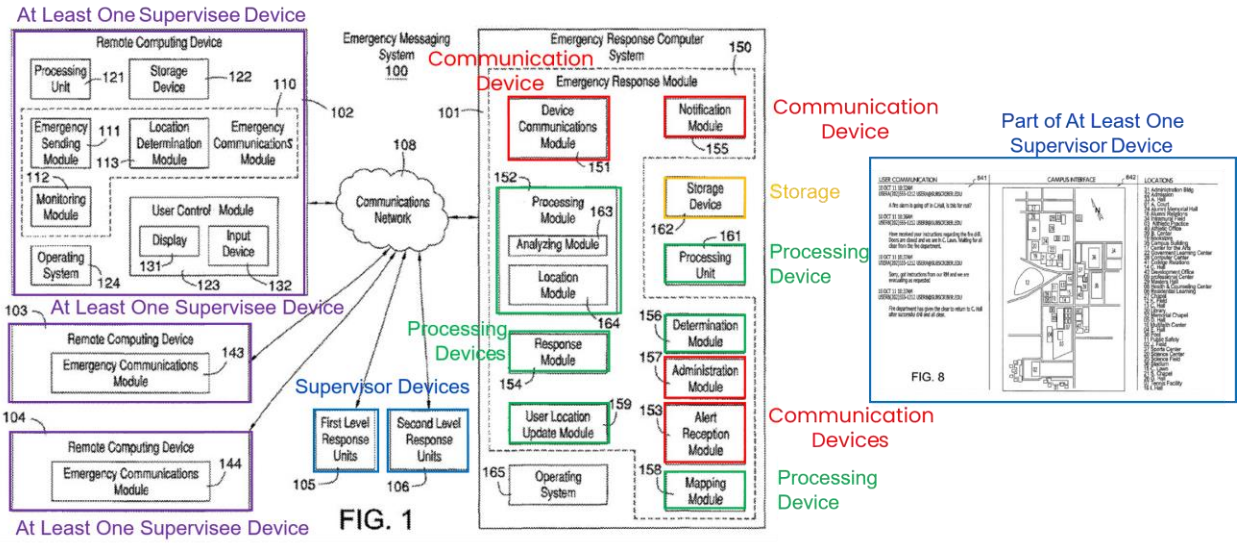
330. In my opinion, user-configurable grid resolution was a well-known design choice in geofencing systems as of the March 5, 2019 priority date. The reason is that a fixed geofence may cover areas of very different physical size and operational importance, so a system that lets the administrator select cell size or cell count can balance location precision against processing, storage, and display requirements. A finer grid provides more precise localization where room- or building-level response matters; a coarser grid reduces unnecessary subdivisions where only area-level response is needed. Azmoodeh expressly teaches that the number of cells may be defined based on the size of the geo-fence or user input. Ex.1010 ¶[0046].

331. Third, the combination would have produced predictable results and a POSITA would have had a reasonable expectation of success. Rauner already implements a GPS-integrated grid: mapping module 158 "creates an alphanumeric grid over the graphical representation," "translates grid coordinates to GPS coordinates," and "associates GPS coordinates within the grid box." Ex.1009 ¶[0094]. Rauner also uses building schematics with coordinate plotting, including a

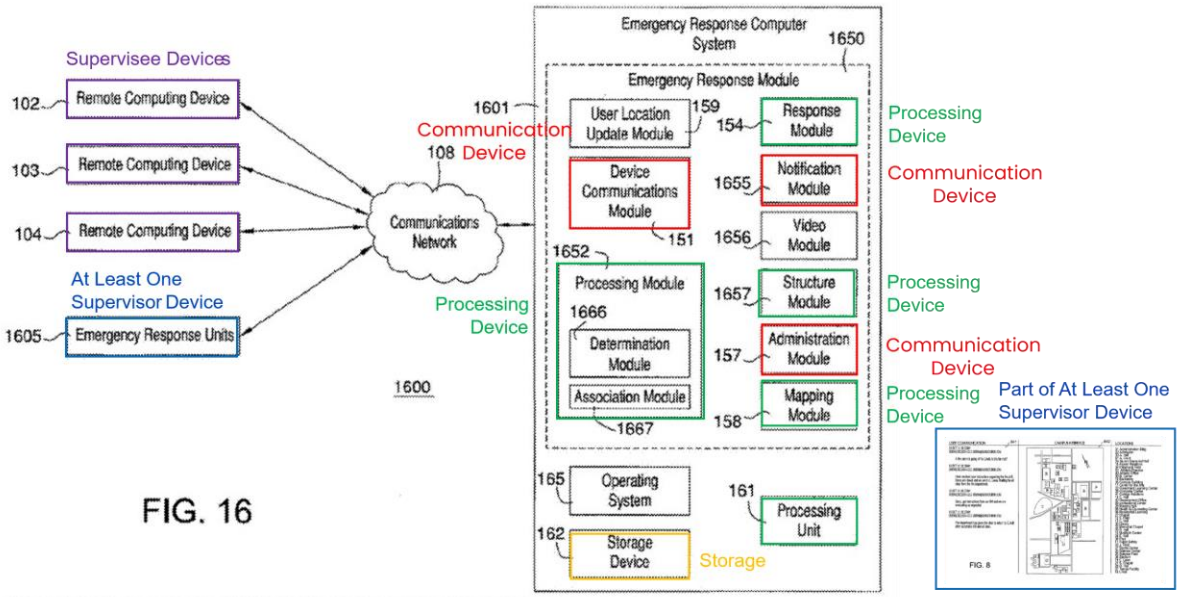
polygon over a GPS-integrated map and X, Y, and Z axis information for plotting device locations. Ex.1009 ¶¶[0197]-[0198].

332. Azmoodeh's technique operates on geospatial data. It receives geolocation data that may include longitude, latitude, altitude, a polygon, or a free-form shape corresponding to a region in a map image, and it divides the region encompassed by the resulting geo-fence into cells. Ex.1010 ¶¶[0018], [0043]-[0046]. More specifically, 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. Ex.1009 ¶[0097]; Ex.1010 ¶[0033]. Dividing a known geofence area by a user-specified cell count or cell size is basic arithmetic performed on coordinates that Rauner already computes, and Rauner's administrator already enters configuration values through the administrator's terminal interface and administration module 157. Ex.1009 ¶[0092]. In my opinion, incorporating that cell-based division into Rauner's existing grid framework is therefore no more than applying a known technique to a known system to achieve predictable results. A POSITA would have expected success because both systems operate on coordinate data referenced to a map substrate, so the subdivision

logic can be applied to Rauner's established coordinate ranges without redesigning mapping module 158.



Ex.1009, Figs. 1 and 8 (annotated).

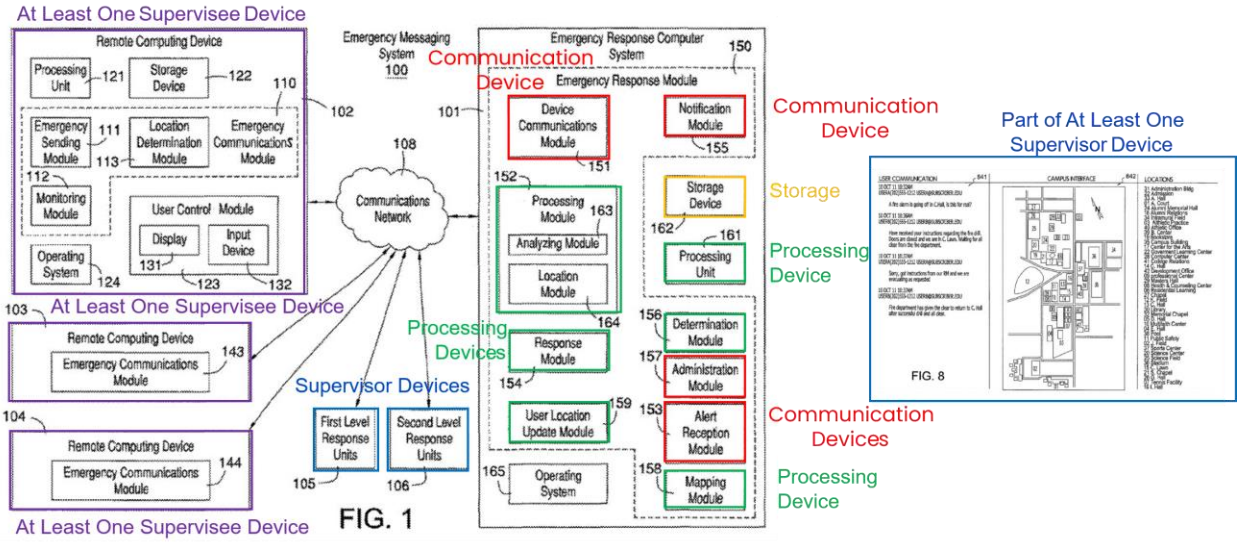


Ex.1009, Figs. 16 and 8 (annotated).

3. Claim 1

1[pre]: "A method for facilitating supervision of individuals based on geofencing, the method comprising:"

333. For limitation 1[pre], I map the claimed method for facilitating supervision of individuals based on geofencing to supervising a defined institutional population using geofences to monitor locations and coordinate emergency response. Rauner states that the target group may include "all students, faculty, staff, etc. at a university or college campus," "all workers at a work location or office building," and individuals located in a public space or region served by an emergency response group. Ex.1009 ¶[0048]. These passages identify individuals who are subject to location-based monitoring and emergency messaging.



Ex.1009, Figs. 1 and 8 (annotated).

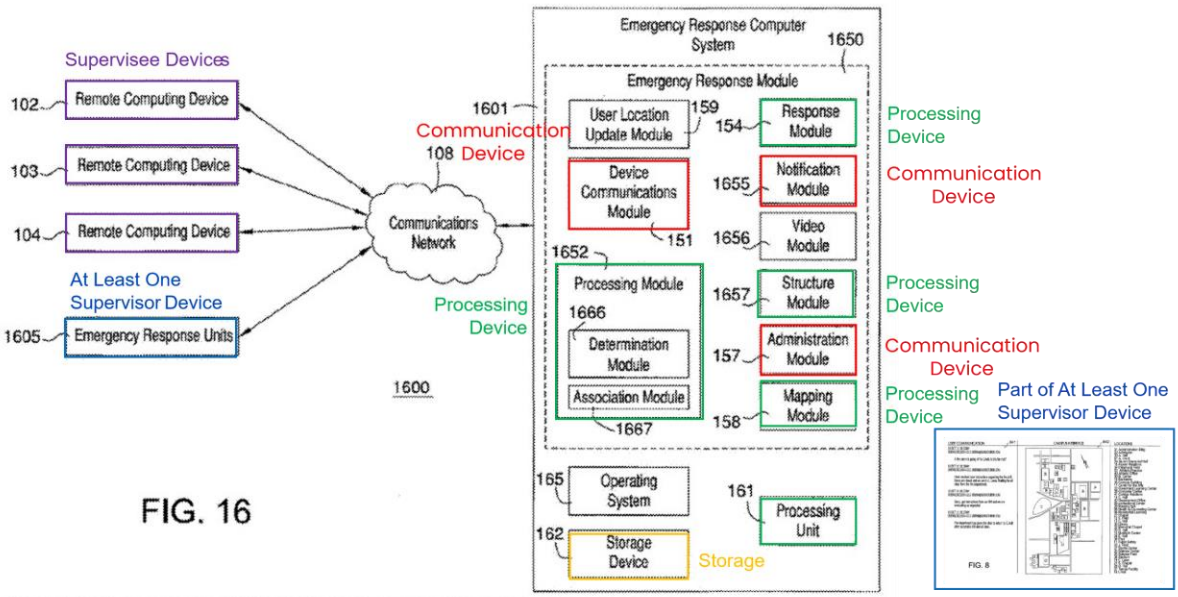
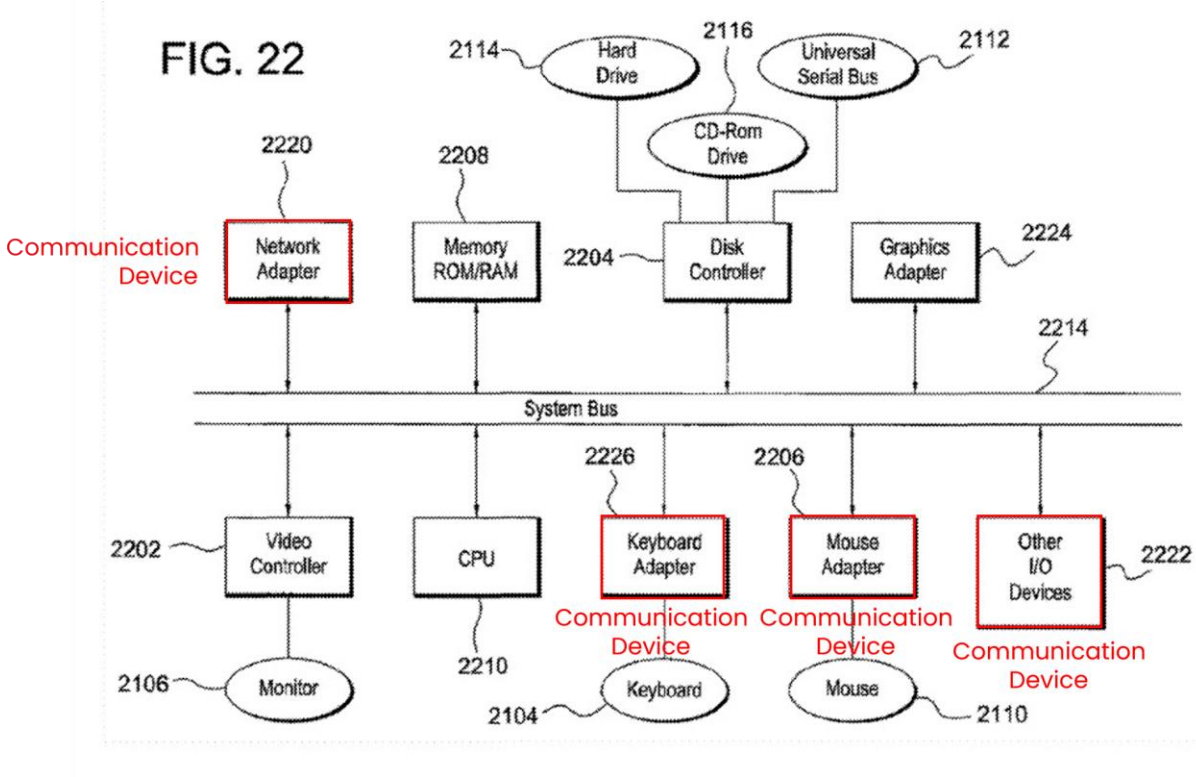


FIG. 16

Ex.1009, Figs. 16 and 8 (annotated).



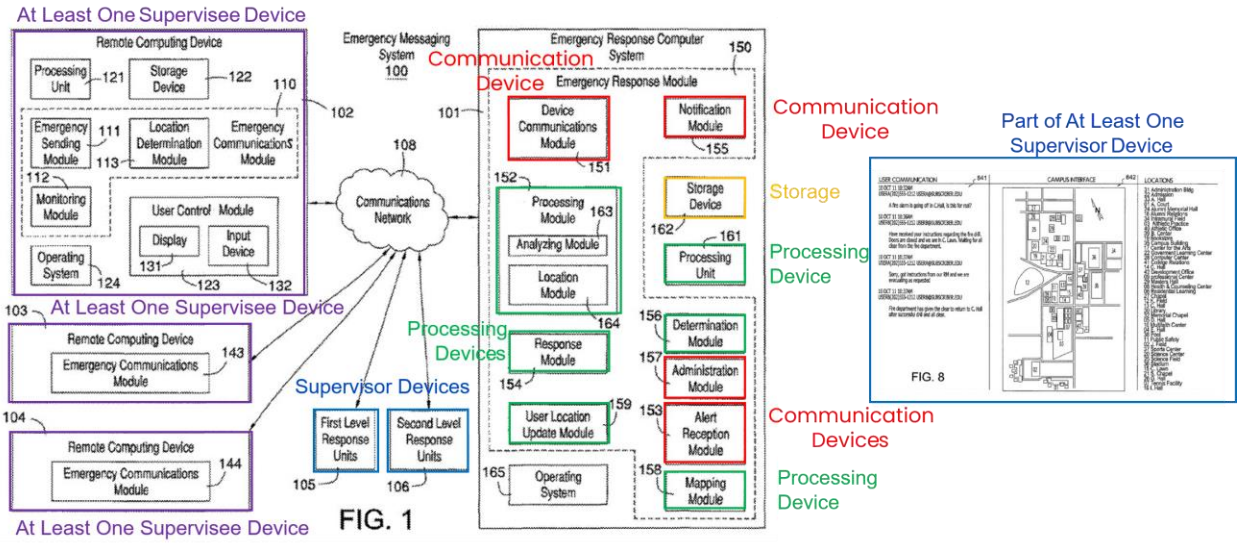
Ex.1009, Fig. 22 (annotated).

334. Rauner's abstract further explains that its emergency response computer system operates with mobile computing devices for a set of device users, produces reports identifying the locations of those devices, and coordinates emergency responders based on message content, device locations, and timing. Ex.1009, Abstract. Rauner also states that "Geofences are graphic representations of a defined geographic area" and can be used to observe emergency events occurring in that location. Ex.1009 ¶[0239]. Thus, the system supervises individuals through location information evaluated against defined geographic areas. Ex.1009, ¶¶[0037], [0176], [0244]. In my opinion, that is "a method for facilitating supervision of individuals based on geofencing," and limitation 1[pre] is disclosed.

a. ***1[a]: "receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor;"***

335. For limitation 1[a], the communication device = the communications function (including programs, middleware, and software) of emergency response computer system 101, including device communications module 151, notification module 155/1655, administration module 157, alert reception module 153, and the communications modules shown in Fig. 22, which includes network adapter 2220, keyboard adapter 2226, mouse adapter 2206, and other input/output devices 2222 coupled to the system bus 2214. Rauner states that device communications module 151 communicates with remote computing devices 102, 103, and 104 using

communications network 108, and receives emergency trigger messages from users through those devices. Ex.1009 ¶[0067]. Rauner's summary likewise describes "a device communications module configured to run on a first processor" and "configured to receive two or more emergency trigger messages from one or more users via the two or more sending computing devices." Ex.1009 ¶[0034].



Ex.1009, Figs. 1 and 8 (annotated).

336. The at least one supervisor device = the system administrator's terminal interface (as shown in Fig. 8, for example), PSAP computers, and the first and second level response unit devices. Rauner explains that the emergency response computer system is hosted in the cloud and accessed by PSAP computers through an online browser application and web browser interface. Ex.1009 ¶[0031]. Rauner identifies first level response units such as police, fire, and ambulance services, and second level response units such as government officials and university

administrators. Ex.1009 ¶¶[0057]-[0058]. Rauner further states that device communications module 151 notifies the appropriate first and second level response units through communications network 108. Ex.1009 ¶[0137]. For limitation 1[a], the relevant supervisor device is the system administrator's terminal interface, because that is the device through which the administrator enters the configuration inputs.

337. The security parameters include administrator-designated mass event trigger words and Clery event trigger words, distance thresholds, mass event triggers, and escalation rules.[2] Rauner states that administration module 157 gives the system administrator the ability to designate mass event trigger words. Ex.1009 ¶[0089]. Rauner separately states that administration module 157 gives the administrator the ability to designate Clery event trigger words. Ex.1009 ¶[0090]. These are supervisor-selected configuration inputs that determine which incoming communications are treated as security-related events and what reporting or escalation workflow follows.

338. Rauner also supplies the predetermined trigger-word list itself: "homicide, murder, slaughter, rape, assault, arson, fire, weapon, gun, shoot,

[2] Clery event trigger words are a campus safety tool that was created in response to The Cleary Act that "requires colleges and universities to report campus crime data, support victims of violence, and publicly outline the policies and procedures they have put into place to improve campus safety." Ex.1029.

shooting, rifle, pistol, kill, handgun, bomb, explosion, gas, flood, earthquake, rob, steal, burglar, burglary, stolen car, stole car, stole my car, drug, cocaine, marijuana, and/or heroin." Ex.1009 ¶[0076]. This is security-oriented configuration input because it determines which message content triggers emergency analysis and escalation.

339. Rauner further states that administration module 157 allows the administrator to set "predefined thresholds for various system functionalities, *e.g.*, mass event trigger limits such as number of messages within a set time." Ex.1009 ¶[0092]. These thresholds calibrate when the system treats a collection of communications as a mass security event and therefore govern the system's response to security events.

340. Those inputs therefore provide security information that a POSITA could use to determine which geographic areas warrant monitoring and which response level should be used.

341. For the receiving, Rauner states that administration module 157 runs on processing unit 161 and is used by a system administrator to administer and control emergency response module 150. Ex.1009 ¶[0085]. Because the module runs on the server-side processing unit, the configuration application and its saved configuration data reside in the emergency response computer system rather than on the administrator's terminal.

342. Rauner states that the system "operates as a cloud computing environment which is accessed by the PSAP computers through an online browser application" and "is hosted in the cloud and is accessed by the PSAP computers through a web browser interface." Ex.1009 ¶[0031]. This is a client-server architecture: the user's machine provides a browser client, while the emergency response computer system and its modules are remote server-side functions.

343. Rauner describes the administrator's actual configuration operation. In the example for mass event trigger words, "a system administrator logs into administration module 157 and enters configuration page," enters the trigger list, and saves the changes. Ex.1009 ¶[0089]. Rauner similarly states that the administrator can set thresholds through administration module 157. Ex.1009 ¶[0092]. Logging into a server-hosted administration module and entering a configuration page is a remote-access operation.

344. Fourth, because the configuration application runs on the server, the server is reached over a network through a browser, and the administrator logs in remotely to enter the parameters, the administrator's inputs travel from the administrator's terminal across communications network 108 to administration module 157 on the server. Rauner therefore satisfies "receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor."

345. Rauner's disclosure that administration module 157 saves changes to a change log containing the administrator's user information, date, and time further corroborates that the input arrived at the server from a distinct remote user session. Ex.1009 ¶¶[0086], [0089]-[0090]. Thus, limitation 1[a], "receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor," is disclosed.

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

346. For limitation 1[b], the geographical location = the graphical map and geospatial data uploaded by the system administrator through the administrator terminal (part of supervisor device). Rauner states that "graphical representations of a target geographical area (*e.g.*, graphical maps) are uploaded into database(s) of storage device 162 and published for display to a display apparatus graphical user interface." Ex.1009 ¶[0094]. This is a geographic input supplied through the administrative interface and received into the system's storage and mapping workflow.

347. Rauner further states that "the system administrator is prompted to give the map a name (*e.g.* Main Campus)" and that mapping module 158 "loads geospatial location of target geographical area." Ex.1009], ¶¶[0094]-[0095]. A named map containing geospatial coordinates is a geographical location received

from the supervisor device. The communication device and receiving pathway is the same as for limitation [1]a. Accordingly, limitation 1[b], "receiving, using the communication device, a geographical location from the at least one supervisor device," is disclosed.

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

348. For limitation 1[c], the processing device = processing unit 161 and its constituent modules, including processing module 152/1652, analyzing module 163, response module 154, determination module 156/1666, and mapping module 158.

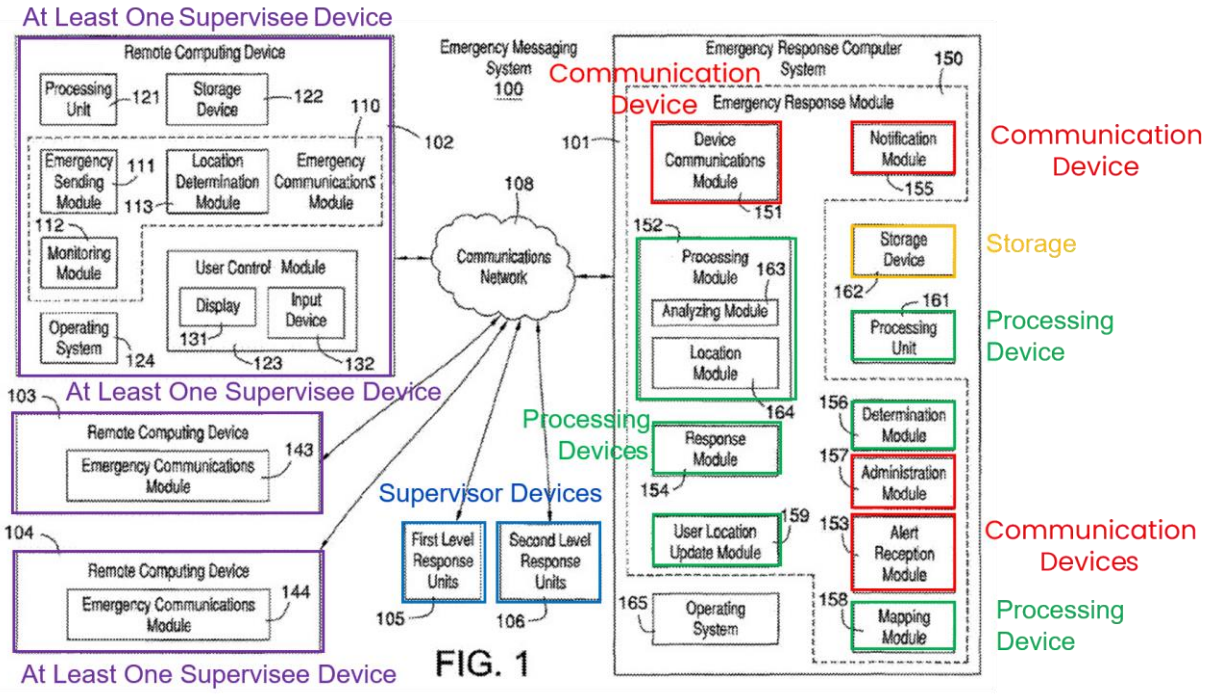


FIG. 1

Ex.1009, Fig. 1 (annotated).

349. Rauner teaches that an administrator configures the security parameters through administration module 157 as part of the same setup process in which the

administrator uploads maps, selects buildings and features, and defines monitored areas. Ex.1009, ¶¶[0076], [0089]-[0090], [0092]-[0094]. Rauner states that mapping module 158 lets the administrator select areas such as buildings, floors, parks, and zones from a graphical display, and that the administrator can identify a structure or feature by clicking on the map, using a draw dialogue, or using a drag-and-select dialogue. Ex.1009 ¶¶[0093]-[0094].

350. Mapping module 158 then "calculates a coordinate range for the space inside the map building feature and associates that coordinate range with that map building/feature." Ex.1009 ¶[0094]. This is analysis of the received geographic location because mapping module 158 converts the administrator's selected map feature into a coordinate range that the system can use. The analysis is "based on" the security parameters because the administrator's trigger words, Clery terms, thresholds, and escalation rules determine which areas are selected, monitored, and associated with security events. The geographic location and security parameters are therefore integrated inputs to a single monitoring configuration.

351. Rauner also uses security information to determine which geographic areas warrant monitoring. It states that the system "compares the geographic area identified in NOAA's tornado warning with all stakeholder defined areas" and "compares the content" of the warning "to select appropriate emergency plans(s)." Ex.1009 ¶[0218]. This is security-driven geographic analysis because the content of

a threat warning defines the relevant geographic area and the system evaluates that area against administrator-defined locations.

352. Additionally, Rauner's processing device jointly analyzes message locations against the administrator-configured security parameters to determine response levels. Rauner states that "response module 154 can determine the appropriate potential level of response to the emergency trigger messages based at least partially upon the frequency and content of the emergency trigger messages and location of the sending of the emergency trigger messages." Ex.1009 ¶[0079]. The quoted passage expressly evaluates location and security-related message content together, so it is analysis of geographical location based on security parameters.

353. Rauner also determines whether trigger messages "included one or more of the predetermined trigger words and if the emergency trigger messages including the predetermined trigger words were sent from locations within a predetermined distance of each other." Ex.1009 ¶[0121]. The predetermined trigger words are security parameters, and the predetermined distance is a location-related threshold. Evaluating both against the message locations is therefore an analysis of the geographical location based on the security parameter. Rauner's response module assigns a second-level response when a predetermined number of trigger messages are sent from locations within a predetermined distance of each other, for

example ten messages containing the trigger word "gun" sent within 500 meters. Ex.1009 ¶¶[0123]-[0124], Claim 8.

354. Finally, Rauner's Claim 8 states the same correlation by reciting a set of "predetermined trigger words," a "predetermined distance between locations," and a "predetermined frequency of emergency trigger messages" as the conditions used to identify the first level or both first and second level response units. Ex.1009, Claim 8. These are further examples of Rauner's analysis of geographic location using security parameters. Thus, limitation 1[c] is disclosed.

d. ***1[d]: "generating, using the processing device, a geofence corresponding to a geographical area based on the analyzing;"***

355. For limitation 1[d], the processing device is the same as limitation 1[c], and the geofence corresponding to the geographical area = the geographic boundary generated from the administrator's selected area and configuration inputs described in 1[b] and 1[c]. Ex.1009, ¶¶[0093], [0239], [0215], [0244]. Rauner discloses "creating a geofence defined by the geographic footprint of a given building and cross referencing the location defined by that geofence with a location based event to select the appropriate building plan/schematic(s) to be made part of the distribution of the triggering event." Ex.1009 ¶[0215]. A geographic footprint is a defined geographic area, and creating the geofence from that footprint is generation of a geofence corresponding to that area.

356. Rauner further states that "Geofences are graphic representations of a defined geographic area that can be manually or automatically created within a Community maintained on the system." Ex.1009 ¶[0239]. The generation flows from the administrator's received map and geographic selection in limitation 1[b] and the security-based analysis in limitation 1[c], because mapping module 158 processes those inputs to produce the geographic representation. Thus, the generated geofence "correspond[s] to a geographical area based on the analyzing," and limitation 1[d] is disclosed. *Id.* ¶¶[0089]–[0094].

e. ***1[e] : "receiving, using the communication device, at least one supervisee data associated with a supervisee from at least one supervisee device;"***

357. For limitation 1[e], the communication device is the same as limitation 1[a] (specifically, the device communications module 151 for this limitation), the supervisee device = remote computing devices 102, 103, and 104, and the supervisee data = the emergency trigger message and location information sent by those devices. Rauner states that, after a user submits an emergency trigger message and emergency sending module 111 receives current location information from location determination module 113, "emergency sending module 111 sends the emergency trigger message and the current location information to device communications module 151 over communications network 108." Ex.1009 ¶[0111].

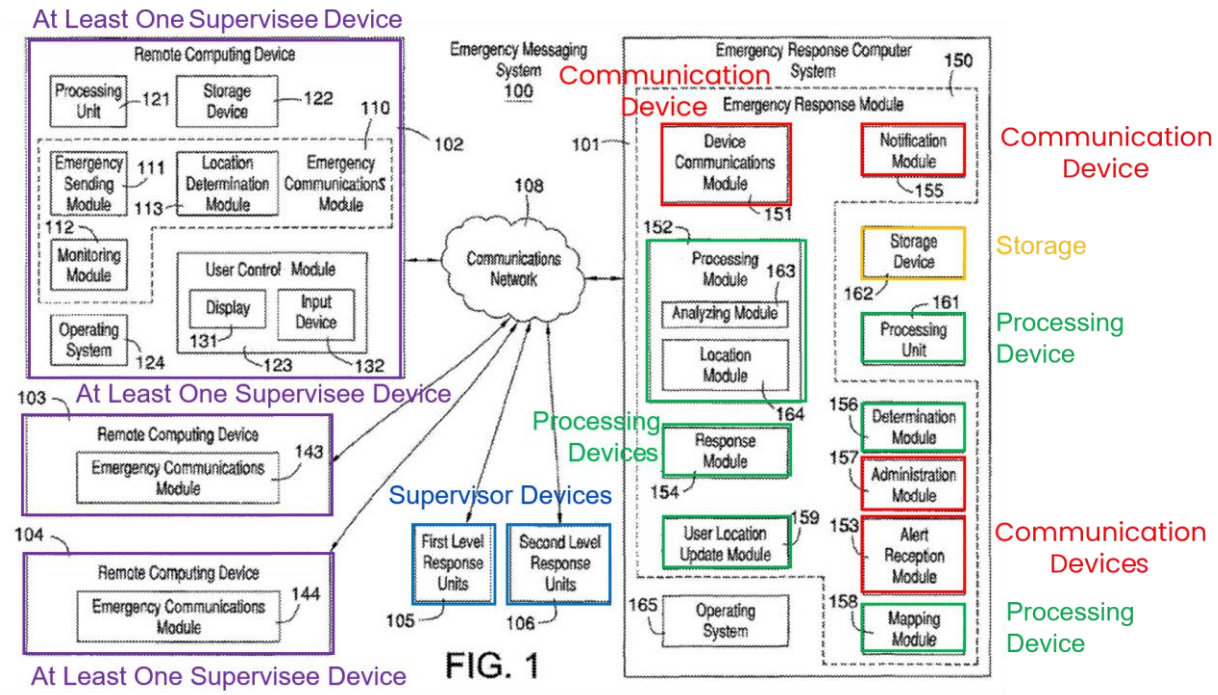


FIG. 1

Ex.1009, Fig. 1 (annotated).

358. Rauner also discloses that remote computing devices 102, 103, and 104 "can periodically communicate their locations to emergency response module 150, which can store their locations in storage device 162." Ex.1009 ¶[0117]. Rauner further states that location determination module 113 determines location "at predetermined intervals (*e.g.*, ten seconds, one minute, ten minutes, and one hour intervals)." Ex.1009 ¶[0182]. This periodic location reporting is data associated with the individual using the device and independently satisfies receipt of "at least one supervisee data" from a supervisee device. Thus, limitation 1[e] is disclosed.

f. ***1[f]: "analyzing, using the processing device, the at least one supervisee data based on the geofence;"***

359. For limitation 1[f], the processing device is the same as limitation 1[c].

360. Rauner states that the system uses a geofencing tool to define an area for census generation and automatically generates a report by "cross referencing the area indicated by the geofence and the locations associated with the individuals." Ex.1009 ¶[0244]. The input locations are the locations associated with the individuals using remote computing devices 102-104, and the comparison reference is the area indicated by the geofence. Cross-referencing those two inputs is analysis of supervisee data based on the geofence.

361. Rauner also discloses that structure module 1657 accesses a database containing the locations of remote computing devices 102, 103, and 104 and "can determine whether any of remote computing devices 102, 103, or 104 are located in the structure at the emergency location." Ex.1009 ¶[0198]. The surrounding disclosure explains that a responder can draw a polygon onto a GPS-integrated map to overlay a building's footprint and that device locations can be plotted into a building schematic using X, Y, and Z axis information. Ex.1009 ¶¶[0197]-[0198].

362. In my opinion, comparing a device location to the polygon or building footprint that defines the geofence is an example of the claimed analysis of supervisee data based on the geofence because the processing device evaluates the device locations against the selected geographic boundary to determine which individuals are within the relevant area. Rauner also describes processing current

location information to identify "one or more affected devices" within a selected geographic area. Ex.1009 ¶[0037].

363. Rauner also states that association module 1667 can associate geographic areas with emergency response units and that the system can determine the response unit associated with a remote computing device's current location, including when a device moves from one geographic area to another. Ex.1009 ¶¶[0176], [0188]-[0189]. That location-to-area association is another processing-device analysis of supervisee location data based on the geofence.

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

364. For limitation 1[g], the processing device is the same as for limitation 1[c]. Rauner states that analyzing module 163, response module 154, determination module 156, and notification module 155 run on processing unit 161 and work together to analyze incoming emergency trigger messages and determine whether a mass event has occurred. Ex.1009 ¶¶[0076], [0078]-[0082]. The supervision notification is generated as the output of that analysis, so it is "based on the analyzing of the at least one supervisee data."

365. Rauner describes a notification form in which the emergency response module receives a "911 call initiated notice message" containing "unique user ID, user name from profile, user location, time, date, call path, time to process call."

Ex.1009 ¶[0050]. This notice contains the supervisee's identity, location, and event information. Because the message is populated and processed after the user's emergency communication is received, it is a supervision notification generated from the analysis of supervisee data.

366. Rauner also describes a mass event warning message. It states that analyzing module 163, response module 154, and determination module 156 analyze content, time, and frequency of message events and that, when the number of events meets a predefined threshold, notification module 155 creates a mass event warning message containing user names, IDs, locations, message or call times, message types, and message content. Ex.1009 ¶¶[0082]-[0083]. The warning is generated after the processing device analyzes the incoming supervisee communications and determines that the threshold has been met, which satisfies the "based on the analyzing" requirement.

367. Rauner further produces reports containing device locations and user profile information. Rauner's Claim 1 recites producing a report with a set of device locations, and Claim 6 recites providing user profile information with those locations, including a name and phone number. Ex.1009, Claims 1 and 6. These reports are generated after the system determines which devices and individuals are within the relevant geographic area, so the report is a supervision notification based on the analysis of supervisee data. Accordingly, limitation 1[g], "generating, using

the processing device, a supervision notification based on the analyzing of the at least one supervisee data," is disclosed.

h. ***1[h]: "transmitting, using the communication device, the supervision notification to the at least one supervisor device; and"***

368. For limitation 1[h], the communication device is the same as limitation 1[a]. Rauner states: "response module 154 can communicate to device communications module 151 which first and second level response units to notify. Device communications module 151 can notify the appropriate first and second level response units via communications network 108." Ex.1009 ¶[0137].

369. Rauner also transmits notifications to the system administrator. The "911 call initiated notice message" is "transmitted to a system administrator contact." Ex.1009 ¶[0050]. Notification module 155 "transmits subscriber emails designated for receipt of emergency messages." Ex.1009 ¶[0083].

370. Rauner further states that the system distributes the "prepared Community alert and report to selected system administrators." Ex.1009 ¶[0119]. Rauner's Claim 1 likewise recites "communicating the report through the communications module to a system user." Ex.1009, Claim 1. Both disclosures describe transmission of a location-based supervision notification through the communications module to a supervisor-facing user.

371. The notification module also forwards the emergency trigger message and location information to the appropriate emergency response unit. Ex.1009 ¶[0168]. In my opinion, Rauner's first and second level response units are examples of the claimed "supervisor device." Rauner explains that the first level response units "can include local police departments, fire departments, ambulance services, and local emergency response teams." Ex.1009, ¶[0057]. Rauner further explains that the second level response units "can be one or more people or groups that are responsible for making decisions regarding distribution of information about an emergency" and "can include local or state government officials, local police or fire chiefs, local and state government disaster agencies, or other officials." *Id.*, ¶[0058]. Therefore, Rauner's first and second level response units comprise supervisors from the local police department and other emergency services, as well as higher level supervision from government agencies, department heads, and elected officials. Thus, limitation 1[h], "transmitting, using the communication device, the supervision notification to the at least one supervisor device," is disclosed.

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

372. For limitation 1[i], the storage device = storage device 162 and its databases. Rauner stores supervisee data. Location module 164 can store received locations in a database of storage device 162. Ex.1009 ¶[0075]. Rauner also states

that remote computing devices periodically communicate their locations to emergency response module 150, which can store those locations in storage device 162. Ex.1009 ¶[0117]. These stored locations are the received supervisee data.

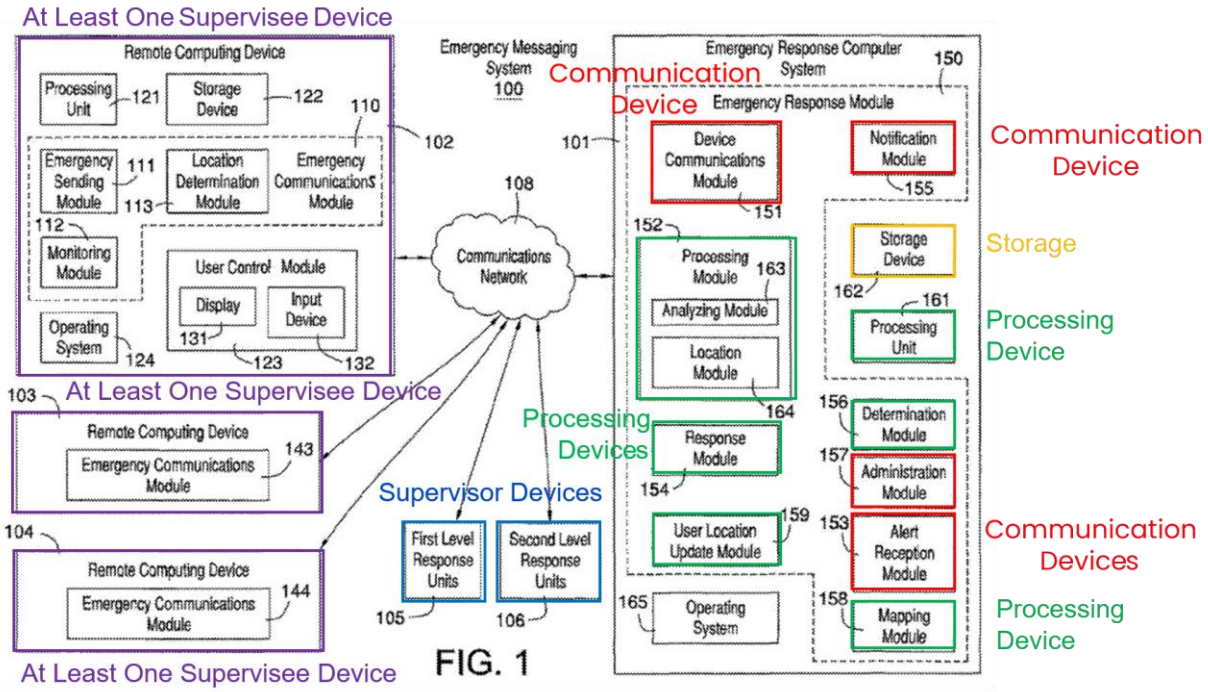


FIG. 1

Ex.1009, Fig. 1 (annotated).

373. Rauner also stores user profiles containing information associated with the individuals and their devices, including name, age, residence, email address, phone number, emergency contact information, current location, and past locations. Ex.1009 ¶[0099]. Rauner explains that past-location history may be retained for selected periods, including days, weeks, or months. The profile and location records therefore independently confirm storage of supervisee data.

374. Rauner stores the supervision notification as well. The 911 call initiated notice message is "recorded into an event log." Ex.1009 ¶[0050]. Rauner further

states that notification module 155 can enter a mass event warning message into a subscriber's message log in a database of storage device 162. Ex.1009 ¶[0083]. The event log and message log preserve the generated notifications in storage device 162, so both categories required by limitation 1[i] are stored. Accordingly, "storing, using a storage device, the at least one supervisee data and the supervision notification" is disclosed.

j. ***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:"***

375. For limitation 1[j], the combination of Rauner and Azmoodeh supplies the geofence area and the structural subdivision into geofence grid boxes. Rauner's alphanumeric grid functions as a coordinate overlay on a graphical representation: mapping module 158 "creates an alphanumeric grid over the graphical representation," translates grid coordinates to GPS coordinates, and associates GPS coordinates within the grid box. Ex.1009 ¶[0094]. Rauner's disclosure is therefore a coordinate overlay and correlation tool.

376. Azmoodeh fills that gap. It teaches that "the mutable geo-fence system divides the geo-fenced area into a grid that comprises a set of cells, where each cell represents portions (in some instances the portions are equal) of the physical location

within the geo-fenced area, and wherein the set of cells sum to make up the whole physical location encompassed by the geo-fence." Ex.1010 ¶[0022]. Azmoodeh's claim 1 likewise recites "dividing the first region encompassed by the geo-fence into a set of cells, each cell among the set of cells representing a portion of the first region." Ex.1010, Claim 1. Each cell is therefore a discrete geofence grid box characterized by its own grid box geofence area, and the cells collectively correspond to the entire geofence area.

RAVE/MSI, EX1005, p. 230

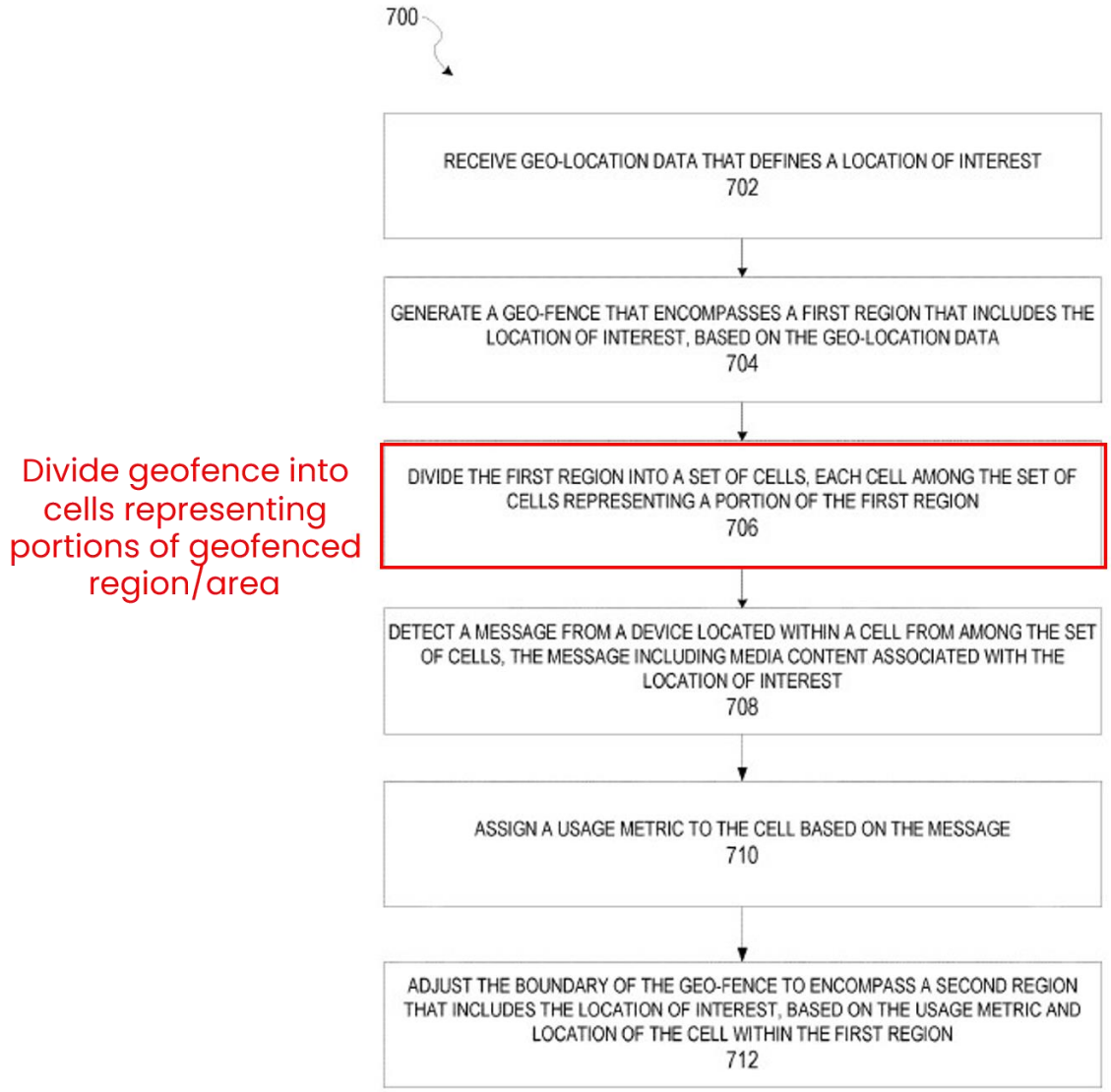


FIG. 7

Ex.1010, Fig. 7 (annotated).

377. In the combination, Azmoodeh's cells subdivide Rauner's geofence, while Rauner supplies the emergency-response geofence, map substrate, and coordinate processing. Therefore, Rauner's geofence and associated grid overlay supply the geofence area corresponding to the geographical area; Azmoodeh's teaching that grid cells structurally subdivide that geofence supplies the plurality of

geofence grid boxes associated with the geofence area; each such cell represents a defined portion, which is the grid box geofence area of the geofence area; and the cells together cover the whole. A POSITA would have made that combination for the reason stated above: adding discrete cells lets Rauner locate a device within a selected campus, building, or other geographic area with a granularity appropriate to the emergency response. The combination therefore discloses "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."

k. ***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:"***

378. For limitation 1[j][1], the grid parameter = the supervisor's input defining the cell count of Azmoodeh's cells. Azmoodeh states that the region encompassed by the geo-fence is divided into a set of cells and that "the number of cells within the region may be defined based on a size of the geo-fence, or based on user input." Ex.1010 ¶[0046]. The user-supplied cell count is a parameter that controls the grid.

379. In the combined system, the grid parameter is received by the communication device as mapped in limitation 1[a]. Administration module 157 is

the component of that communication device through which the administrator enters the grid-calibration input. Rauner states that administration module 157 runs on processing unit 161 and allows the system administrator to administer and control emergency response module 150. Ex.1009 ¶[0085]. The administrator logs into administration module 157, enters a configuration page to enter values, and saves the changes; mapping module 158 provides the graphical interface through which the administrator selects and calibrates the mapped area, including grid recalibration on zoom. Ex.1009 ¶¶[0089], [0092]-[0093]. Because the system is cloud-hosted and reached through a browser, the inbound configuration traffic crosses communications network 108 to the server and reaches administration module 157. Ex.1009 ¶[0031]. A POSITA would have had a reasonable expectation of success in adding this input to Rauner's existing administrative interface for the reason that Rauner already receives map, feature, and configuration inputs through that interface, so the new value would use an existing input and communications path rather than require a new architecture. Thus, limitation 1[j][1] is rendered obvious.

l. ***1[j][2]: "analyzing, using the processing device, the at least one grid parameter;"***

380. For limitation 1[j][2], the processing device is the same as limitation 1[c], and specifically for this limitation the mapping module 158 component. Rauner's mapping module already computes on grid data: it "creates an alphanumeric grid over the graphical representation," "translates grid coordinates to

GPS coordinates," and "associates GPS coordinates within the grid box." Ex.1009 ¶[0094]. That existing processing establishes that Rauner's processing device accepts a grid-related input and converts it into coordinate-referenced map data.

381. In the combined system, Azmoodeh's geo-fence module processes the user-supplied cell count or cell size to define how the first region is subdivided. Azmoodeh states that the number of cells may be based on user input. Ex.1010 ¶[0046]. Processing the user's resolution input to determine the subdivision is "analyzing ... the at least one grid parameter." A POSITA would have expected success for the reason that the input is a numerical or otherwise defined resolution value applied to the coordinate-referenced region already handled by Rauner's mapping module. Accordingly, limitation 1[j][2] is rendered obvious.

m. ***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"***

382. For limitation 1[j][3], the processing device is the same as for limitation 1[c] and the grid box geofence area is the same as for limitation 1[j]. Rauner's mapping module "calculates a coordinate range for the space inside the map building feature and associates that coordinate range with that map building/feature" and "translates grid coordinates to GPS coordinates and associates GPS coordinates within the grid box." Ex.1009 ¶[0094]. This establishes the coordinate-range operation needed to associate a defined geographic area with a map subdivision.

Azmoodeh adds that each cell represents a portion of the physical location within the geo-fenced area and that the cells sum to the whole physical location encompassed by the geo-fence. Ex.1010 ¶[0022].

383. In my opinion, determining and associating coordinates with grid boxes and assigning a geographical location to each grid box determines what area that box covers. And that determining of the grid box geofence area is based on the analysis of the grid parameter because generating a different number of boxes over the same geographic extent changes the area represented by each box.

384. The combined system therefore discloses "determining, using the processing device, the grid box geofence area based on the analyzing of the at least one grid parameter." The determination follows from applying the selected cell count or size to the fixed geographic extent: a finer resolution yields smaller cell areas (grid boxes), while a coarser resolution yields larger cell areas (grid boxes).

n. ***1[j][4]: "generating, using the processing device, a number of geofence grid boxes based on the determining."***

385. For limitation 1[j][4], the processing device is the same as limitation [1c], and the number of geofence grid boxes = the number of cells generated over Rauner's geofence based on the cell count input. Rauner's mapping module creates "an alphanumeric grid over the graphical representation." Ex.1009 ¶[0094]. Azmoodeh's Claim 1 teaches dividing the first region encompassed by the geo-fence

"into a set of cells, each cell among the set of cells representing a portion of the first region," and the specification explains that the number of cells may be defined by user input. Ex.1010, Claim 1; *id*. ¶[0046].

386. The number of boxes is based on the determining because, once the grid-box area is selected over the geofence, the number of boxes needed to cover that extent follows from the area relationship. More boxes correspond to smaller areas at finer resolution; fewer boxes correspond to larger areas at coarser resolution. Thus, the combination meets "generating, using the processing device, a number of geofence grid boxes based on the determining."

387. Rauner's grid and Azmoodeh's cells are both defined over a coordinate-referenced graphical map. Applying Azmoodeh's structural subdivision to Rauner's existing mapping framework therefore requires no change to Rauner's mapping architecture: the same coordinate ranges, GPS translations, and map associations can be used to define the cell boundaries and identify the cell containing a device. That shared teaching supplies both the reason to combine the teachings and the reasonable expectation of success.

388. In my opinion, the combination of Rauner and Azmoodeh discloses or renders obvious each limitation of method claim 1.

RAVE/MSI, EX1005, p. 236

4. Claim 2

389. Claim 2 is disclosed by Rauner in view of Azmoodeh for the reasons discussed below.

a. ***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;"***

390. For limitation 2[a], a named building, feature, or pin-drop zone inside that map of limitation 1[b] is a further location indication associated with that same geographical area. Also, an uploaded schematic associated with a geofenced building is also a further location indication associated with the geographical area.

391. First, Rauner states that "the system administrator can identify a structure or feature of the map in several ways, including by clicking on the map to select a discrete feature, using a draw dialogue, or a drag and select dialogue." Ex.1009, ¶[0094]. This describes a supervisor selecting a particular building or feature inside the previously uploaded geographical map, so the selected feature is a specific location indication associated with the broader geographical area. Rauner then states that, after the administrator identifies the feature and provides a name, "mapping module 158 populates the name to a list of locations associated with that map." The named-location list catalogs particular location indications tied to the map.

392. Second, Rauner discloses pin-drop zones. It states that a manual pin-drop location creation mechanism may be used "to create ad hoc geographic area selection zones," and that, after pins are dropped, a dialogue box prompts for a location name that populates the locations list. A named ad hoc zone is a designation of a particular location within the mapped area, so it independently satisfies "at least one location indication associated with the geographical area." Rauner's claim 2 provides a further confirmation by reciting "retrieving from the database a predefined zone or campus from an administrator, and receiving through a graphical interface of the emergency response computer system an ad hoc selected region." The predefined zone and the ad hoc selected region are both supervisor-supplied location designations associated with the geographic area.

393. The receiving limitation is satisfied for the same reasons as limitation 1[a]. Ex.1009 ¶¶[0031], [0085], [0094]. Limitation 2[a], "receiving ... at least one location indication associated with the geographical area from the at least one supervisor device," is disclosed.

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

394. For limitation 2[b], I map "identifying, using the processing device, at least one location corresponding to the at least one location indication" to mapping module 158's conversion of each named feature or ad hoc zone into usable

geographic coordinates. Rauner states that "mapping module 158 calculates a coordinate range for the space inside the map building feature and associates that coordinate range with that map building/feature (within a predefined coordinate tolerance range)." Ex.1009, ¶[0094]. The calculated coordinate range is the location corresponding to the administrator's indication because it translates the named designation into a specific geospatially identified location that the system can use for monitoring. Limitation 2[b] is therefore disclosed.

395. Rauner further states that mapping module 158 "translates grid coordinates to GPS coordinates and associates GPS coordinates within the grid box." This shows that the processing device converts the graphical designation into a usable geospatial representation. Rauner also discloses that GPS or location-coordinate information may be translated into "Military Grid Reference System (MGRS)" and that the GPS, coordinate, and MGRS information "can be stored in user profiles ... in a database of storage device 162." *Id.* ¶[0070]. Those coordinate translations and stored representations further demonstrate that the processing device identifies a location corresponding to the location indication. Thus, "identifying ... at least one location corresponding to the at least one location indication" is disclosed.

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

396. For limitation 2[c], the processing device is the same as limitation 1[c] and 1[f], but at the granularity of the identified discrete location rather than the geofence as a whole. Rauner states that structure module 1657 "can determine whether any of remote computing devices 102, 103, or 104 are located in the structure at the emergency location." Ex.1009, ¶[0198]. This is a per-location analysis of the supervisee data because it determines whether each supervisee device is inside the particular identified structure. Limitation 2[c] is disclosed.

397. Rauner also states that determination module 156 uses stored device location information "to determine which remote computing devices 102, 103, and 104 are within a certain predetermined distance of the emergency." *Id.* ¶[1039]. The system consequently evaluates supervisee location data against a specific emergency location and determines which devices are proximate to that point. That proximity analysis is analysis "based on the at least one location." Thus, the processing device is "analyzing ... the at least one supervisee data based on the at least one location," and limitation 2[c] is disclosed.

398. Finally, determination module 1666 tracks movement between identified geographic areas. Rauner explains that, when a device moves from geographical area 1807 to geographical area 1808, determination module 1666

changes the emergency response unit associated with the device from the first unit to the second unit and stores that information in storage device 162. *Id.* ¶[0175]. This evaluates the supervisee device's location data against identified areas and changes the system's handling based on the area in which the device is located. Thus, the processing device is "analyzing ... the at least one supervisee data based on the at least one location," and limitation 2[c] is disclosed.

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."***

399. For limitation 2[d], the processing device is the same as limitation 1[c], and the "location anomaly" corresponds to determining threat escalation events and spatial clustering escalation events. Rauner states that the frequency trigger for emergency call or text events creates a Threat Escalation Event by monitoring the number of events "for a defined geographic location" and creating the event "when the frequency of call/text events exceeds a defined threshold." *Id.* ¶[0208]. Determining that activity at a particular location exceeds the defined threshold is a determination that activity is anomalous relative to the expected baseline for that location. In my opinion, Rauner's "Threat Escalation Event" meets the claimed "location anomaly."

RAVE/MSI, EX1005, p. 241

400. Additionally, Rauner describes a content-based Threat Escalation Event. Rauner states that the content trigger creates a secondary event by monitoring emergency call or text content "for a defined geographic location" and creating a Threat Escalation Event "when the content of call/text events meets defined criteria." The system is therefore determining, for a particular location, whether the supervisee event content crosses a security criterion. That location-specific departure from the configured content condition is likewise a location anomaly.

401. Further, Rauner describes spatial clustering in which the system determines whether trigger messages "were sent from locations within a predetermined distance of each other" and assigns the higher response level if the conditions are met. *Id.* ¶[0121]. Rauner gives the example that, if ten trigger alert messages include the word "gun" and all ten were sent within 500 meters of each other, response module 154 assigns a second level of response. *Id.* ¶[0124]. Rauner's claim 8 likewise correlates "predetermined trigger words," a "predetermined distance between locations," and a "predetermined frequency of emergency trigger messages." A spatial cluster of security-related messages is a location-based anomaly because the concentration of events in that location is itself the abnormal condition.

402. Therefore, it is my opinion that limitation 2[d] is disclosed by Rauner.

403. Rauner's escalation determination drives the response level and the resulting notification: response module 154 determines the level, determination module 156 selects which first and second level response units to notify, and device communications module 151 transmits the resulting notification. This is the same notification framework mapped in limitations 1[g] and 1[h]. Accordingly, the generating of the supervision notification is based on the determining of the location anomaly. Limitation 2[d] is disclosed.

5. Claim 3

a. *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:"*

404. For limitation 3[a], I map the "supervisee event" to Rauner's Emergency Event and the associated action to the emergency response workflow. Rauner states that the system "distributes an 'Emergency Event' that takes the location from the device and pairs it with a profile managed by the user that enables sharing emergency health information, an image, emergency contacts, etc." EX1009, ¶[0208]. This is an event generated from activity on the supervisee's own remote computing device and therefore supplies the claimed supervisee event. Rauner also describes the notice payload as a "911 call initiated notice message" containing "unique user ID, user name from profile, user location, time, date, call path, time to

process call." *Id.* ¶[0050]. Those fields are the event and associated identity, location, and timing data carried in the supervision notification mapped in limitation 1[g], so the notification "comprises at least one supervisee event."

405. Rauner expressly associates that event with an action. It states that the event and profile "are automatically distributed with the emergency communication event to all individuals/entities in an emergency response work-flow defined by the community based on services available for the location ... based on proximity, status, hierarchy, event type, etc." *Id.* ¶[0110]. The workflow is the associated action because it identifies the responders and communications conduct selected for the event. A POSITA would also understand an automatically selected emergency response workflow based on location, status, hierarchy, and event type to be an action associated with the Emergency Event. Limitation 3[a] is disclosed.

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

406. For limitation 3[b], the processing device determines the action based on the supervision notification in multiple ways. First, Rauner states that response module 154 "can determine the appropriate potential level of response to the emergency trigger messages based at least partially upon the frequency and content of the emergency trigger messages and location of the sending of the emergency trigger messages." Ex.1009, ¶[0079]. Determining the emergency response

workflow that is appropriate is a determination of an action based on the supervision notification. Second, selecting the first or second response level is a determination of the action because it determines the type and scope of response that follows from the notification. Rauner further states that determination module 156 uses the location of the emergency trigger messages to "determine which (if any) of first level response units 105 and second level response units 106 to notify." Selecting the appropriate responders is likewise a determination of the action based on the supervision notification.

407. Rauner also states that the system "automatically initiates many to many location integrated communications in response to a trigger event" by building a recipient list based on location, capabilities, and role and initiating a tactical communication exercise. *Id.* ¶[0252]. Building the recipient list and selecting the resulting communication exercise are processing-device determinations made from the incoming supervision notification. Thus, "determining ... the at least one action based on the supervision notification" is disclosed.

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."***

408. For limitation 3[c], the processing device is the same as limitation 1[c], and Rauner states: "The system automatically places the 'caller' and each of the

individuals/entities in the emergency response work-flow into a group messaging in which each of the participating individuals can see shared text based communications from each of the other individuals." Ex.1009, ¶[0110]. The "caller" is the supervisee, the user of remote computing device 102, 103, or 104, and the individuals and entities in the emergency response workflow include the supervisor devices identified in limitation 1[a]. The group messaging session therefore establishes a communication session between a supervisor device and a supervisee device. Placing the caller and the responding entities into a shared group messaging environment is that establishment. The action is performed based on the determination of the response workflow, so the limitation is disclosed.

409. Rauner also states that emergency messaging system 100 "can provide one-way and/or two-way communication between users, administrators of emergency messaging system 100, and emergency response units." *Id.* ¶[0049]. It also describes "opening one-way and/or two-way emergency messaging communication between the emergency messaging services system and the portable communication devices within the selected geographic area." *Id.* ¶[0038]. These disclosures describe session establishment. Rauner additionally discloses directory-based text or instant messaging "based on a tiered system that controls access and group messaging through assigned tier groups," explaining that the group messaging connects emergency responders with users requiring assistance and connects

responders with each other. *Id.* ¶[0044]. That tiered directory structure supplies an additional supervisor-to-supervisee communication path.

410. Finally, Rauner describes "multi-modal many-to-many location integrated communications" shared with an unlimited number of devices in parallel, with each communication including location information, and states that the system automatically initiates those communications in response to a trigger event. *Id.* ¶[0250]. This confirms that the communication session may be text-based, multi-modal, and location-integrated while still being established by the processing system between the selected supervisor and supervisee devices. Accordingly, the action comprises "an establishment of a communication session between the at least one supervisor device and the at least one supervisee device," and the claim 3 limitation is disclosed.

6. Claim 4

411. In my opinion, claim 4 is disclosed by Rauner in view of Azmoodeh.

a. ***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"***

412. For limitation 4[a], the processing device is the same as limitation 1[c], and Rauner states that the 911 call initiated notice message includes "unique user ID, user name from profile." Ex.1009, ¶[0050]. Producing a unique user ID and profile name from the incoming emergency message is an identification of the

supervisee derived from analysis of the supervisee's event and location data. Rauner also states that "The system associates the 'caller's' (user managed) emergency information profile with the emergency communication event." *Id.* ¶[0110]. Associating the event with a specific user profile is an example of the identifying of the supervisee.

413. Therefore, "identifying ... the supervisee based on the analyzing of the at least one supervisee data," is disclosed.

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."***

414. For limitation 4[b], the storage device is the same as limitation 1[i], and I map the claimed supervisee profile data to the profiles stored in storage device 162. Rauner states: "A profile for each portable communication device associated with each user can be stored in one or more databases of storage device 162. The profile may include information of the individual ... such as name, age, residence, email address, phone number, emergency contact information, current location of the user, past locations of the user." Ex.1009, ¶[0099]. Rauner also states that the Emergency Event "pairs it with a profile managed by the user that enables sharing emergency health information, an image, emergency contacts, etc." *Id.* ¶[0208]. That pairing is the claimed retrieval of profile data associated with the identified supervisee.

415. The notification is supported in three ways. First, the 911 notice message includes "user name from profile," showing that notification content is populated from retrieved profile data. *Id.* ¶[0050]. Second, Rauner's claim 6 requires a report including "a name and a phone number for each one of the device users." *Id.* Claim 6. Third, Rauner's census report includes "contact information, current locations, home address and work address for individuals." *Id.* ¶[0244]. Each disclosure shows profile information entering the notification or report after the user is identified. Thus, "the generating of the supervision notification is based on the retrieving," and limitation 4[b] is disclosed.

416. Claim 4 is disclosed.

7. Claim 6

a. ***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;"***

417. In my opinion, claim 6 is disclosed by Rauner in view of Azmoodeh for the reasons discussed below.

418. For limitation 6[a], the communication device is the same as limitation 1[a], and I address two independently sufficient channels. First, Rauner discloses geo-referenced sensor feeds. It identifies "a variety of sensors relevant to emergency communication including traffic, motion/activity, heat, air quality, water quality, radiation levels, moisture, etc." Ex.1009 ¶¶[0212]-[0213]. These sensors produce

data about environmental conditions. Rauner further states that the system "allows creation of georeferenced definition of an area within which the system should monitor location associated sensors for a defined output parameter(s)." *Id.* ¶[0213]. The georeferenced monitoring area ties the sensor data to the geographical area corresponding to the geofence. Thus, the sensor measurements are "environment data associated the geographical area corresponding to the geofence."

419. Rauner's claim 14 recites external electronic monitoring systems "comprised of at least one of a fire alarm, traffic sensors, motion sensors, heat sensors, air quality sensors, water quality sensors, radiation sensors, and moisture sensors" that provide "a feed of sensor information." Ex.1009, Claim 14. The claim language identifies the feed as information supplied by external monitoring systems, so the feed is the claimed environment data associated with the geofenced area. This independently satisfies limitation 6[a] through the geo-referenced sensor channel.

420. For limitation 6[a], the sensor feeds also arrive at the server through the communication device mapped in limitation 1[a]. Network adapter 2220 is the hardware network interface of the computer implementing emergency response computer system 101. Rauner states that "various I/O devices such as a disk controller 2204, a graphics adapter 2224, a video controller 2202, a keyboard adapter 2226, a mouse adapter 2206, a network adapter 2220, and other I/O devices 2222 can be coupled to system bus 2214." *Id.* ¶[0203]. Rauner further explains that

"network adapter 2220" can be coupled to one or more antennas, may be part of a wireless network interface controller card or built into the motherboard chipset, and, in other embodiments, can be a wired network adapter. Ex.1009 ¶¶[0203]-[0205]. A POSITA would have understood an external sensor feed to be received either through device communications module 151, Rauner's software-level network-facing communications component, or through network adapter 2220, the hardware-level network interface on which that module depends, because those are the server's external communications interfaces . The two are complementary layers of one ingress path in that the software module sends and receives over the same physical adapter, so identifying either identifies the claimed receiving structure. Rauner ¶[0068] independently confirms that the communications interface may be "any suitable form of wired or wireless connection including, but not limited to, USB (universal serial bus) connection, serial connection, cellular communication, IEEE 802.11, etc." Ex.1009 ¶[0068]. Thus, limitation 6[a] is disclosed by the geo-referenced sensor channel.

421. Second, Rauner discloses third-party hazard feeds. Alert reception module 153 "can be configured to receive event or alert notifications from ... FEMA, the U.S. State Department ... USGS, ... CDC, ... NOAA, and ... FDA." *Id.* ¶[0069]. Alert reception module 153 is a part of the communication device mapped in limitation 1[a]. The third-party alerts therefore are received using the

communication device. Rauner further describes NOAA tornado warnings identifying "geographic parameters for the area threatened by the storm" and radiation threat warnings for "a defined geographic area." *Id.* ¶[0215]. Each alert is geographically parameterized environment data associated with the geofence. Limitation 6[a] is disclosed by either channel.

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."***

422. For limitation 6[b], the processing device is the same as limitation 1[c], and I analyze both channels described for limitation 6[a]. Rauner states that the "system is designed to consume risk information and turn it into emergency alerts." Ex.1009 ¶¶[0212]-[0213]. Thus, the system receives risk or environmental information, evaluates it, determines whether it represents a threat, and produces an alert. A POSITA would understand "consume risk information and turn it into emergency alerts" to involve analysis of the received information before the alert is produced.

423. First, Rauner states that, when "a sensor(s) within the defined area meets the defined trigger requirements, the data from the sensor(s) is distributed to mobile/web services according to an administrator defined distribution list as an event." Ex.1009 ¶[0213]. Evaluating whether the sensor output meets the defined

trigger requirements is the claimed analyzing of the environment data. It also determines at least one threat because the trigger requirements are the threshold at which a reported environmental condition is treated as dangerous or requiring emergency handling. Thus, the sensor path independently supplies the analysis and the threat determination required by limitation 6[b].

424. Also, Rauner states that the "System processes these external events by comparing the georeferenced event location information to locations for available sensor(s)" and distributes "the emergency warning event along with output from indicted sensor feed(s)." Ex.1009 ¶[0214]. Comparing the hazard's geographic location against the monitored locations is analysis of the received environment data and determines whether the hazard affects the supervised geographic area. Rauner further states that "Threat Information may also be distributed by localized feeds where automated analysis and distribution of threat information [is] based on cross referencing the location associated with the threat and the location of users and/or Communities." *Id.* ¶[0242]. The location cross-reference determines whether the external hazard is a threat to the supervised population, so this path independently satisfies the claim's analysis requirement.

425. The threat determination drives the notification. Rauner states that the system "prepares a report and alert for any indicated Community based on the [external] alert with a prebuilt recipient list" and "distributes the prepared

Community alert and report to selected system administrators." Ex.1009 ¶¶[0118]-[0119]. The report and alert are generated after the system compares the hazard location with user and Community locations and determines which Community is affected. Thus, the generating of the supervisor notification is based on the threat determination. This is the same notification framework mapped in limitations 1[g] and 1[h]. Although this claim uses "supervisor notification" while claim 1 elsewhere uses "supervision notification," the analysis is the same under either reading because the alert and report are transmitted to the selected system administrators and other supervisor devices.

8. Claim 7

426. Claim 7 is disclosed by Rauner in view of Azmoodeh for the reasons discussed below.

a. ***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;"***

427. For limitation 7[a], structure module 1657 is configured to "determine whether a schematic exist for the structure" and to "provide access to the schematic of the structure to emergency response unit(s) 1605." Ex.1009, ¶[0174]. The schematic is the claimed blueprint because it is the facility layout used to understand the emergency location. Rauner further states that structure module 1657 "can determine whether there are any geo-fenced building schematics accessible for the

emergency location by cross-referencing the emergency location with geo-fenced building schematic feeds" and "can query the databases stored in storage device 162." *Id.* ¶[0195]. Querying those databases is retrieval using storage device 162, the storage device mapped in limitation 1[i].

428. The schematic is associated with the geographical area corresponding to the geofence. Rauner contemplates "creating a geofence defined by the geographic footprint of a given building and cross referencing the location defined by that geofence with a location based event to select the appropriate building plan/schematic(s)." *Id.* ¶[0215]. The schematic is selected by reference to the building's own geofence, so it is associated with the geographical area corresponding to that geofence. A POSITA would understand a building plan or schematic selected by the building's geofence to be the blueprint required by the claim. Limitation 7[a] is disclosed.

b. ***7[b]: "analyzing, using the processing device, the blueprint and the at least one supervisee data; and"***

429. For limitation 7[b], structure module 1657 "can access a database in storage device 162 that includes information regarding the locations of remote computing devices 102, 103, and 104" and "can determine whether any of remote computing devices 102, 103, or 104 are located in the structure at the emergency location." Ex.1009, ¶[0198]. The processing device therefore cross-references the locations of the supervisee devices, the supervisee data mapped in limitation 1[e],

against the retrieved building schematic. That joint use of the schematic and the device-location data is "analyzing ... the blueprint and the at least one supervisee data." Limitation 7[b] is disclosed.

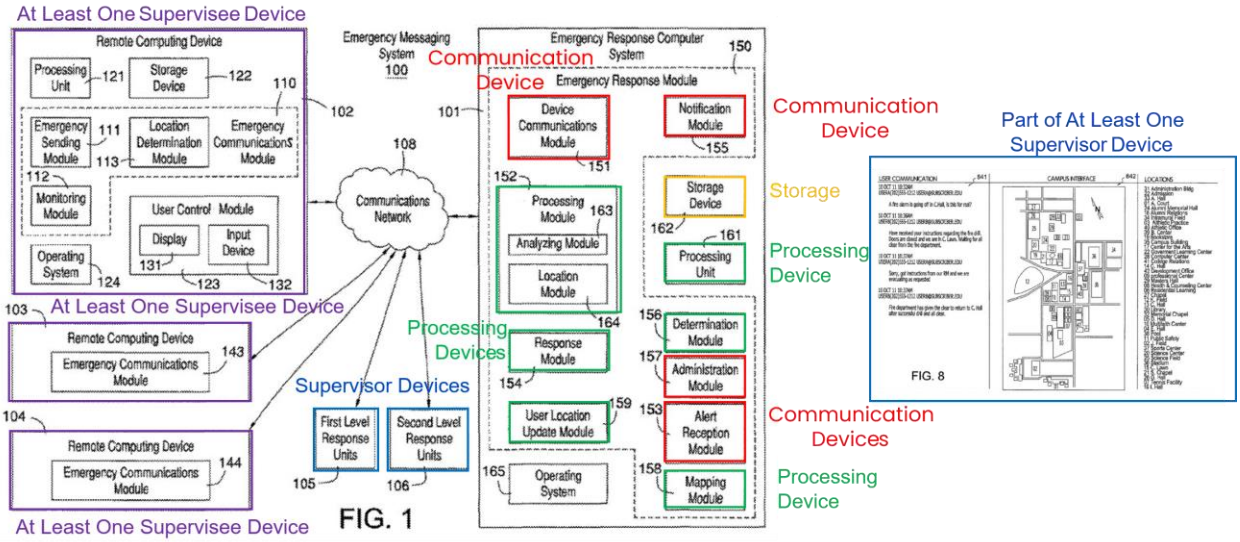
c. ***7[c]: "determining, using the processing device, a location of the supervisee on the blueprint based on the analyzing of the blueprint and the at least one supervisee data, wherein the generating of the supervision data is based on the determining."***

430. For limitation 7[c], structure module 1657 of the same processing device as limitation 1[c] "can plot the locations of any remote computing devices, which are located in the structure, into a building schematic," with "locations of individuals plotted into the schematic using the appropriate X, Y, and Z axis information." Ex.1009, ¶[0198]. Plotting individual locations using X, Y, and Z coordinates is a determination of the supervisee's location on the blueprint based on the analysis of the blueprint and supervisee data. Plotting a device's coordinates onto the schematic determines and represents that location. Limitation 7[c] is disclosed.

431. Structure module 1657 "can be further configured to provide information about a location of one or more persons in the structure to the emergency response units." *Id.* ¶[0174]. The schematic with plotted device locations is delivered to response units through the tactical emergency management interface. In addition, structure module 1657 "can use specific user locations within a building schematic to trigger pre-defined ingress/egress/evacuation plans and provide these to

appropriate emergency response units." *Id.* ¶[0199]. These disclosures show that the location-on-blueprint determination drives both the content of the supervision data, the schematic with plotted locations, and downstream response actions, the evacuation plans, each transmitted to supervisor devices through the notification framework mapped in limitations 1[g] and 1[h].

432. The claim uses "supervision data" in this limitation, whereas claim 1 and the surrounding framework use "supervision notification." Under either reading, Rauner's schematic with plotted locations and the location-triggered evacuation plans satisfy the limitation.



Ex.1009, Figs. 1 and 8 (annotated).

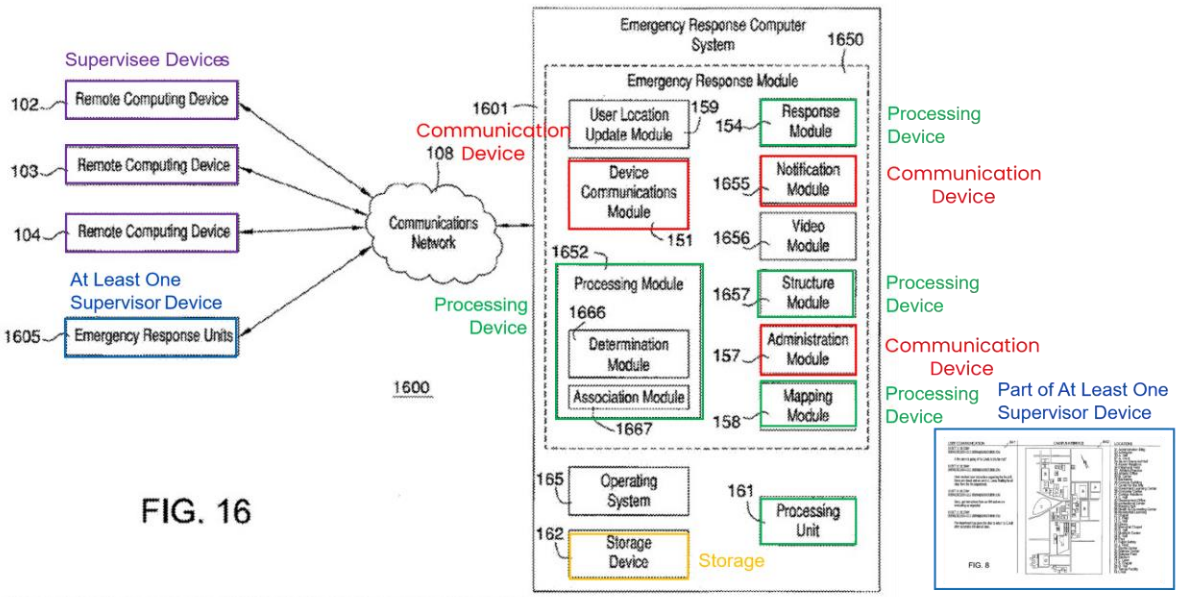


FIG. 16

Ex.1009, Figs. 16 and 8 (annotated).

9. Claim 8

a. 8[a]: "The method of claim 1, wherein: the at least one supervisee device comprises at least one sensor"

433. For limitation 8[a], Rauner's remote computing device 102 is the supervisee device mapped in limitation 1[e]. Rauner states that "Input device 132 can include buttons, a keyboard, a touchpad ... microphone, mouse, trackball, or other input mechanisms." Ex.1009 ¶¶[0061]-[0062]. The microphone is a sensor included in or coupled to the supervisee device. The '757 Patent itself treats a microphone as a sensor of the claimed type, listing "audio sensors (such as a microphone)" among the sensors a supervisee device may comprise. Ex.1001, 24:39-43. Thus, the limitation is disclosed.

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

434. For limitation 8[b], I rely on the microphone and a voice signal made by the supervisee. Rauner states that "the emergency trigger message can be a sound recording, and the user can record the emergency trigger message using input device 132." Ex.1009, ¶[0105]. Rauner repeats the same disclosure in the second embodiment, stating that the emergency trigger message can be a sound recording and that the user can record it using input device 132. The user's own recorded voice is a signal made by the supervisee, and the microphone on the supervisee's own device detects that signal. The disclosed input device is configured to receive the user's sound recording, so the limitation is disclosed.

435. A voice recording is affirmatively produced by the person. Therefore, Rauner's disclosure directly identifies the user as the source of the recorded sound. Thus, "the at least one sensor is configured for detecting at least one signal made by the supervisee" is disclosed.

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

436. For limitation 8[c], Rauner states that emergency sending module 111 sends the emergency trigger message and the current location information to device communications module 151. The audio recording captured by the microphone therefore becomes the emergency trigger message, the supervisee data mapped in

limitation 1[e], and is transmitted to the processing device for analysis. Rauner further states that "a device communications module can convert the audio recording into text." Server-side transcription for analysis by the processing modules confirms that the recording is the operative supervisee data. Accordingly, the sensor generates "the at least one supervisee data based on the detecting," and limitation 8[c] is disclosed.

437. Taken together, the microphone detects the supervisee's recorded voice, emergency sending module 111 transmits the resulting emergency trigger message and location, and device communications module 151 converts the recording for processing. The claimed sensor, signal, and generated supervisee data are therefore present in the same operational path so claim 8 is disclosed.

10. Claim 10

a. ***10[pre]: "A system for facilitating supervision of individuals based on geofencing, the system comprising:"***

438. In my opinion, claim 10 is the system counterpart to method claim 1 and is disclosed for the same reasons. It recites a communication device, processing device, and storage device "configured for" the same functions recited as active method steps in claim 1, and it incorporates the same grid-parameter limitations in 1[j] through 1[j][4]. Applicant agreed during prosecution that the generic "communication device," "processing device," and "storage device" are subject to

§112(f) and correspond to standalone functions inside a server computer, simple programs and databases. Ex.1004, 207-208. I therefore apply the same mappings discussed above. Ex.1009 ¶¶[0067], [0069], [0081], [0085], [0203]-[0204].

b. ***10[a]: "a communication device configured for:"***

439. For limitation 10[a], Rauner discloses that structure as described for 1[a]. Ex.1009 ¶¶[0067], [0081], [0085], [0137].

c. ***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;"***

440. Limitation 10[a][1] corresponds to limitation 1[a], incorporated here. The communication device performs the function of 1[a]. Thus, Rauner meets 10[a][1].

d. ***10[a][2]: "receiving, using the communication device, a geographical location from the at least one supervisor device;"***

441. Limitation 10[a][2] corresponds to limitation 1[b], incorporated here. The communication device performs the function of 1[b]. Thus, Rauner meets 10[a][2].

e. ***10[a][3]: "receiving at least one supervisor data associated with a supervisee from at least one supervisee device; and"***

442. Limitation 10[a][3] has the issued-text discrepancy addressed in the Ground 1 analysis: it recites "supervisor data associated with a supervisee from at

least one supervisee device," although the remainder of claim 10 refers to supervisee data. On the antecedent basis in the remainder of the claim, I understand this to refer to the supervisee data corresponding to limitation 1[e], incorporated here, and the analysis is identical to 1[e], and the data received from the supervisee device is routed to supervisor devices, so it includes data provided for or concerning the supervisor. Thus, under either reading, the communication device performs the claimed receiving.

f. ***10[a][4]: "transmitting a supervision notification to the at least one supervisor device;"***

443. Limitation 10[a][4] corresponds to limitation 1[h], incorporated here. The communication device performs the function of 1[h]. Thus, Rauner meets 10[a][4].

g. ***10[b]: "a processing device configured for:"***

444. For limitation 10[b], Rauner discloses that structure as described for limitation 1[c].

h. ***10[b][1]: "analyzing the geographical location based on the at least one security parameter;"***

445. Limitation 10[b][1] corresponds to limitation 1[c], incorporated here. The processing device performs the function of 1[c]. Rauner therefore meets 10[b][1].

i. ***10[b][2]: "generating a geofence corresponding to a geographical area based on the analyzing;"***

446. Limitation 10[b][2] corresponds to limitation 1[d], incorporated here. The processing device performs the function of 1[d]. Rauner therefore meets 10[b][2].

j. ***10[b][3]: "analyzing the at least one supervisee data based on the geofence; and"***

447. Limitation 10[b][3] corresponds to limitation 1[f], incorporated here. The processing device performs the function of 1[d]. Rauner therefore meets 10[b][3].

k. ***10[b][4]: "generating the supervision notification based on the analyzing of the at least one supervisee data; and"***

448. Limitation 10[b][4] corresponds to limitation 1[g], incorporated here. The processing device performs the function of 1[d]. Rauner therefore meets 10[b][4].

l. ***10[c]: "a storage device configured for storing the at least one supervisee data and the supervision notification, wherein:"***

449. For limitation 10[c], storage device 162 and its databases correspond to the storage device in limitation 1[i], incorporated here. As explained for 1[i], Rauner meets 10[c].

m. ***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,"***

450. For limitation 10[d], the geofence and grid-based limitations are the system counterparts to limitations 1[j] through 1[j][4]. The communication device's receipt of the grid parameter and the processing device's grid functions are therefore the same as analyzed for claim 1.

n. ***10[d][1]: "wherein the communication device is further configured for receiving at least one grid parameter from the at least one supervisor device"***

451. Limitation 10[d][1] corresponds to limitation 1[j][1], incorporated here, and is disclosed for the same reasons as 1[j][1].

o. ***10[d][2]: "wherein the processing device is further configured for: analyzing the at least one grid parameter;"***

452. Limitation 10[d][2] corresponds to limitation 1[j][2], incorporated here, and is disclosed for the same reasons as 1[j][2].

p. ***10[d][3]: "determining the grid box geofence area based on the analyzing of the at least one grid parameter; and"***

453. Limitation 10[d][3] corresponds to limitation 1[j][3], incorporated here, and is disclosed for the same reasons as 1[j][3].

q. ***10[d][4]: "generating a number of geofence grid boxes based on the determining."***

454. Limitation 10[d][4] corresponds to limitation 1[j][4], incorporated here, and is disclosed for the same reasons as 1[j][4].

455. Each element of claim 10 requires the components to be "configured for" the recited functions. As discussed above for claim 1, the combined Rauner-Azmoodeh system performs each function corresponding to the claimed limitations. In my opinion, performance of the method steps discussed above indicates that each respective component of the Rauner-Azmoodeh system tasked with performing the method step is configured for doing so. Therefore, based on my analysis above, it is my opinion that the components of the components are "configured for" the recited functions of each element of claim 10.

11. Claim 11: "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: identifying at least one location corresponding to the at least one location indication; analyzing the at least one supervisee data based on the at least one location; and 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."

456. Claim 11 is the system counterpart to claim 2. The communication device of claim 10 is configured for the receiving function in 11[a], corresponding

to claim 2[a]. The processing device of claim 10 is configured for 11[b], 11[c], and 11[d], corresponding respectively to claim 2[b], 2[c], and 2[d]. Because the claim 10 devices are configured for those functions, claim 11 is disclosed for the same reasons as claims 2 and 10.

12. Claim 12: "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: determining the at least one action based on the supervision notification; and 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."

457. Claim 12 is the system counterpart to claim 3. The claim 10 processing device is configured for the claim 12 functions: 12[a] corresponds to claim 3[a], 12[b] corresponds to claim 3[b], and 12[c] corresponds to claim 3[c]. Because the claim 10 processing device performs those functions, it is configured for them, and claim 12 is disclosed for the same reasons as claims 3 and 10.

13. Claim 13: "*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, 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.*"

458. Claim 13 corresponds to claim 4. Claim 13[a] corresponds to claim 4[a]: the claim 10 processing device is configured for the supervisee-identification

function. Claim 13[b] corresponds to claim 4[b]: the claim 10 storage device is configured for the profile-data retrieval function. Because those claim 10 devices are configured for the corresponding functions, claim 13 is disclosed for the same reasons as claims 4 and 10.

14. Claim 15: "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: 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."

459. Claim 15 corresponds to claim 6. The communication device of claim 10 is configured for 15[a], corresponding to claim 6[a], and the processing device is configured for 15[b], corresponding to claim 6[b]. Because the claim 10 devices are configured for those functions, claim 15 is disclosed for the same reasons as claims 6 and 10.

RAVE/MSI, EX1005, p. 267

15. Claim 16: "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, wherein the processing device is further configured for analyzing the blueprint and the at least one supervisee data; and 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."

460. Claim 16 corresponds to claim 7. Claim 16[a] corresponds to claim 7[a]: the storage device of claim 10 retrieves the facility blueprint. Claim 16[b] corresponds to claim 7[b]: the processing device of claim 10 analyzes the blueprint and the at least one supervisee data. Claim 16[c] corresponds to claim 7[c]: the same processing device determines the supervisee's location on the blueprint and generates supervision data based on that determination. Because the claim 10 devices are configured for each of those functions, claim 16 is disclosed for the same reasons as claims 7 and 10.

16. Claim 17: "*The system of claim 10, wherein the at least one supervisee device comprises at least one sensor, wherein the at least one sensor is configured for detecting at least one signal made by the supervisee, wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting*."

461. Claim 17 corresponds to claim 8: 17[a] corresponds to 8[a], 17[b] corresponds to 8[b], and 17[c] corresponds to 8[c]. Because the claim 10 system

performs those functions, it is configured for them, and claim 17 is disclosed for the same reasons as claims 8 and 10.

D. Ground 4: Claims 5, 9, 14, and 18 Are Rendered Obvious By Rauner In View Of Azmoodeh And Further In View Of Noland + Knowledge Of A POSITA

462. In my opinion, claims 5 and 9 depend from claim 1, and claims 14 and 18 depend from claim 10. Claims 1 and 10 are rendered obvious by Rauner in view of Azmoodeh as set out in the Ground 3 analysis, including limitations 1[pre] through 1[j][4] and 10[pre] through 10[d][4]. The additional limitations of claims 5, 9, 14, and 18 are rendered obvious by that Rauner-Azmoodeh combination further in view of Noland. Ex.1008 ¶¶[0015]-[0019].

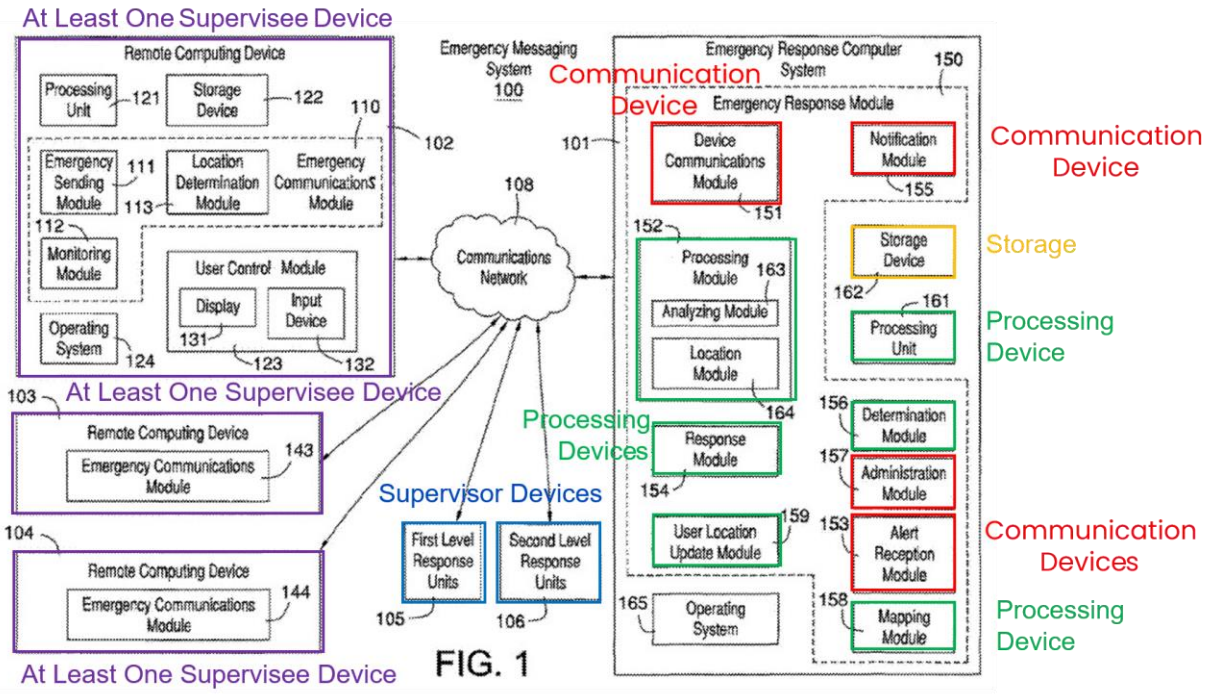


FIG. 1

Ex.1009, Fig. 1 (annotated).

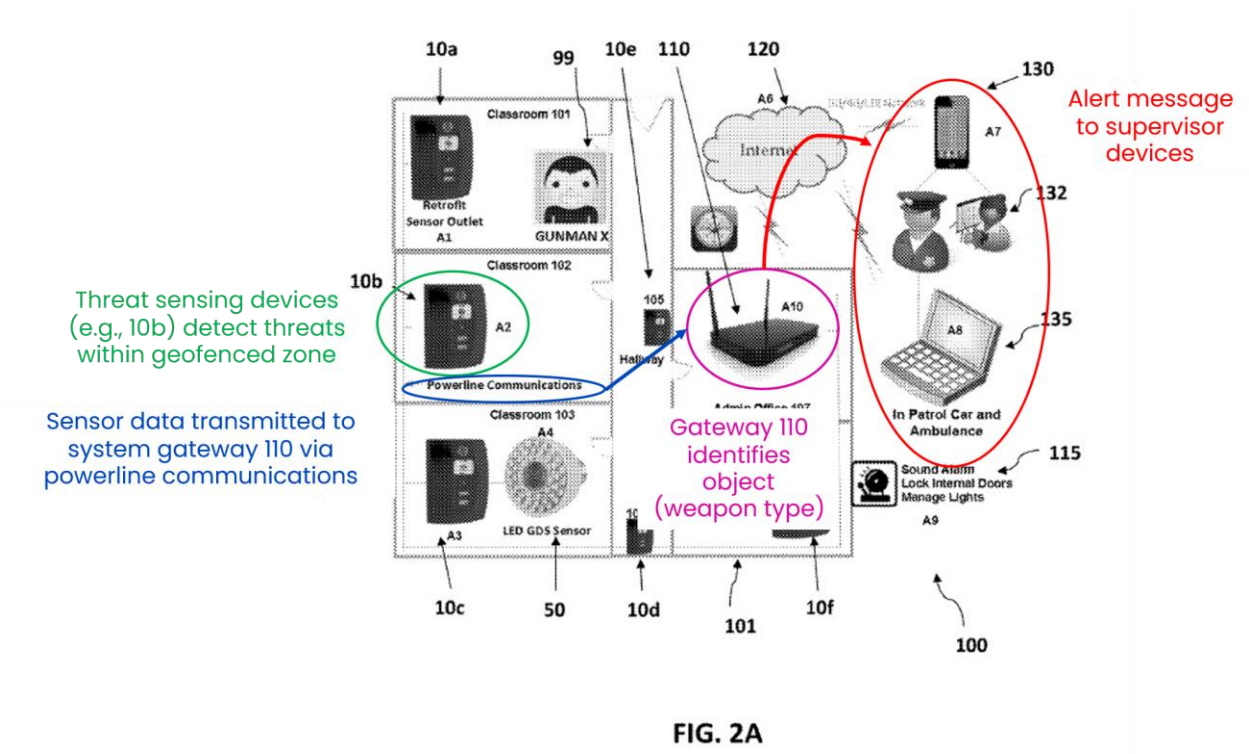


FIG. 2A

Ex.1008, Fig. 2A (annotated).

463. I apply the same mappings corresponding to my Ground 3 analysis throughout this Ground 4 analysis with some additions from Noland.

1. A POSITA Would Have Been Motivated To Combine The Rauner-Azmoodeh Combination With Noland

464. First, Noland is analogous art to the '757 Patent under the applicable test: a reference is analogous art if it is from the same field of endeavor as the claimed invention or is reasonably pertinent to the particular problem faced by the inventor. This Ground 4 analysis addresses adding Noland to the already-combined Rauner-Azmoodeh system, and therefore incorporates the Ground 3 motivation-to-combine analysis for the Rauner-Azmoodeh.

465. All three references and the ’757 Patent are directed to the same field of endeavor: facilitating supervision of individuals based on geofencing. Ex.1001, 1:7-10. Rauner supervises defined institutional populations within selected geographic areas, identifying target groups including “all individuals physically located within a specific geographic location (*e.g.*, a zip code, a city, a county, a state, a university or college campus, work location, office building, airport, public space, or a region served by a specific emergency response group).” Ex.1009 ¶[0048]. This shows monitoring and coordinating responses for people located within campuses, buildings, municipalities, and other defined areas. 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.” Ex.1008 ¶¶[0015]-[0019], [0061], [0148].

466. Noland also expressly teaches that a geofence can “define a predefined boundary, such as a school attendance zone or a specific building boundary that can be monitored,” including “the entry and exit of persons bearing a location-aware device.” This is the same geographic-area monitoring context as Rauner and the ’757 Patent. Noland is therefore analogous art to the ’757 Patent.

467. Noland is also reasonably pertinent to the particular problem faced by the inventor. Noland monitors entry and exit within a defined boundary, identifies

persons and threats, and communicates actionable information to responders and school personnel. Thus, a POSITA seeking to improve Rauner's geofenced supervision and notification system would have considered Noland because it addresses the supervision, presence-identification, and threat-communication.

468. Second, Rauner itself expressly invites adding Noland's capability to the already-combined Rauner-Azmoodeh system. Rauner states that its geofence-based distribution model "can be used to integrate external sensors, systems and resources into the work-flow for discovering, responding to and communicating about emergencies." Ex.1009, ¶[0211]. This is an express invitation to integrate an external threat sensor and processing system such as Noland's.

469. Rauner then identifies "gunshot detection" among the external sensor sources that can serve as trigger events, alongside "airborne contaminant sensor, water contaminant sensor, radiation sensor, … alarm system, door sensor, [and] motion sensor." Ex.1009 ¶¶[0211]-[0212]. In my opinion, Noland improves on that generalized reference by providing specific implementation details for detecting and classifying different types of weapons. Noland supplies the acoustic and image classification logic that resolves a detection into weapon type, caliber, attachments, shot count, and shooter location. Ex.1008 ¶¶[0107]-[0108], [0111], [0127], [0129]. A POSITA seeking to implement the capability Rauner names would therefore have looked to a gunshot-detection system such as Noland's, because Noland supplies the

sensors and gateway logic needed to detect and classify gunshot events rather than merely to report that a discharge occurred.

470. Rauner supplies an integration pathway as well. It describes an example in which "[a] gunshot detection system indicates a firearm discharge at a location" and explains that the event is distributed by cross-referencing its location with stakeholder-defined geographic areas. This is an example of using a gunshot-detection output in Rauner's geofence-based distribution model. Ex.1009 ¶¶[0216], [0223].

471. Third, Rauner's existing event-processing pipeline already consumes external sensor events of the same kind Noland produces. Rauner states: "System processes these external events by comparing the georeferenced event location information to locations for available sensor(s). If/When the external event achieves, the data from the indicated sensor(s) is distributed to mobile/web services according to an administrator defined distribution list." Ex.1009 ¶[0214]. Rauner therefore already receives, georeferences, compares, and distributes external sensor events.

472. Fourth, adding Noland's weapon detection and classification would improve the quality and urgency of the notifications that Rauner already distributes, enabling supervisors and responders to make more informed decisions about threats within supervised areas. Noland identifies that operational benefit directly: "the threat sensing system 100 can also advise 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 (*e.g.*, the level of body armor that might be required) and necessary tactics." Because Noland itself identifies the benefit of communicating weapon information, this motivation comes from the references themselves. Ex.1008 ¶[0156].

473. Fifth, a POSITA would also have been motivated to add Noland's NFC-based personnel identification because it would confirm who is physically present within a monitored geofence, as I described for Ground 2. Noland teaches that "near field sensors could be used to allow the system to identify mobile phones, other mobile devices and the owners of those phones, and monitor the arrival and departure of those device owners from the geo-fenced area." Ex.1008 ¶[0148]. This serves Rauner's supervisory objectives because Rauner already maintains stored profiles linked to user identities and tracks individuals within geofenced areas. Ex.1009 ¶¶[0037], [0099], [0244]. Thus a POSITA would have understood that Noland's NFC reader could be installed at the geofenced facility and report its reads to Rauner's server like any other external sensor event. Passive, proximity-based identification would therefore complement, rather than replace, Rauner's GPS-based tracking: GPS reports where a device says it is, while an NFC read at a fixed sensor independently confirms presence at that sensor.

474. Azmoodeh independently confirms that the base Rauner-Azmoodeh system already contemplates the relevant component class. Azmoodeh describes

communication components including "Near Field Communication (NFC) components," "BLUETOOTH® components (*e.g.*, BLUETOOTH® Low Energy)," and "WI-FI® components." It also identifies components that "detect identifiers," including "Radio Frequency Identification (RFID) tag reader components, NFC smart tag detection components" and teaches deriving "location via detecting an BLUETOOTH® or NFC beacon signal that may indicate a particular location." Ex.1010 ¶¶[0066]-[0067]. These disclosures confirm that NFC and RFID reader components were standard, well-understood components in the art. Adding Noland's NFC identification is therefore an incremental use of components already present in the base system, not a new hardware class, which is a reason supporting both obviousness and expectation of success. Ex.1008 ¶¶[0074], [0148], [0156]; Ex.1010 ¶¶[0066]-[0067].

475. Sixth, the combined system would have produced predictable results. Noland's system gateway 110 outputs weapon-type, caliber, shooter-location, and shot-count data. Rauner's processing unit 161 and Noland's system gateway 110 are both server-side processors that receive, analyze, and act on incoming sensor data. Noland's structured, georeferenced event data is therefore the same kind of data that Rauner's event pipeline already consumes. Because Rauner's pipeline already georeferences, compares, and distributes external sensor events, as described above, integrating Noland requires only directing Noland's output into that existing pipeline

rather than building a new one. Ex.1009 ¶[0214]. Integrating the gateway's logic into Rauner's processing device would therefore require directing Noland's sensor output to Rauner's existing event-processing pipeline, with no change to the basic receive-analyze-notify sequence. In my opinion, that is the application of known techniques to a known system to achieve predictable results, and I would have expected success because the two systems use compatible server-side processing and communications pathways. Ex.1008 ¶¶[0096], [0100], [0107]; Ex.1009 ¶¶[0053]-[0054], [0211]-[0214].

2. Claim 5

476. Claim 5 is rendered obvious by the Rauner-Azmoodeh-Noland combination for the reasons set out for claim 1 in Ground 3 and for the additional reasons discussed below.

a. ***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;"***

477. For limitation 5[a], I map "at least one object associated with the supervisee" to the weapon that Noland's system identifies within the supervisee's geofenced area. Noland states that system gateway 110 analyzes sound waveform data "to determine whether the sound waveform indicates a valid gunshot or gunshots and, if so, to further determine the general type of weapon (*e.g.*, shotgun, handgun, long rifle) that could have produced that sound waveform, and establish

the location or room number of the shooter(s).” This shows that the gateway identifies an object, the weapon, and establishes the location of the associated event. Because that location is determined to be within the supervisee’s geofenced area, the identified weapon is an object associated with the supervisee under the zone-presence theory used here. Ex.1008 ¶[0107].

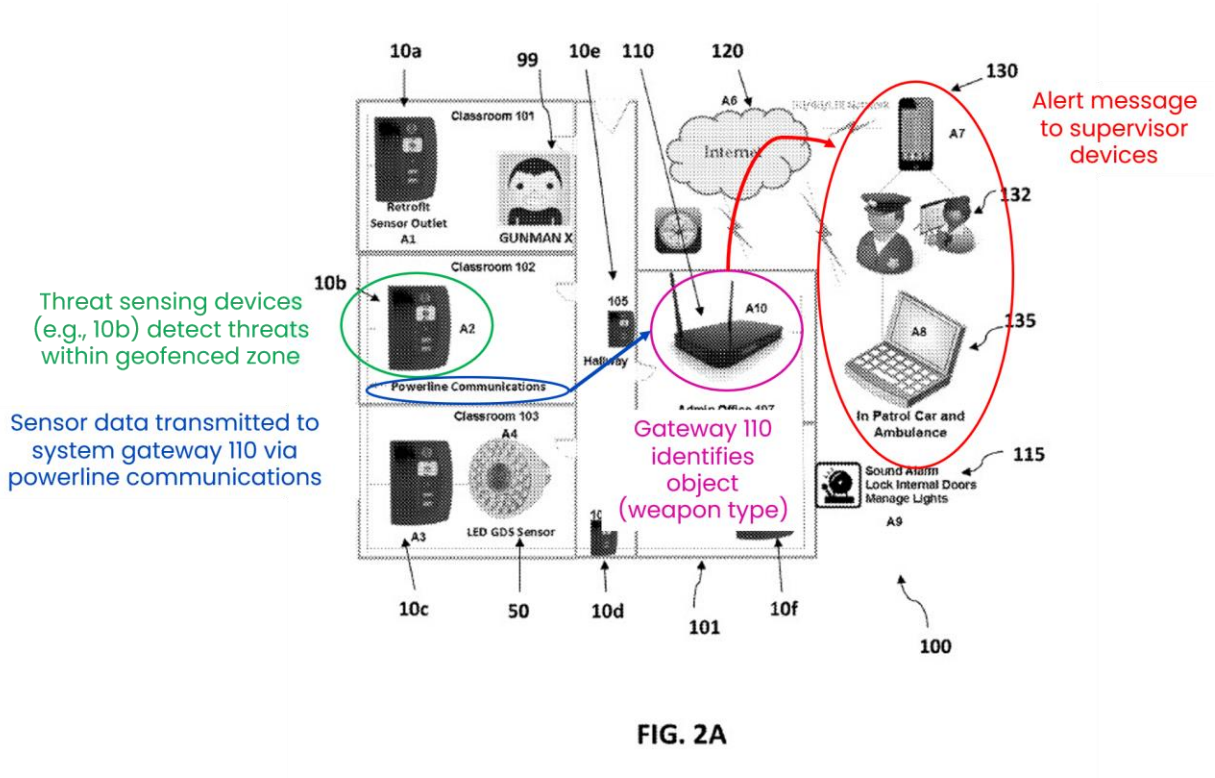


FIG. 2A

Ex.1008, Fig. 2A (annotated).

478. Noland further explains that the gateway “determines not only the validity of a suspect gunshot waveform and determines, from the waveform, the type of weapon involved and location of the waveform, but also independently evaluates each subsequent sound waveform to determine if more than one weapon is being used and/or more than one shooter is involved.” This shows that the identification

extends beyond detecting a generic event: it identifies the weapon type and can distinguish multiple weapons and shooters. A POSITA would understand the location determination to supply that association because the weapon event is georeferenced to the same supervised zone. Ex.1008 ¶[0108].

479. Noland also uses image-based classification. It states that processors compare image data against a library "according to a classification system of weapon, attachments (*e.g.*, muzzle brake, flash suppressor, etc.), caliber (*e.g.*, 9 mm, 40 S&W, 45 ACP, 0.223, 0.308, etc.), direction of fire, and resulting muzzle flash." This provides a second, image-based identification of the weapon and its characteristics, corroborating the acoustic identification. Ex.1008 ¶[0127].

480. In the combined system, Noland's system gateway 110 performs this identification as part of the processing device mapped to Rauner's processing unit 161. The acoustic and location data analyzed by the gateway is georeferenced event data of the same kind mapped as supervisee data in Ground 3 limitation 1[e], and the gateway's output is processed through the Rauner device communications module 151 and notification framework mapped in limitations 1[g] and 1[h]. In my opinion, a POSITA would have understood this integration to make the processing device identify an object based on supervisee data because both the gateway and Rauner's processing unit are centralized server-side processors that receive and analyze incoming sensor data, and the location field ties the weapon event to the supervised

zone. Thus, the claim phrase "identifying, using the processing device, at least one object associated with the supervisee based on the analyzing of the at least one supervisee data" is rendered obvious.

481. Noland Figure 2A, annotated above, illustrates this architecture: threat sensing devices 10a–10n report gunshot data to system gateway 110, which determines "the general type of weapon" and establishes the shooter's location. Ex.1008 ¶¶[0091], [0107].

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."***

482. In my opinion, Noland's system gateway 110, as integrated into Rauner's processing device, determines the lethality of the identified object and generates an alert reflecting that determination, and Rauner's notification framework then incorporates that alert into the supervision notification sent to supervisors. Noland states that "the threat sensing system 100 can also advise 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 (*e.g.*, the level of body armor that might be required) and necessary tactics." EX.1012, ¶[0156]. Assessing the level of threat posed by the identified weapon, including the body armor needed to withstand it, is an assessment of that weapon's lethality. For example, a long rifle firing .308 caliber rounds versus a handgun firing 9 mm rounds calls for a different level of body armor and tactics; that

differentiation is a determination of lethality based on the identified weapon. Ex.1008 ¶[0156].

483. Noland's classification disclosures reinforce that conclusion. It classifies image data according to "weapon, attachments (*e.g.*, muzzle brake, flash suppressor, etc.), caliber (*e.g.*, 9 mm, 40 S&W, 45 ACP, 0.223, 0.308, etc.), direction of fire, and resulting muzzle flash." Classifying the weapon by caliber supplies information about the projectile and weapon characteristics that bear directly on lethal capacity. Ex.1008 ¶[0127].

484. Noland's acoustic classification provides the same relationship from another modality. It states that processors compare acoustic data according to a classification system of "weapon, attachments (*e.g.*, suppressor, etc.), caliber, direction of fire, and resulting acoustic waveform," and explains that an unsuppressed .22 LR handgun can produce gunshots of over 160 decibels while a suppressor reduces the volume by about 30 dB. This shows that Noland uses weapon, caliber, attachment, and acoustic-output characteristics to distinguish the threat posed to human life by the identified object. Ex.1008 ¶[0129].

485. Noland states that the processing means to recall and transmit stored data includes instructions to transmit "pertinent information of a probable gunshot event." This shows that the processing result is selected for communication as part of the alert process. Ex.1008 ¶[0035].

486. Noland specifies the information included in the transmission: "the type of weapon(s) involved, the number of threats, the location of the threat, the last known location of the threat, the number of shots fired." Ex.1008 ¶[0100]. Because the determined weapon type and related characteristics are included in the information sent to responders, the alert content is based on the identification and the resulting threat assessment. Ex.1008 ¶[0100].

487. Noland likewise states that the Emergency Notice can include "the room/zone number of the active shooter, the type of weapon involved, the number of shots fired," and "whether more than one shooter appears to be active." Noland's claim 6 further recites that communications "comprise a map of a building, a location of a shooter within the building, a number of shots fired, and identification of a type of weapon or weapons discharged." These disclosures show that the weapon identification and associated threat assessment are used in generating the communication itself. Ex.1008 ¶[0238]; claim 6.

488. Noland provides a further transmission example: "information regarding the Gunman X 99 and the weapon discharge (*e.g.*, location of weapon discharge, acoustic signature, image signature, determined weapon type, determined caliber, etc.) is sent via the Internet 120 to designated mobile devices 130 and local authorities 132." In the combined system, this determined weapon-type and caliber information is carried in the supervision notification transmitted to the supervisor

devices through Rauner's notification framework, as mapped in Ground 3 limitations 1[g] and 1[h]. In my opinion, weapon-type and caliber classification constitutes a lethality determination because those characteristics determine the threat level and the response information that the notification communicates. Thus, "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" is rendered obvious.

3. Claim 9

a. *9[a]: "The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises:"*

489. For limitation 9[a], Rauner already supplies the claimed association, independent of Noland. Rauner describes a notice message containing "unique user ID, user name from profile." This shows that the monitored user is associated with an identification used in the emergency-response system. Rauner also states that a profile for each portable communication device associated with each user is stored in storage device 162 and may include "name, age, residence, email address, phone number, emergency contact information, current location of the user, past locations of the user." Additionally, in the combined system, the supervisee's NFC identifier is stored with that profile. Ex.1008, ¶¶[0034], [0074]. Thus, each supervisee is

already associated with an identification and a stored identity profile in the base system. Ex.1009 ¶¶[0050], [0099].

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"***

490. For limitation 9[b], in the combined system, the supervisee's device additionally carries an NFC identification readable by Noland's near-field sensors. Noland teaches that its threat sensing devices comprise "a near field communication (NFC) device and/or a far-field communication device (*e.g.*, standard RF, Wi-Fi, etc.), to communicate directly with nearby portable devices (*e.g.*, radio-frequency identification 'RFID' integrated into an ID Badge, etc.) or mobile devices." Ex.1008 ¶[0074]. Thus, Noland's near-field sensors identify mobile phones and their owners within at a geo-fenced facility, using an NFC device, while Rauner supplies the underlying user-ID and profile association. Ex.1008 ¶¶[0074], [0148].

491. Azmoodeh corroborates that these were standard components in the art, rather than supplying the claimed personnel-identification step. Azmoodeh identifies "Near Field Communication (NFC) components," "BLUETOOTH® components (*e.g.*, BLUETOOTH® Low Energy)," and "WI-FI® components," as well as "Radio Frequency Identification (RFID) tag reader components, NFC smart tag detection

components." It further teaches location "via detecting an BLUETOOTH® or NFC beacon signal that may indicate a particular location." These disclosures confirm the technical compatibility of Noland's NFC reader and identification with the base Rauner-Azmoodeh system. Ex.1010 ¶¶[0066]-[0067].

492. Rauner independently discloses that its communications interface may be "any suitable form of wired or wireless connection including, but not limited to, USB (universal serial bus) connection, serial connection, cellular communication, IEEE 802.11, etc." IEEE 802.11 is Wi-Fi, which is also one of the claim's enumerated alternatives. Noland likewise states that the gateway receives data from threat sensing devices using wireless protocols including "900 MHz, Wi-Fi, Zigbee, and Z-wave," and communicates with in-building devices via wireless connections including "ZWave or Zigbee, Bluetooth, WiFi, etc." Zigbee and Bluetooth are also enumerated in the claim. Thus, the combined system practices several independent paths within the claimed short-range protocol alternatives. Ex.1009 ¶[0068]; Ex.1008 ¶¶[0106], [0230].

493. Additionally, a POSITA would have known that NFC target devices respond to communication requests with an "NFC Identifier," typically depicted as "NFCID*n.*" Ex.1034, 9. In the specific case of a target response, "Random Identifier NFCID2" is transmitted to the requesting device. *Id.*, 11, 22. Therefore, a POSITA

would have known that an NFC communication includes at least one "NFC identification" as required by the limitation.

494. In the combined system, the NFC indication received by Noland's facility-deployed threat sensing device is communicated to Rauner's device communications module 151, part of the communication device mapped in Ground 3 limitation 1[a], through the same event pipeline by which Noland's sensor data reaches Rauner's server. Rauner already receives and distributes georeferenced external sensor events, and Noland's gateway already communicates processed event data over network pathways. Accordingly, the claim phrase "receiving, using the communication device, at least one NFC indication ... wherein the receiving is performed over short range wireless communication comprising at least one of Bluetooth, Zigbee, Ultra-wideband, Wi-Fi and NFC" is rendered obvious.

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."***

495. For limitation 9[c], Noland identifies the person. Noland states that near-field sensors "identify mobile phones, other mobile devices and the owners of those phones." Ex.1008 ¶[0148]. Identifying the owner of the detected phone or device is identifying the supervisee.

496. Noland also teaches the stored records used to resolve the NFC read to a person. It states that recorded information may be "linked to employee IDs, student

IDs, RFIDs, class schedules, attendance records," and that personal information of participants is stored for use by the notification system. A POSITA would understand the NFC identifier to be matched against those stored records so that the gateway resolves the detected device to the corresponding person. Noland's owner lookup and stored personnel records perform the function of "identifying the supervisee." Ex.1008 ¶¶[0034], [0025].

497. Noland states that its SMS notification is transmitted "to a list of recorded information of personnel and personal information." This means the identified personnel records determine which information and recipients are used in the notification process. In the combined system, the identification is performed by Noland's gateway logic integrated with Rauner's processing unit 161, and the resulting identity is used by Rauner's notification modules to select and populate the supervision notification. Ex.1008 ¶[0036].

498. This mirrors the identification-and-retrieval framework already established for claim 4 in Ground 3. Once the supervisee is identified by the NFC indication, the storage device retrieves the associated Rauner profile, including "name, age, residence, email address, phone number, emergency contact information," and that profile data is incorporated into the supervision notification through the Ground 3 limitations 1[g] and 1[h] framework. Thus, the claim phrase "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" is rendered obvious. Ex.1009 ¶[0099].

499. Finally, this modification would have been obvious. NFC was a well-known short-range wireless identification protocol as of the March 5, 2019 priority date; Noland teaches its use to identify device owners within a geofenced area; and the base Rauner-Azmoodeh system already includes NFC reader components. Applying that known identification technique to the known monitoring system would have required only routing the NFC indication into the existing communication and processing path, with the predictable result of confirming the identity and presence of a supervisee. Claim 9 is therefore met.

4. Claim 14: "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 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."

500. Claim 14 is the system counterpart to method claim 5. Claim 14[a] corresponds to claim 5[a], and claim 14[b] corresponds to claim 5[b]. Because the method analysis shows that the combined Rauner-Azmoodeh-Noland system performs the functions, Claim 14 is disclosed for the same reasons as claim 5, because the same integrated server-side processing performs the corresponding functions. Ex.1009 ¶¶[0053]-[0054], [0097]; Ex.1008 ¶¶[0107], [0156].

RAVE/MSI, EX1005, p. 287

5. Claim 18: "The system of claim 10, wherein the supervisee is associated with at least one near field communication (NFC) identification, 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, wherein the processing device is further configured for identifying the supervisee based on the at least one NFC indication, wherein the generating of the supervision notification is based on the identifying."

501. Claim 18 is the system counterpart to method claim 9. Claim 18[a] corresponds to claim 9[a], claim 18[b] corresponds to claim 9[b], claim 18[c] corresponds to claim 9[c], and claim 18[d] corresponds to the notification-dependency portion of claim 9[c]. Claim 18 omits claim 9's separate requirement that receipt occur over "short range wireless communication comprising at least one of Bluetooth, Zigbee, Ultra-wideband, Wi-Fi and NFC." That omission removes a requirement, while the combined system nevertheless performs the NFC receipt and identification functions analyzed for claim 9. Because the method analysis shows that the combined system performs each remaining function, the claim 10 devices are necessarily configured for doing so, and claim 18 is disclosed for the same reasons as claims 9 and 10. Ex.1008 ¶¶[0074], [0148]; Ex.1009 ¶¶[0053]-[0054], [0097].

X. INVALIDITY OF '421 PATENT CLAIMS 1-24 UNDER 35 U.S.C. § 103

502. In my opinion the '421 patent is invalid based on the following grounds:

Ground	Claims	Reference(s)

1	1-4, 6, 10, 11-14, 16, 20, 21	Staton + knowledge of a POSITA
2	5, 7, 8, 15, 17-19, 22-24	Staton + Noland + knowledge of a POSITA
3	9	Staton + Smith + knowledge of a POSITA
4	1-4, 6-8, 10-14, 16-21	Rauner + Azmoodeh + knowledge of a POSITA
5	5, 15, 22-24	Rauner + Azmoodeh + Noland + knowledge of a POSITA
6	9	Rauner + Azmoodeh + Smith + knowledge of a POSITA

A. Ground 1: Claims 1-4, 6, 10-14, 16, and 20-21 of the '421 Patent Is Rendered Obvious By Staton (Ex.1007) + Knowledge Of A POSITA

1. Claim 1

a. Scope of this opinion and relationship to my '757 analysis

503. In my opinion, Staton discloses or renders obvious every limitation of claim 1 of the '421 Patent. I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 1 of the '757 Patent in Section [IX.A.1] above. This section identifies what I am mapping to each element, explains why my

RAVE/MSI, EX1005, p. 289

’757 analysis applies equally to these claims, and addresses the one textual difference between them. I do not repeat the element-by-element analysis, and nothing in this section is intended to modify it.

504. The ’421 Patent is a continuation-in-part of the application that issued as the ’757 Patent, was filed October 11, 2022 as U.S. Application No. 18/045,781, and claims priority to Provisional Application No. 62/814,097 filed March 5, 2019. It shares the same sole inventor and largely the same specification as the ’757 Patent. I have assumed, without conceding, that the challenged claims are entitled to the March 5, 2019 priority date, and I have applied that date here exactly as I applied it to the ’757 Patent. My opinion as to the level of ordinary skill in the art is also unchanged.

b. ***Claim 1 of the ’421 Patent is substantially similar to claim 1 of the ’757 Patent***

505. I have compared the two claims limitation by limitation. Limitations 1[pre] through 1[j][4] of ’421 claim 1 recite the same method steps, in the same order, as limitations 1[pre] through 1[j][4] of ’757 claim 1. Because the claims are substantially similar, and because the ’421 Patent carries largely the same specification as the ’757 Patent, the technical mappings I applied to ’757 claim 1 apply.

506. Some of the opinions I gave for ’757 claim 1 include descriptions from the ’757 Patent specification in addition to the teachings of Staton, and I confirm

that the disclosures I relied on appear in the '421 specification as well. First, for my opinion that Staton's processing components track the claimed "processing device," the '421 Patent states that "the method disclosed herein may be performed by one or more computing devices," Ex.1003, 6:36-37, and that "the present disclosure may be embodied in hardware and/or in software (including firmware, resident software, micro-code, etc.)." *Id.,* 29:14-20. Second, for my opinion that allocating the location-to-geofence comparison between the server and the client would have been a routine design choice, the '421 Patent states that "one or more steps of the method may be performed by a server computer" and that "[s]imilarly, one or more steps of the method may be performed by a client computer," *id.,* 9:1-3; that "the 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," *id.,* 6:64-67; and that the server "may be configured to analyze the location data." *Id.,* 25:50-60.

507. There is one difference in wording. Issued '757 claim 1 includes, within limitation 1[j][1], the phrase "wherein the processing device is further configured for". Issued '421 claim 1 does not; its 1[j][1] recites only "receiving, using the communication device, at least one grid parameter from the at least one supervisor device" before proceeding directly to the analyzing step.

508. In my opinion that difference is immaterial to the obviousness analysis. The phrase in the ’757 claim is a configured-for recitation embedded in a method claim whose surrounding steps are already affirmatively recited as performed “using the processing device”. Its omission from the ’421 claim therefore does not change my analysis. Under either wording, the same sequence is required: the grid parameter is received through the communication device, and the analyzing, determining, and generating steps are performed by the processing device. Staton performs that sequence as I identified above. My conclusion is therefore the same for the ’421 claim 1 as for the ’757 claim 1.

509. For the reasons stated in my analysis of ’757 claim 1, which I incorporate here, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 1 of the ’421 Patent.

2. Claim 2

510. In my opinion, Staton discloses or renders obvious every limitation of claim 2 of the ’421 Patent. I have compared claim 2 from both patents limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 2 of the ’757 Patent in Section [IX.A.2] above, which I incorporate here.

511. For limitation 2[c], I set out in my ’757 claim 2 analysis two theories, under the remote notify router 681 pathway and under the response router 620

pathway, together with an alternative obviousness rationale addressing direct server-side comparison of the supervisee's location to the designated location; I incorporate all three here and reach the same conclusion for '421 claim 2.

512. For the reasons stated in my analysis of '757 claim 2, which I incorporate here, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 2 of the '421 Patent.

3. Claim 3

513. In my opinion, Staton discloses or renders obvious every limitation of claim 3 of the '421 Patent. I have compared claim 3 from both patents limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 3 of the '757 Patent in Section [IX.A.3] above, which I incorporate here.

514. For the reasons stated in my analysis of '757 claim 3, which I incorporate here, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 3 of the '421 Patent.

4. Claim 4

515. In my opinion, Staton discloses or renders obvious every limitation of claim 4 of the '421 Patent. I have compared claim 4 in both patents limitation by limitation. They are substantively similar in wording. Therefore, I reach that

RAVE/MSI, EX1005, p. 293

conclusion for the same reasons, and on the same disclosures, that I set out for claim 4 of the ’757 Patent in Section [IX.A.4] above, which I incorporate here.

516. For the reasons stated in my analysis of ’757 claim 4, which I incorporate here, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 4 of the ’421 Patent.

5. Claim 6

517. In my opinion, Staton discloses or renders obvious every limitation of claim 6 of the ’421 Patent. I have compared claim 6 in both patents limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 6 of the ’757 Patent in Section [IX.A.5] above, which I incorporate here.

518. For the reasons stated in my analysis of ’757 claim 6, which I incorporate here, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 6 of the ’421 Patent.

6. Claim 10

519. In my opinion, Staton discloses or renders obvious every limitation of claim 10 of the ’421 Patent.

a. ***10[a]: The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises:***

520. For limitation 10[a], the “at least one identification” is the PDA address information that uniquely identifies each supervisee’s device within the backend

control system. Staton states that "[t]he resources database 670 stores relational information of PDAs and instrumentation modules" and that "all relational information associated to one PDA permits the database to search and find all other related PDAs, preferences, permissions, etc." Ex.1007, 24:23-28. Staton further states that the command receiver 690 "tags each outbound message with the correct PDA 105 address" by "searching the resources database 670 and retrieving the address information," which confirms that the address information is a stored per-device identifier rather than a transient routing artifact. *Id.,* 24:33-39. Because PDA 105 is carried by the monitored individual, the address information that identifies that PDA is an identification with which the supervisee is associated. The '421 Patent itself treats address information as a form of identification, listing a network device with a unique IP or MAC address among its examples. Ex.1003, 7:49-52.

b. ***10[b]: receiving, using the communication device, at least one indication corresponding to the at least one identification from the at least one supervisee device; and***

521. For limitation 10[b], the claimed "indication corresponding to the at least one identification" is the address tag carried on each inbound packet from the supervisee device. Staton states that "[a]s the gateway system 151-153 receives each inbound packet of data, the gateway system 151-153 tags each packet with the date and time of arrival, the PDA 105 manufacturer information, the PDA's 105 address information, and repackages the packet for transmission to the codec 155." *Id.,*

20:47-54. The tagged address information corresponds to the same stored identification described for 10[a], and it arrives at the backend with the supervisee device's own transmission. The gateways are the communication components of the backend control system 150, so the indication is received "using the communication device" and it comes "from the at least one supervisee device." Staton corroborates that the inbound packet is examined on arrival, stating that "each inbound packet that the codec 155 receives is first examined to determine the PDA model." *Id.,* 21:14-22.

c. ***10[c]: identifying, using the processing device, the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying.***

522. For limitation 10[c], the processing device identifies the supervisee from that indication by resolving the tagged address against the stored relational records. Staton states that PDA-to-PDA communications are "transmitted and received after a screening process through the back end control system 150," and that "the backend control system 150 checks in the resources database 670 for the correct permissions, preferences, settings, network mode, of the PDA sending and receiving the command." *Id.,* 23:58-63. Checking the sending PDA against its stored record is the act of determining which supervisee the incoming data concerns. Staton confirms the result of that resolution, stating that "when the backend control system 150 processes a received message by one PDA, the backend control system 150 can

relay the data in the message to the correct PDA." *Id.,* 24:64-67. The system would struggle to select the correct recipient without first identifying the sender.

523. The notification dependency in limitation 10[c] is also met because the generating of the supervision notification is based on that identification. Staton states that the remote notify router 681 "queries the resources database 670 to find out if the configuration information or event information received requires a notification" and that, "[i]f a notification is required, the remote notify router 681 retrieves the contact information for the appropriate PDA 105, the instrument module 195 or the communications device 177" before it "formats and encodes the message." *Id.,* 22:18-35. The query and the contact retrieval both operate on the identified PDA's relational data, so the notification is generated only after, and on the basis of, the identification. That is the same notification pathway I mapped for limitations 1[g] and 1[h].

524. Accordingly, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 10 of the '421 Patent.

7. Claim 11

525. In my opinion, Staton discloses or renders obvious every limitation of claim 11 of the '421 Patent. Claim 11 is the system counterpart to claim 1, and it corresponds to claim 10 of the '757 Patent. I have compared the two claims

limitation by limitation. They recite the same communication device, processing device, and storage device functions, and the same geofence and grid-box limitations, with the sole difference that '757 claim 10 recites "at least one supervisor data associated with a supervisee" in limitation 10[a][3] where '421 claim 11 recites "at least one supervisee data associated with a supervisee" in limitation 11[a][3]. In my opinion that difference does not affect my analysis: as I explained for '757 limitation 10[a][3], the antecedent basis in the remainder of the claim shows that the recitation refers to the supervisee data of limitation 1[e], and the '421 wording simply states expressly what the '757 wording conveys by antecedent. Therefore, I reach the same conclusion for the same reasons, and on the same disclosures, that I set out for claim 10 of the '757 Patent in Section [IX.A.7] above, which I incorporate here.

526. Because claim 11 is an apparatus claim, the § 112(f) constructions Applicant conceded during prosecution for the "communication device," "processing device," and "storage device" apply directly to it, and I applied those constructions in the '757 claim 10 analysis I incorporate here.

527. For the reasons stated in my analysis of '757 claim 10, and my claim 1 analysis of '421 claim 1, which I incorporate here, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 11 of the '421 Patent.

RAVE/MSI, EX1005, p. 298

8. Claim 12

528. In my opinion, Staton discloses or renders obvious every limitation of claim 12 of the ’421 Patent. Claim 12 is the system counterpart to claim 2 and corresponds to claim 11 of the ’757 Patent. I have compared the two claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 11 of the ’757 Patent in Section [IX.A.8] above, which I incorporate here.

529. For the reasons stated in my analysis of ’757 claim 11, which I incorporate here, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 12 of the ’421 Patent.

9. Claim 13

530. In my opinion, Staton discloses or renders obvious every limitation of claim 13 of the ’421 Patent. Claim 13 is the system counterpart to claim 3 and corresponds to claim 12 of the ’757 Patent. I have compared the two claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 12 of the ’757 Patent in Section [IX.A.9] above, which I incorporate here.

531. For the reasons stated in my analysis of ’757 claim 12, which I incorporate here, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 13 of the ’421 Patent.

10. Claim 14

532. In my opinion, Staton discloses or renders obvious every limitation of claim 14 of the ’421 Patent. Claim 14 is the system counterpart to claim 4 and corresponds to claim 13 of the ’757 Patent. I have compared the two claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 13 of the ’757 Patent in Section [IX.A.10] above, which I incorporate here.

533. For the reasons stated in my analysis of ’757 claim 13, which I incorporate here, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 14 of the ’421 Patent.

11. Claim 16

534. In my opinion, Staton discloses or renders obvious every limitation of claim 16 of the ’421 Patent. Claim 16 is the system counterpart to claim 6 and corresponds to claim 15 of the ’757 Patent. I have compared the two claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set

RAVE/MSI, EX1005, p. 300

out for claim 15 of the ’757 Patent, which I incorporate here, including the mapping of the claimed environment data to the measurements taken by the environment-condition sensors connected to Staton’s instrument module 195.

535. For the reasons stated in that analysis, which I incorporate here, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 16 of the ’421 Patent.

12. Claim 20

536. In my opinion, Staton discloses or renders obvious every limitation of claim 20 of the ’421 Patent. Claim 20 is the system counterpart to claim 10, and like claim 10 it recites a generic “identification” rather than a near field communication identification.

a. ***20[a]: The system of claim 11, wherein the supervisee is associated with at least one identification,***

537. For limitation 20[a], the identification is the PDA address information stored in resources database 670, for the reasons I gave for limitation 10[a].

b. ***20[b]: wherein the communication device is further configured for receiving at least one indication corresponding to the at least one identification from the at least one supervisee device,***

538. For limitation 20[b], the communication device is configured for receiving the corresponding indication because Staton’s gateway system tags each inbound packet with “the PDA’s 105 address information” as it receives the packet from the supervisee device. Ex.1007, 20:47-54.

c. ***20[c]: wherein the processing device is further configured for identifying the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying.***

539. For limitation 20[c], the processing device is configured for identifying the supervisee from that indication because the backend "checks in the resources database 670 for the correct permissions, preferences, settings, network mode, of the PDA sending and receiving the command," and then "can relay the data in the message to the correct PDA." *Id.,* 23:60-24:5. The notification dependency is disclosed through the remote notify router's database query and contact retrieval before it "formats and encodes the message." *Id.,* 22:18-35. Because Staton's backend performs each of these functions, its communication device and processing device are configured for them.

540. Accordingly, it is my opinion that Staton in view of the knowledge of a POSITA discloses or renders obvious each limitation of claim 20 of the '421 Patent.

RAVE/MSI, EX1005, p. 302

13. Claim 21: The system of claim 11, wherein each geofence grid box is further characterized by: a) storing at least one emergency contact number associated with the geographical area represented by the grid box geofence area; b) wherein the emergency contact number includes a 911 service or equivalent emergency service specific to then geographical area of the grid box; and c) wherein the processing device is configured to automatically select and transmit supervisee data to the stored emergency contact number upon detecting an emergency situation within the corresponding grid box geofence area.

541. In my opinion, Staton discloses every limitation of claim 21 of the '421 Patent. Claim 21 has no counterpart in the '757 Patent, so I analyze it on its own.

a. ***21[a]: The system of claim 11, wherein each geofence grid box is further characterized by: a) storing at least one emergency contact number associated with the geographical area represented by the grid box geofence area;***

542. Staton supplies the stored emergency contact number associated with the geographical area represented by each grid box geofence area. Staton states that the control center, upon receiving a geofence event message, "looks up the correct PDAs to contact in the resources database 670 and any other parties that must be contacted, such as the police or 911." Ex.1007, 26:65-27:3; *see also id.*, 22:22–36. That disclosure identifies 911 and the police as stored contacts, held in the resources database alongside the relational and contact information for the devices.

543. In Staton, as described above for limitation 1[j], each of the activated geofence grid boxes collectively define the geofence. Therefore, the stored

emergency contact number is associated with each geographical area represented by each grid box geofence area because the geofence is comprised of each grid box and the emergency contact number is looked up and identified based on and with association to the event associated with that geofence. *Id.* 26:62-27:2. Therefore, Staton discloses limitation 21[a].

b. ***21[b]: b) wherein the emergency contact number includes a 911 service or equivalent emergency service specific to then geographical area of the grid box; and***

544. As discussed above, Staton states that the control center, upon receiving a message reporting the occurrence of an event, "looks up the correct PDAs to contact in the resources database 670 and any other parties that must be contacted, such as the police or 911." Ex.1007, 26:65-27:3; *see also id.*, 22:22–36. That disclosure identifies 911 and equivalent emergency services such as the police as stored contacts, held in the resources database and specific to each geographical zone. *Id.,* 22:22–28, 26:62-27:2, 30:43-46. Therefore, Staton discloses limitation 21[b].

c. ***21[c]: c) wherein the processing device is configured to automatically select and transmit supervisee data to the stored emergency contact number upon detecting an emergency situation within the corresponding grid box geofence area.***

545. Staton further states that the remote notify router 681, after determining that notification is required, "retrieves the contact information for the appropriate

PDA 105, the instrument module 195 or the communications device 177" and "then formats and encodes the message sent to the PDA 105, the instrument module 195 or the communications device 177," which is placed in an outbound queue for gateway transmission. *Id.,* 22:22-36. The message so transmitted carries the supervisee's geocoded location and event information, because that is the content the history recorder places in the remote notify queue. *Id.,* 22:16-22. The selection and transmission are automatic because the router performs them in response to the event without supervisor intervention.

546. In my opinion Staton discloses limitation 21[c].

547. Accordingly, it is my opinion that Staton in view of the knowledge of a POSITA renders obvious each limitation of claim 21 of the '421 Patent.

B. Ground 2: Claims 5, 7, 8, 15, 17-19, 22, 23, and 24 of the '421 Patent Are Rendered Obvious By Staton (Ex.1007) In View Of Noland (Ex.1008) + Knowledge Of A POSITA

1. A POSITA would have combined Staton with Noland

548. Claims 5, 7, and 8 depend from claim 1, and claims 15, 17, 18, and 19 depend from claim 11. I explained above why Staton discloses or renders obvious claims 1 and 11, and I incorporate that analysis here. Claim 22 is a separate independent method claim, and claims 23 and 24 depend from it; I analyze those three claims on their own below. For this Ground I rely on Staton in view of Noland

for the reasons that follow as well as for the corresponding combination rationale in my ’757 analysis, which I incorporate here.

549. Both references are directed to the same field of endeavor as the ’421 Patent: facilitating supervision of individuals based on geofencing. Ex.1003, 1:7-18. 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 discloses a threat sensing system for automated gunshot detection and emergency response that likewise operates over geographically defined areas, including school and building boundaries, and uses near field sensors to monitor the arrival and departure of device owners from a geo-fenced area. Ex.1008 ¶¶[0015]-[0019], [0148]. Each reference is therefore in the field of endeavor of the claimed invention and is also reasonably pertinent to the problem the named inventor addressed.

550. A POSITA would have been motivated to incorporate Noland’s weapon identification, facility schematics, audio/video sensors, and supervisee-initiated panic button into Staton’s system in order to improve the quality and urgency of Staton’s supervision notifications. Weapon type and lethality inform the response to a detected threat, facility schematics locate the threat within a building rather than merely within a zone, live audio and video from the threat location would give supervisors and responders real-time situational awareness, and a panic button

lets the supervised individual report a threat that automated sensors cannot detect. Ex.1008 ¶¶[0104], [0156]. Staton's events are typically generated automatically when a rule is broken or a threshold is exceeded. Noland supplies a mechanism for mechanism for allowing a supervisee to initiate an event that may not be detected by a sensor, stating that "each staff member may be equipped with a key fob 'panic button' device." Ex.1007, 6:50-57, 13:65-14:4; Ex.1008 ¶[0104]. In my opinion a POSITA would have recognized the panic button as a manual-override complement to Staton's automated event detection, improving the system's ability to respond to a personal threat visible only to the supervised individual.

551. A POSITA would also have had a reasonable expectation of success in making the combination. Staton's instrument module architecture was expressly designed to accept external sensor input: the instrument module "can be mounted, attached, manufactured, or otherwise included upon/in various articles or electrical devices, or in the PDA itself," and it "works to collect, process, and communicate information about the article or electrical devices to which the instrument module is connected." Ex.1007, 6:34-43. Staton further discloses that the instrument module can be configured to detect that a preconfigured event has occurred and to execute an operation upon detecting the signal, and that upon detection it "transmits an event message" to PDA 105. *Id.,* 9:2-9. Adding a panic button to that architecture therefore uses the module for exactly the function it was built to perform. As to Noland's

gateway functions, both Staton's backend control system 150 and Noland's system gateway 110 receive, analyze, and act on incoming event data, so integrating Noland's weapon-identification and schematic-location output into Staton's processing components would have required only routine software changes rather than a new architecture. *Id.,* 6:34-8:8; Ex.1008 ¶¶[0107], [0113].

2. Claim 5

552. In my opinion Staton in view of Noland renders obvious every limitation of claim 5 of the '421 Patent. I have compared claim 5 of both patents limitation by limitation. '421 claim 5 is substantively similar in wording to '757 claim 5. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 5 of the '757 Patent in my Ground 2 analysis above, which I incorporate here, including the mapping of the claimed object to the weapon that Noland's system gateway 110 identifies within the supervisee's geofenced zone and the mapping of lethality to Noland's weapon-type and caliber classification.

3. Claim 7

553. In my opinion Staton in view of Noland renders obvious every limitation of claim 7 of the '421 Patent. I have compared the two claims limitation by limitation. '421 claim 7 is substantively similar in wording to '757 claim 7. Therefore, I reach that conclusion for the same reasons, and on the same disclosures,

RAVE/MSI, EX1005, p. 308

that I set out for claim 7 of the ’757 Patent in my Ground 2 analysis above, which I incorporate here, including the mapping of the claimed blueprint to Noland’s pre-loaded facility schematics and floor plans and the room-level location determination Noland’s gateway performs.

4. Claim 8

554. In my opinion Staton in view of Noland renders obvious every limitation of claim 8 of the ’421 Patent.

555. I note that this mapping differs from the one I applied to claim 8 of the ’757 Patent. That earlier mapping remains correct and independently sufficient for the substantively similar ’421 claim, and I do not withdraw it.

a. ***8[a]: The method of claim 1, wherein the at least one supervisee device comprises at least one sensor,***

556. For limitation 8[a], the supervisee device comprises a sensor because Staton’s instrument module 195 and PDA 105 “can be in the same housing,” and the instrument module is expressly designed to be “included upon/in various articles or electrical devices, or in the PDA itself.” Ex.1007, 10:26-27, 6:34-43. In the combined system, the panic button includes a sensor, i.e., a button, that a user can press implemented in or connected through that instrument module, so the supervisee device comprises at least one sensor. Noland supplies the panic button, stating that “each staff member may be equipped with a key fob ‘panic button’ device.” Ex.1008 ¶[0104]. In my opinion a POSITA would have implemented the

key fob through the instrument module because the instrument module already provides the detection and reporting path to PDA 105 that a panic alert requires.

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

557. For limitation 8[b], the sensor is configured for detecting a signal made by the supervisee because the panic button detects the supervisee's deliberate button press. Noland states that the key fob is "linked to the staff member" and that, when activated, it "immediately provides positional information regarding not only the staff member, but also of the threat." Ex.1008 ¶[0104]. Noland also describes the activation as a manual override of the sensing system's automated values. *Id.* ¶[0037]. The press is therefore a signal originating from the supervisee. Staton's instrument module architecture already contemplates detection of exactly this kind: the module is configurable to detect when "a preconfigured event has occurred" and to "execute an operation upon the detection of the signal." Ex.1007, 9:2-5.

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

558. For limitation 8[c], the sensor is configured for generating the supervisee data based on that detecting. Staton states that when the instrument module 195 receives a signal from a connected device, it determines whether an event has occurred and transmits an event message to PDA 105, which in turn transmits it to the backend control system. *Id.,* 9:2-9. The event message so generated

is supervisee data because it reports an emergency associated with the monitored individual, and Noland confirms that the panic-button activation supplies the supervisee's positional information along with the threat information as described in the preceding section. Ex.1008 ¶¶[0037], [0104]. The generation is "based on the detecting" because the module composes and transmits the message only after it detects the button press.

559. Accordingly, it is my opinion that Staton in view of Noland renders obvious each limitation of claim 8 of the '421 Patent.

5. Claim 15

560. In my opinion Staton in view of Noland renders obvious every limitation of claim 15 of the '421 Patent. Claim 15 recites the processing device of claim 11 as configured for the functions of limitations 5[a] and 5[b], and is therefore invalid for the same reasons as claims 5 and 11.

6. Claim 17

561. In my opinion, Staton discloses or renders obvious every limitation of claim 17 of the '421 Patent. Claim 17 is the system counterpart to claim 7. The storage and processing devices of claim 11 perform the functions in 17[a]-[c], which correspond to 7[a]-7[c]. Because the claim 11 devices are configured for the claim 7 functions, claim 17 is invalid for the same reasons as claims 7 and 11.

RAVE/MSI, EX1005, p. 311

562. Claim 17 also and corresponds to claim 16 of the ’757 Patent. I have compared the two claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 16 of the ’757 Patent, which I incorporate here. For the reasons stated in that analysis, which I incorporate here, it is my opinion that claim 17 of the ’421 Patent is disclosed for the same reasons as its ’757 counterpart.

7. Claim 18

563. In my opinion Staton in view of Noland renders obvious every limitation of claim 18 of the ’421 Patent. Claim 18 is the system counterpart to claim 8, with limitations 18[a]-[c] corresponding to 8[a]-8[c]. . Claim 18 is therefore disclosed for the same reasons as claims 8 and 11, which I incorporate here.

8. Claim 19

564. In my opinion Staton in view of Noland renders obvious every limitation of claim 19 of the ’421 Patent.

a. ***19[a]: The system of claim 18, wherein: the at least one signal made by the supervisee comprises shaking the supervisee device abruptly, pressing a button, or speaking a specific phrase, wherein: the at least one sensor is configured for detecting the at least one signal,***

565. For limitation 19[a], the claim is written in the alternative, so disclosure of any one of the three listed signals satisfies it. The panic-button press I mapped for claim 18 is “pressing a button.” Ex.1008 ¶[0104]. The instrument module detects

that press and, upon detection, generates an event message and supplies positional information. Ex.1007, 9:2-9; Ex.1008 ¶[0104].

b. ***19[b]: and the supervisee device is configured to optionally make an emergency call when the at least one sensor detects the at least one signal;***

566. For limitation 19[b], the supervisee device is configured to optionally make an emergency call when the sensor detects the signal. Staton states that "a PDA 105 can be configured with a calling number for the monitoring PDA 106, such that when an event occurs, PDA 105 automatically dials monitoring PDA 106." Ex.1007, 24:56-25:7. Thus, the call is optional because Staton's events are individually configurable, so the supervisor determines which events trigger the automatic dial and which do not. *Id.,* 11:27-50.

c. ***19[c]: wherein a phone number dialed in the emergency call is determined based on the geofence.***

567. For limitation 19[c], the phone number dialed is determined based on the geofence. Staton states that when a message reporting the occurrence of an event arrives at the control center, "the control center looks up the correct PDAs to contact in the resources database 670 and any other parties that must be contacted, such as the police or 911." *Id.,* 26:65-27:3. The event that triggers that lookup is a geofence event, because Staton states that "the entering or leaving a geographical area that has been geofenced can be an event itself" and that an event related to a geographical zone can trigger communication from one PDA to another. *Id.,* 13:65-14:13. The

recipient of the resulting call is therefore selected using data generated by the supervisee's position relative to the geofence. In my opinion a POSITA would have understood that relationship to satisfy the limitation because the lookup operates on the event record, and the event record exists only because the geofence boundary was crossed, so the geofence supplies the condition that determines which stored number is dialed.

568. Accordingly, it is my opinion that Staton in view of Noland renders obvious each limitation of claim 19 of the '421 Patent.

9. Claim 22

569. In my opinion Staton in view of Noland renders obvious every limitation of claim 22 of the '421 Patent. Claim 22 is an independent method claim with no counterpart in the '757 Patent, so I analyze it on its own. I note at the outset that claim 22 does not recite the geofence grid boxes, the grid parameter, or any of the other grid-box limitations that appear in claims 1 and 11. It recites instead the same supervision architecture, a sensor in the supervisee device, audio and video recordings, proximity-based selection among nearby sensors, and sensor-to-sensor tracking of the supervisee.

570. Limitations 22[pre] through 22[h] recite the same method steps I addressed for limitations 1[pre] through 1[i] of claim 1, with two exceptions: claim 22 omits the step of generating a geofence, and limitation 22[e] analyzes the

RAVE/MSI, EX1005, p. 314

supervisee data "based on the geographical location" rather than based on the geofence. For the steps that are common to both claims, I apply the mappings I set out for claim 1 and incorporate that analysis here, including the communication device, processing device, storage device, supervisor device, and supervisee device mappings.

571. Limitation 22[e] is satisfied on an independent basis, and in my opinion it is satisfied more readily than the corresponding step of claim 1. Limitation 1[f] requires that the supervisee data be analyzed based on the geofence, which required me to connect Staton's zone construction to its position testing. Limitation 22[e] requires only that the supervisee data be analyzed based on the geographical location received from the supervisor device in limitation 22[b]. Claim 22 recites no geofence at all, so nothing in limitation 22[e] requires that the analysis be derived from a generated boundary. Staton analyzes the supervisee's reported position against the geographical location the supervisor selected: a geographical area is mapped to each pixel 505 of the pixel map 500 that represents the selected area, Ex.1007, 16:47-52, and the system determines which pixel a reported position falls in when it evaluates that position against the selected area. *Id.,* 15:4-9. That evaluation is an analysis of supervisee data based on the geographical location, whether or not the selected area is characterized as a geofence. The same disclosures I relied on for limitation 1[f] therefore satisfy limitation 22[e].

RAVE/MSI, EX1005, p. 315

572. Limitations 22[i] through 22[k] recite the same three sensor requirements as limitations 8[a] through 8[c]; however, I rely on a different sensor for the claim 22 sensor elements than I did for the claim 8 sensor elements.

a. ***22[i]: the at least one supervisee device comprises at least one sensor,***

573. For limitation 22[i], the supervisee device comprises at least one sensor. Staton's instrument module 195 and PDA 105 "can be in the same housing," and the instrument module is expressly designed to be "included upon/in various articles or electrical devices, or in the PDA itself," and to "collect, process, and communicate information about the article or electrical devices to which the instrument module is connected." Ex.1007, 10:26-27, 6:34-43. Noland's sensors are designed for exactly that kind of external connection: the acoustic and image sensors "can optionally be provided outside of the threat sensing device 10 housing 12, using one or more of the communication port(s) 16 and associated cable or connector," and may be "connected to the housing 12, through an input/output port (*e.g.*, port 16), or hardwired directly into the threat sensing device 10." Ex.1008 ¶[0068]. Noland further discloses that the input/output ports of the threat sensing device "may be used to send and receive data externally to and from some external device (*e.g.*, a sensor, a motion sensor, an output device, a countermeasure, etc.)," so that "any data output from the external device would be sent to the system gateway 110 through the threat sensing device." *Id.* ¶[0201]. In the combined system, Noland's acoustic and image-

based sensors report through Staton's instrument module, and because that module can reside in the same housing as PDA 105, the supervisee device comprises at least one sensor within the meaning of the claim. Ex.1007, 10:26-27.

574. Staton's instrument module is the component through which the supervisee device acquires sensor input, and Staton expressly contemplates that the module serves articles and devices to which it is connected rather than only components inside the PDA shell. *Id.,* 6:34-43. A POSITA implementing the combination would have had the room-mounted sensors report through that module, because the module already supplies the detection and reporting path to PDA 105 and from PDA 105 to the backend. *Id.,* 9:2-9.

b. ***22[j]: wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,***

575. For limitation 22[j], the sensor is configured for detecting at least one signal made by the supervisee. Noland's acoustic sensors 20 "record[] audio of an acoustic event using one or more acoustic sensors," and its image-based sensors 40 "observe images in the field of view using one or more optic sensors." Ex.1008 ¶[0130]. A sound or a movement made by the monitored individual within the sensor's field of view or pickup range is a signal made by the supervisee that those sensors detect. Noland confirms that its sensors detect human-originated signals, disclosing that geophone sensors "can be used to distinguish kids from adults based on the amplitude and frequency of their footsteps and can be programmed to detect

other patterns," (*id.* ¶[0147]), and that the vision-based system detects "an individual being threatened and holding their hands up," along with "body posture" and "multiple targets" *Id*. ¶¶[0118], [0119]. Staton's instrument module architecture already contemplates detection of this kind, because the module is configurable to detect when "a preconfigured event has occurred" and to "execute an operation upon the detection of the signal." Ex.1007, 9:2-5.

c. ***22[k]: wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting,***

576. For limitation 22[k], the sensor is configured for generating the supervisee data based on that detecting. In Noland, the detected image and acoustic data "is then transmitted to and stored in a physical computer-readable storage medium," Ex.1008 ¶[0130], and the sensors report the sensed information to the system gateway 110. *Id*. ¶[0091]. In Staton, the instrument module generates and transmits an event message to PDA 105 upon detecting a signal from a connected device, and PDA 105 transmits it onward to the backend control system. Ex.1007, 9:2-9. The generation is "based on the detecting" because in both references the data is composed only after the sensor registers the signal.

d. ***22[l]: wherein the supervisee data comprises audio and video recordings;***

577. For limitation 22[l], the supervisee data comprises audio and video recordings. Noland's image-based sensors "may further comprise built-in

communication module configured to transmit live video and audio to the system gateway 110 for storage or dissemination (*e.g.*, to school and city emergency coordination facilities, etc.) as needed." Ex.1008 ¶[0126]. Noland separately confirms that the two modalities are captured together, stating that the acoustic sensors record audio while the image-based sensors observe images, and that "[t]he image data and the acoustic data is then transmitted to and stored in a physical computer-readable storage medium." *Id.* ¶¶[0126], [0130].

e. ***22[m]: wherein the at least one sensor is selected from one or more nearby sensors based on the most proximal nearby sensor by geographical location in real-time; and***

578. For limitation 22[m], the sensor is selected from one or more nearby sensors based on the most proximal nearby sensor by geographical location in real time. Noland deploys many sensors across the monitored area, disclosing "a plurality of threat sensing devices 10a, 10b, 10c, . . . , 10n, where n represents any integer, distributed through classrooms, hallways, rooms, gymnasium, cafeteria, and offices throughout the school." Ex.1008 ¶[0091]. Each device's geographical location is known to the system, because "the geometry of each room (*e.g.*, dimensions of the room, etc.) and location (*e.g.*, room number, location in school, etc.) in which a threat sensing device 10 is installed is entered into the system, as is the location, height and orientation of the threat sensing device," (*id.* ¶[0113]), and because the administrator identifies each installed unit "by its school name, room number, and room type . . .

or zone location." *Id*. ¶[0225]. Noland then selects among those sensors by proximity. It states that "the sound waveform determined to have the greatest amplitude is the threat sensing device 10 closest to the gunshot (*i.e.*, establishing the location of the gunshot)," and that "[t]he system gateway 110 correlates the known location of the threat sensing device 10 closest to the location of the gunshot." *Id.* ¶[0111]. Noland repeats the point in its description of the gateway's processing, stating that "[t]he system gateway 110 can use the highest 'rating' reporting gunshot sensor device to determine the location of the shooter." *Id.* ¶[0205]. The selection is in real time because Noland performs it on the arriving sensor reports as the event unfolds: the gateway "has an internal clock and emits multiple pulses per second to receive, sequentially, information from each connected threat sensing device 10," and it uses those time stamps and times of arrival to resolve the event location. *Id.* ¶[0145]. Noland also discloses that each device is separately addressable for this purpose, because "each threat sensing device 10a . . . 10n is assigned a unique hardware address that is recognized by the system gateway 110." *Id.* ¶[0095]. Selecting the device with the strongest reported signal from among the devices whose locations the system already stores is a selection of the most proximal nearby sensor by geographical location.

f. ***22[n]: wherein the at least one sensor tracks the supervisee as the supervisee moves between the one or more nearby sensors.***

579. For limitation 22[n], the sensor tracks the supervisee as the supervisee moves between the nearby sensors. Noland's sensors hand tracking off from one to the next. Noland states that the images its image-based sensors record "enable application of facial recognition software and hardware to operate and to also track potential threats (*e.g.*, within a room and from room to room)." Ex.1008 ¶[0116]. It further states that "[a]fter facial identification images have been obtained by the threat sensing device 10, the threat sensing system 100 can report facial recognition information to other threat sensing device located throughout a facility to more quickly and accurately track the threat." *Id.* ¶[0124]. Noland also discloses a time-based algorithm that distinguishes a single individual moving between rooms from two individuals in separate rooms, stating that it can "determine if one shooter is moving to different rooms or two shooters are active in two different rooms." *Id.* ¶[0229]. Each of those disclosures describes tracking of an individual as the individual passes from the coverage of one sensor into the coverage of another.

580. Noland's tracking disclosures describe tracking a threat or shooter while limitation 22[n] requires tracking "the supervisee." In my opinion the difference does not affect the analysis, for three reasons. First, the tracking mechanism Noland discloses is indifferent to the role of the person tracked. Facial

recognition applied to captured images, reported from one threat sensing device to the others, and resolved by a time-based algorithm operates on whatever face the sensors capture; nothing in the technique depends on that person being hostile. *Id.* ¶¶[0116], [0124], [0229]. Second, Noland applies the same tracking to persons who are not threats. It discloses pre-programming the sensors "to look for a particular person of interest even in the absence of any particular threat," giving the example of a suspended student whose images are added to an alert database so the system "can activate an alert if the student unexpectedly shows up at school while on suspension," together with "the point of entry." *Id.* ¶[0125]. It discloses using its geo-fence "to track the entry and exit of persons bearing a location-aware device, such as a smart phone having a location-based service (LBS) activated," and discloses that "[n]ear field sensors could be used to allow the system to identify mobile phones, other mobile devices and the owners of those phones, and monitor the arrival and departure of those device owners from the geo-fenced area." *Id.* ¶[0148]. It discloses tracking first responders, stating that geo-fencing allows "the system to locate first responders as they arrive at the location of the adverse event and track a location of, or presence of, such first responders." *Id.* Noland therefore tracks monitored persons as well as threats. Third, the supervisee in the combined system is the person carrying Staton's PDA 105, and Staton's architecture already reports that person's position continuously to the backend. In the combination, the

tracked individual is the supervisee because the supervisee is the person the system is deployed to monitor. For these reasons a POSITA would have understood Noland's sensor-to-sensor tracking to track the supervisee, and would have had a reasonable expectation of success in applying it to the monitored individual, because doing so requires no change to the technique and Noland already applies it to non-threatening persons of interest. *Id.* ¶[0125].

581. Accordingly, it is my opinion that Staton in view of Noland renders obvious each limitation of claim 22 of the '421 Patent.

10. Claim 23

582. In my opinion Staton in view of Noland renders obvious every limitation of claim 23 of the '421 Patent.

a. ***23[a]: The method of claim 22, wherein: the supervision notification is sent to a first distinct group of one or more supervisor devices correlated with the geographical location;***

583. For limitation 23[a], the notification is sent to a first distinct group of supervisor devices correlated with the geographical location. Staton states that the control center, upon receiving a message reporting the occurrence of an event, "looks up the correct PDAs to contact in the resources database 670 and any other parties that must be contacted, such as the police or 911." Ex.1007, 26:65-27:3. The resulting recipient set is a distinct group of devices, and it is correlated with the geographical location because the lookup operates on an event record carrying the

geocoded location of the event. *Id.,* 22:18-35. Noland performs the same correlation through its own architecture, routing notifications from the system gateway serving the affected building to "mobile devices 130, dispatchers 132, first responder portable devices 135," and routing them through "the local 911 Emergency Management Center" for that location. Ex.1008 ¶[0091]; *id*. ¶[0198]. Noland also states that the recipients are chosen "as appropriate to the adverse event," which is the event occurring at that location. *Id*. ¶[0092].

b. ***23[b]: the first distinct group of one or more supervisor devices is comprised of nearby first responders and dispatchers; and***

584. For limitation 23[b], the first distinct group comprises nearby first responders and dispatchers. Noland identifies both categories as recipients, disclosing transmission to "dispatchers 132, first responder portable devices 135," (*id.* ¶[0091]), and to "law enforcement first responders, EMSA (Medical), dispatchers and emergency management centers." *Id*. ¶[0109]. Noland also discloses a mobile messaging channel to "the Gunshot Emergency Manager located in dispatch or the 911 center." *Id.* ¶[0019]. Those recipients are nearby in the sense the claim requires because Noland locates and tracks them relative to the event: its geo-fencing allows "the system to locate first responders as they arrive at the location of the adverse event and track a location of, or presence of, such first responders." *Id.* ¶[0148]. Noland further supplies the responders with "closest entry point(s)" for the

affected building, confirming that the system reasons about responder proximity to the event location. *Id.* ¶[0109].

c. ***23[c]: the supervision notification may be sent to a second distinct group of one or more supervisor devices based on the location and expertise of the second distinct group.***

585. For limitation 23[c], the notification may be sent to a second distinct group of supervisor devices based on the location and expertise of that group. Noland discloses distinct additional recipient groups differentiated by professional role. It states that notification reaches "designated first-responders, government personnel, and school officials . . . as appropriate to the adverse event," Ex.1008 ¶[0092], and that client software is installed for "first responders and other potentially affected entities or groups (*e.g.*, school districts, government officials, transportation offices, hospitals, clinics, etc.)" so the system "is able to send adverse event related information to potentially involved computer systems and receive inputs therefrom." *Id*. ¶[0109]. It separately discloses two-way communication among "police, first responders, teachers, administrators, government authorities and, optionally, parents." *Id.* A hospital, a transportation office, and a school administrator are groups distinguished by expertise rather than by first-responder status, and each is selected for the event at its location. Noland also discloses notifying "communication systems of other nearby business and schools," giving the example of a shooting in one end

of a mall broadcast "to all other tenants in that mall or surrounding areas," which is a second recipient group selected by location. *Id.* ¶[0136].

586. In my opinion a POSITA would have been motivated to implement these role-differentiated recipient groups in Staton's system. Staton already stores per-device contact and relational records in resources database 670 and already selects recipients from them for each event. Ex.1007, 24:12-16, 26:65-27:3. Adding a role or expertise attribute to those stored records, and selecting on it alongside the location Staton already evaluates, makes the recipient set more granular without altering the lookup Staton already performs. A POSITA would have expected success because the modification stores an additional field on records Staton already maintains and supplies that field to a selection step Staton already executes.

587. Accordingly, it is my opinion that Staton in view of Noland renders obvious each limitation of claim 23 of the '421 Patent.

11. Claim 24: The method of claim 22, wherein: wherein the supervisee is associated with at least one identification, wherein the communication device is further configured for receiving at least one indication corresponding to the at least one identification from the at least one supervisee device, wherein the processing device is further configured for identifying the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying.

588. In my opinion Staton in view of Noland renders obvious every limitation of claim 24 of the '421 Patent. Claim 24 depends from claim 22 and recites

substantively the same three requirements recited in claims 10 and 20, which I addressed in my Ground 1 analysis above. I incorporate that analysis here.

589. Accordingly, it is my opinion that Staton in view of Noland renders obvious each limitation of claim 24 of the '421 Patent.

C. Ground 3: Claim 9 of the '421 Patent Is Rendered Obvious By Staton (Ex.1007) In View Of Smith (Ex.1011) + Knowledge Of A POSITA

1. A POSITA would have combined Staton with Smith

590. Claim 9 depends from claim 1. I explained above why Staton discloses or renders obvious claim 1, and I incorporate that analysis here. For the three additional limitations of claim 9, I rely on Staton in view of Smith for the reasons that follow.

591. Both references are directed to the same field of endeavor as the '421 Patent: facilitating supervision of individuals based on geofencing. Ex.1003, 1:7-18. Staton defines geographical zones, loads them onto a portable device, and generates event messages when the device enters or leaves a zone. Ex.1007, 13:65-14:13. Smith is in that same field, and specifically concerns three-dimensional, altitude-based geofencing. Smith defines virtual boundaries in a geographical space and triggers actions based on the position of a tracked device relative to those boundaries, stating that it provides "a method of three-dimensional geofencing" in which "[a] boundary-related event and an action to be triggered based on the position of a

trackable object is defined with respect to the virtual boundary." Ex.1011, Abstract. Each reference is therefore in the field of endeavor of the claimed invention and is also reasonably pertinent to the problem the named inventor addressed.

592. A POSITA would have been motivated to incorporate Smith's altitude parameter into Staton's zone-definition process, and Smith itself supplies the reason. Smith identifies the two-dimensional character of prior geofencing as a specific technical shortcoming, stating that "prior art geofencing techniques are generally two-dimensional (*i.e.*, are defined within a planar map) and thus do not comprehend an altitude, height, or 'z-axis' attribute," with the consequence that "such systems are not capable of determining, for example, whether a user is actually located within an apartment complex or other tall structure" and "are not able to determine whether a user has changed floors within a home." Ex.1011, 1:27-36. Staton's zones exhibit exactly that limitation: Staton defines its zones by latitude and longitude attributes mapped into a planar pixel map, Ex.1007, 15:27-34, so a Staton zone drawn around a multi-story building cannot distinguish a supervisee on one floor from a supervisee on another. In my opinion a POSITA supervising persons in the environments Staton expressly contemplates, which include a home environment, a work environment, and a school zone, Ex.1007, 2:40-45, would have recognized that floor-level resolution matters in each of them, because a report that a child is somewhere inside a multi-story school does not tell a responder where to go.

593. Smith states the emergency-response benefit directly, disclosing that "first responders may use altitude data to determine which floor (*e.g.*, 981 or 982) the user is on during an emergency situation, such as during a fire." Ex.1011, 5:62-65. That is the same supervision purpose Staton's system serves, and it is the purpose the '421 Patent's specification describes.

594. A POSITA would also have had a reasonable expectation of success because Staton already reports altitude as part of its position telemetry, disclosing that "the PDA may detect geographical boundaries crossings, route and schedule adherence of a individual or host vehicle, reporting of position, speed, mileage, direction of travel, acceleration and altitude of the PDA, an individual or a host vehicle." Ex.1007, 5:10-14. The altitude value already travels from the supervisee device to the backend in the ordinary course of Staton's operation, so the combination does not require Staton to acquire any new category of data. What Staton lacks is the use of altitude as a boundary-defining input, and that is what Smith supplies. Smith confirms that the necessary sensing is conventional, disclosing that the altitude value may be estimated using "an altimeter module 520, an altimeter module 521, and or an accelerometer module 522," Ex.1011, 3:58-62, and claiming estimation "via at least one of a barometer, an altimeter, and an accelerometer located within the trackable object." *Id.,* claim 13. Extending Staton's zone definition by one axis therefore uses data Staton already transmits and sensors

a POSITA would have recognized as standard, and it leaves Staton's zone-construction and event-processing framework otherwise intact. Adding Smith's technique of using altitude/z-axis attribute information to define a boundary in Staton's system would therefore been within the level of skill in the art, and would require nothing more than a straightforward software implementation of Smith's disclosures.

2. Claim 9

595. In my opinion Staton in view of Smith renders obvious every limitation of claim 9 of the '421 Patent.

596. Before turning to the individual limitations, I address the relationship between the two altitude disclosures in the combination. Smith's altitude parameter is an input the user supplies to define the boundary. Smith's method recites "receiving, via the user-carried mobile device, user input defining a virtual boundary in a three-dimensional geographical space, the virtual boundary including lateral position parameters and an altitude parameter." Ex.1011, claim 1. Smith confirms that the definition is a user act performed through an interface, stating that "[d]efining the boundary may be accomplished by a user (using an appropriate user interface) operating a computing device or the trackable object itself," and that "the user defines the boundary explicitly using position and range values." *Id.,* 4:63-67.

Staton's altitude, by contrast, is telemetry the supervisee device reports about its own position. Ex.1007, 5:10-16.

a. ***9[a]: The method of claim 1, wherein: the at least one security parameter comprises an altitude,***

597. For limitation 9[a], the at least one security parameter comprises an altitude. In the combined system, the supervisor supplies an altitude alongside the zone-defining properties Staton already accepts. Staton's zones carry a set of supervisor-configured properties: "[t]he properties of a Zone include a name, description and a flag determining if the Zone is an off-limits Zone or an enclosed Zone," Ex.1007, 14:50-55, and "each irregular Zone may have additional parameters such as speed threshold of the entity, flagged as a 'no-fly zone,' color coded in order of danger or security threat, communication enabled or disabled, etc." *Id.,* 16:11-17. Those are the properties I mapped as the security parameter for limitation 1[a]. Smith's altitude parameter is a property of the same kind, supplied by the same actor through the same configuration interface, and serving the same function of determining what the resulting boundary covers. Adding it to Staton's existing property set makes the security parameter comprise an altitude. I note that Staton's own property list is expressly open-ended, since it recites the enumerated parameters as examples followed by "etc." *Id.,* 16:11-17.

RAVE/MSI, EX1005, p. 331

b. ***9[b]: the at least one grid parameter comprises a building floor, and***

598. For limitation 9[b], the at least one grid parameter comprises a building floor. Nothing in claim 9 requires the building floor to be the only grid parameter, and nothing requires it to displace the resolution setting I mapped in claim 1.

599. The building floor functions as a grid parameter in the combined system. A grid parameter, as claim 1 uses the term, is a supervisor-supplied input that the processing device analyzes in order to determine the extent of each grid box and the number of grid boxes generated. Staton's resolution value performs that function horizontally: "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," and "[t]he increase in number of rectangles increases the resolution because each rectangle covers less geographical area." Ex.1007, 15:46-57. A floor designation performs the same function vertically. Each floor is a defined slice of the structure, the set of floors partitions the structure's vertical extent, and the number of floors the supervisor designates determines how many such slices exist and how much of the building each one spans. Smith discloses the structure so divided, describing a building that "includes multiple (*i.e.*, 3) stories, or 'floors', including a first floor, a second floor 982, and a third floor 981," and a system that determines "whether a trackable object 504 (carried by a user, not illustrated) is on the third floor 981 or

982, and act[s] accordingly." Ex.1011, 5:32-48. Smith further confirms that the floor is the frame of reference in which the supervisor sets the boundary's vertical extent, stating that "the current location of the trackable object is set as the z-distance for a boundary (*e.g.*, first floor, second floor, etc.)." *Id.,* 5:3-6.

600. In the combined system, therefore, the supervisor's input defines a grid in both dimensions: the resolution value determines how finely the selected area is subdivided in plan, and the floor designation determines how the resulting column is subdivided in elevation. Each resulting cell is a grid box characterized by a grid box geofence area, consistent with limitation 1[j]. A POSITA would have expected success in making that extension because Staton's subdivision logic is already parameter-driven and already converts a supervisor-supplied granularity value into a count and extent of subdivisions, Ex.1007, 15:46-57, and because the floor designation supplies the same kind of value along a different axis.

c. ***9[c]: the building floor is estimated from the altitude.***

601. For limitation 9[c], the building floor is estimated from the altitude. Smith discloses the estimation as a two-stage operation. First, available altitude information is "provided to an altitude estimation module 1002, which determines an altitude (z-value) estimate 1004," with "weights and/or confidence levels" associated with each input "to determine an optimal estimate." Ex.1011, 4:37-44. Second, that estimate is supplied with the lateral position data to a decision module

that resolves the object's position against the defined boundary: "conventional two-dimensional positioning data (*e.g.*, GPS data) 1003 is determined and provided to decision module 1005 along with altitude data 1004," and "decision module 1005 determines which, if any, action 1008 should occur." *Id.,* 4:44-50. Smith states the floor-level output of that operation in terms, disclosing that the system "might determine whether a trackable object 504 . . . is on the third floor 981 or 982, and act accordingly," Ex.1011, 5:46-48, and that "first responders may use altitude data to determine which floor (*e.g.*, 981 or 982) the user is on during an emergency situation." *Id.,* 5:62-65. Determining which floor the user is on from the altitude estimate is the estimation of a building floor from an altitude that limitation 9[c] recites.

602. I note that limitation 9[c] confirms the reading of limitation 9[b] I gave above. Limitation 9[c] recites that the system derives the floor from an altitude value, which is consistent with the supervisor supplying an altitude that defines the vertical grid and the system resolving floor identity from it. The two limitations describe the two halves of a single operation, and Smith discloses both halves.

603. Accordingly, it is my opinion that Staton in view of Smith renders obvious each limitation of claim 9 of the '421 Patent.

RAVE/MSI, EX1005, p. 334

D. Ground 4: Claims 1-4, 6-8, 10-14, and 16-21 of the '421 Patent Are Rendered Obvious By Rauner (Ex.1009) In View Of Azmoodeh (Ex.1010) + Knowledge Of A POSITA

604. Claim 1 is an independent method claim and claim 11 is an independent system claim. Claims 2, 3, 4, 6, 7, 8, and 10 depend from claim 1, and claims 12, 13, 14, 16, 17, 18, 19, 20, and 21 depend from claim 11.

605. In my opinion Rauner's emergency response computer system includes components corresponding to the claimed communication device, processing device, and storage device, for the reasons I set out in my Ground 3 analysis of the '757 Patent in Section [IX.C] above, which I incorporate here.

1. A POSITA would have combined Rauner with Azmoodeh

606. I set out the Rauner-Azmoodeh combination rationale in my '757 Ground 3 analysis in Section [IX.C.1] above, and I incorporate it here in full. That analysis establishes that both references are in the same field of endeavor as the Asserted Patents, facilitating supervision of individuals based on geofencing, and are also reasonably pertinent to the problem the named inventor addressed; that Rauner supplies the geofence, the map substrate, the coordinate processing, and the emergency-response architecture, while Azmoodeh supplies the structural subdivision of the fenced region and the user-configurable count of subdivisions; that a POSITA would have been motivated to add that subdivision in order to determine where within a geofenced area a device is located rather than merely that

it is inside; and that a POSITA would have had a reasonable expectation of 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," to Rauner's mapping module 158, which already creates a GPS-integrated "alphanumeric grid" and calculates coordinate ranges for each grid box, because both references implement geofencing as processor-executed software, because dividing a known geofence area by a user-specified cell count or cell size is basic arithmetic performed on coordinates Rauner already computes, and because Rauner's administrator already enters configuration values through administration module 157. Ex.1009 ¶¶[0092]-[0094], [0097]; Ex.1010 ¶¶[0033], [0046].

607. Two points warrant statement in the '421 context.

608. First, the analogous-art analysis applies to the '421 Patent for the same reason it applies to the '757 Patent. The problem to be solved in the '421 Patent relates to conventional geofencing applications not allowing a user to create a geofence easily, Ex.1003, 1:22-29, and the '421 Patent carries largely the same specification as the '757 Patent. My conclusion that Rauner and Azmoodeh are analogous art is therefore the same for the '421 claims as for the '757 claims.

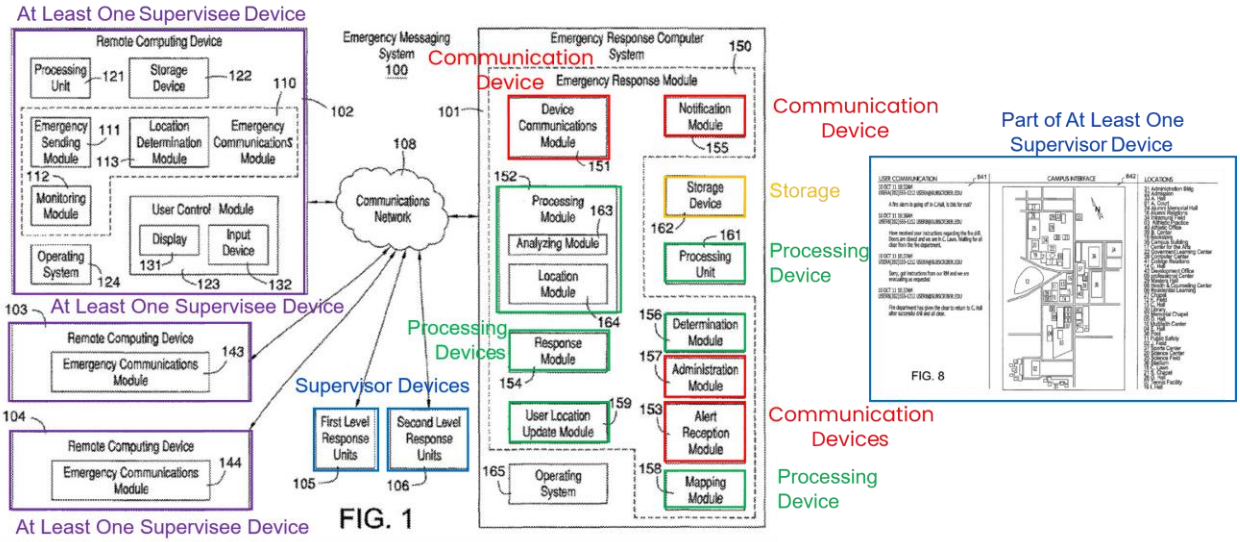
609. Second, Applicant explained in the '421 Patent prosecution record has a similar disclosure regarding the claimed devices. Ex.1004, 207-208.

RAVE/MSI, EX1005, p. 336

610. I set out this ground's rationale by cross-reference rather than repetition because Ground 4 is the predicate for Grounds 5 and 6, and those grounds build on the same Rauner-Azmoodeh combination.

2. Claim 1

611. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 1 of the '421 Patent. I reach that conclusion for the same reasons that I set out for claim 1 of the '757 Patent in my Ground 3 analysis in Section [IX.C.2] above, which I incorporate here.



Ex.1009, Figs. 1 and 8 (annotated).

612. I apply the same mappings throughout this analysis.

613. I have compared claim 1 of both patents limitation by limitation. Limitations 1[pre] through 1[j][4] of '421 claim 1 recite substantially the same method steps as limitations 1[pre] through 1[j][4] of '757 claim 1, and the '421

Patent carries largely the same specification as the ’757 Patent. The two claims are therefore substantially similar, and the technical mappings I applied to ’757 claim 1 in the Ground 3 analysis apply here.

614. There is one difference in wording. Issued ’757 claim 1 includes, within limitation 1[j][1], the phrase “wherein the processing device is further configured for,” and issued ’421 claim 1 does not; its 1[j][1] recites only “receiving, using the communication device, at least one grid parameter from the at least one supervisor device” before proceeding directly to the analyzing step. In my opinion that difference is immaterial to the obviousness analysis. The omitted phrase is a configured-for recitation embedded in a method claim whose surrounding steps are already affirmatively recited as performed “using the processing device.”

615. As to the priority date, I have assumed, without conceding, that the challenged claims are entitled to the March 5, 2019 priority date, and I have applied that date in assessing Rauner and Azmoodeh. My opinion as to the level of ordinary skill in the art is as I stated it above. I understand that Rauner qualifies as prior art based on its effective filing date, and that Azmoodeh, published October 5, 2017, qualifies as prior art as of its publication.

616. For the reasons stated in my Ground 3 analysis of ’757 claim 1, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 1 of the ’421 Patent.

RAVE/MSI, EX1005, p. 338

3. Claim 2

617. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 2 of the ’421 Patent. Claim 2 depends from claim 1 and corresponds to claim 2 of the ’757 Patent. I have compared the two claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 2 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here.

618. For the reasons stated in my analysis of ’757 claim 2, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 2 of the ’421 Patent.

4. Claim 3

619. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 3 of the ’421 Patent. Claim 3 depends from claim 1 and corresponds to claim 3 of the ’757 Patent. I have compared the two claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 3 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here.

RAVE/MSI, EX1005, p. 339

620. For the reasons stated in my analysis of ’757 claim 3, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 3 of the ’421 Patent.

5. Claim 4

621. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 4 of the ’421 Patent. Claim 4 depends from claim 1 and corresponds to claim 4 of the ’757 Patent. I have compared the two claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 4 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here.

622. For the reasons stated in my analysis of ’757 claim 4, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 4 of the ’421 Patent.

6. Claim 6

623. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 6 of the ’421 Patent. Claim 6 depends from claim 1 and corresponds to claim 6 of the ’757 Patent. I have compared the two claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set

RAVE/MSI, EX1005, p. 340

out for claim 6 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here.

624. For the reasons stated in my analysis of ’757 claim 6, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 6 of the ’421 Patent.

7. Claim 7

625. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 7 of the ’421 Patent. Claim 7 depends from claim 1 and corresponds to claim 7 of the ’757 Patent. I have compared the two claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 7 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here.

626. For the reasons stated in my analysis of ’757 claim 7, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 7 of the ’421 Patent.

8. Claim 8

627. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 8 of the ’421 Patent. Claim 8 depends from claim 1 and corresponds to claim 8 of the ’757 Patent. I have compared the two claims

limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 8 of the '757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here, as well as an additional basis based on Rauner's panic button, as set forth below.

- For limitation 8[a], as discussed for claim 8 of the '757 Patent in my Ground 3 analysis, Rauner discloses that the supervisee device, remote computing device 102, includes a microphone as part of input device 132. Ex.1009, ¶¶[0061]-[0062]. This type of sensor was also envisioned by the '421 patent. Ex.1003, 24:55-59 ("audio sensors (such as a microphone)"). Additionally, Rauner teaches that input device 132 includes sensors such as a panic button. Ex.1009, ¶¶[0061], [0110]. The panic button is a sensor because it detects the presence of a user-initiated action—pressing.
- For limitation 8[b], as discussed for claim 8 of the '757 Patent in my Ground 3 analysis, Rauner discloses that the microphone detects the user's voice, which is a signal made by the supervisee. Ex.1009, ¶[0105], [0180]. Additionally, Rauner discloses that the button detects a signal made by the supervisee in the form of the supervisee's press. Ex.1009, ¶¶[0110], [0088].

RAVE/MSI, EX1005, p. 342

- For limitation 8[c], as discussed for claim 8 of the ’757 Patent in my Ground 3 analysis, Rauner discloses that the microphone’s audio recording generates supervisee data based on the detecting of the user’s voice, which is transmitted to device communications module 151, along with the supervisee’s location. Ex.1009, ¶¶[0111], [0113]. Additionally, Rauner discloses that a detection of the user’s button press initiates an Emergency Communication Event, and the emergency sending module transmits it to device communications module 151, along with the device location, as supervisee data. Ex.1009, ¶¶[0110]-[0111].

628. For the reasons stated in my analysis of ’757 claim 8, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 8 of the ’421 Patent.

9. Claim 10

629. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 10 of the ’421 Patent.

a. ***10[a]: The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises:***

630. For limitation 10[a], the supervisee is associated with at least one identification. In Rauner, each monitored individual is associated with a stored user record carrying a unique identifier. Rauner states that the “911 call initiated notice

message" produced when a user reports an emergency includes "unique user ID, user name from profile, user location, time, date, call path, time to process call." Ex.1009 ¶[0050]. The unique user ID is an identification with which the supervisee is associated, and the reference to the user name "from profile" confirms that the identifier is resolved against a stored record rather than generated for the single message. Rauner describes that stored record, reciting "storing in one or more databases a profile for the portable communication devices associated with each of the two or more users." *Id.* ¶[0037]. The profile is maintained in storage device 162, which Rauner identifies as the repository for user profiles together with the location information written into them. *Id.* ¶[0070].

b. ***10[b]: receiving, using the communication device, at least one indication corresponding to the at least one identification from the at least one supervisee device; and***

631. For limitation 10[b], the communication device receives an indication corresponding to that identification from the supervisee device. Rauner states that, after the user submits an emergency trigger message, "emergency sending module 111 sends the emergency trigger message and the current location information to device communications module 151 over communications network 108." *Id.* ¶[0111]. Device communications module 151 is part of the communication device I mapped for limitation 1[a], and emergency sending module 111 runs on the supervisee's own remote computing device, so the transmission is received using the

communication device from the supervisee device. Rauner confirms that the transmission carries the information that ties the message to the stored user record, stating that the system "associates the 'caller's' (user managed) emergency information profile with the emergency communication event." *Id.* ¶[0110]. In my opinion that information is the claimed indication corresponding to the identification because the backend uses it to attach the caller's profile to the event. Rauner describes the same inbound path for location data, stating that "emergency communications module 110 transmits GPS location information to device communications module 151" and that "user location update module 159 updates the user profile stored in a database of storage device 162 with GPS location information." *Id.* ¶[0071]. Writing the received data into that user's profile is based on resolving the transmission to that user.

c. ***10[c]: identifying, using the processing device, the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying.***

632. For limitation 10[c], the processing device identifies the supervisee based on that indication. The notice message Rauner generates carries the resolved identity as its output, including the "unique user ID" and the "user name from profile." *Id.* ¶[0050]. In my opinion that output reflects a successful identification has occurred because the name cannot be populated from the profile in the database unless the processing device has first determined which profile corresponds to the

incoming message. Rauner places that resolution in the server-side processing components, stating that processing module 1652 "can be configured to receive the location information of the remote computing device sending the emergency trigger information (the 'emergency location') from device communication module 151 and process the emergency location information," and that the associated determination module 1666 runs on processing unit 161. *Id.* ¶¶[0167]-[0168]. Those are parts of the processing device components I mapped for limitations 1[c] and 1[f].

633. The notification dependency in limitation 10[c] is also disclosed because the generating of the supervision notification is based on that identification. The 911 call initiated notice message is itself the notification Rauner transmits, and it is composed of the identified user's stored data before being "transmitted to a system administrator contact." *Id.* ¶[0050]. Rauner's reports carry the same dependency, because its claim 6 recites providing user profile information with the reported device locations, including a name and a phone number. Ex.1009, claim 6. The notification therefore cannot be generated in the form Rauner describes until the supervisee has been identified and that supervisee's profile data retrieved. That is the same notification pathway I mapped for limitations 1[g] and 1[h].

634. Accordingly, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 10 of the '421 Patent.

10. Claim 11

635. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 11 of the '421 Patent. Claim 11 is the independent system counterpart to claim 1, and it also corresponds to claim 10 of the '757 Patent. I incorporate the Rauner-Azmoodeh combination rationale discussed above. *See* Sections [IX.C.1-3] and [X.D.1-2].

636. I have compared claim 11 of the '421 Patent and claim 10 of the '757 Patent and claim 11 of the '421 Patent to claim 1 of the '421 Patent limitation by limitation. They recite the substantively similar limitations, with the sole difference that '757 claim 10 recites "at least one supervisor data associated with a supervisee" in limitation 10[a][3] where '421 claim 11 recites "at least one supervisee data associated with a supervisee" in limitation 11[a][3]. In my opinion that difference does not affect my analysis because the antecedent basis in the remainder of the claim shows that the recitation refers to the supervisee data of limitation 1[e], and the '421 wording simply states expressly what the '757 wording conveys by antecedent.

637. Because claim 11 is an apparatus claim, the § 112(f) constructions Applicant conceded during prosecution for the "communication device," "processing device," and "storage device" apply. As I explained in the introduction to this ground and in subsection 1, those constructions come from the '421

prosecution record, and the Rauner components I identified for claim 1 above are the corresponding structures and they perform the same functions.

638. For the reasons stated in my Ground 3 analysis of ’757 claim 10 and my Ground 4 analysis of ’421 claim 1, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 11 of the ’421 Patent.

11. Claim 12

639. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 12 of the ’421 Patent. Claim 12 is the system counterpart to claim 2 and corresponds to claim 11 of the ’757 Patent. I have compared these claims limitation by limitation. They are substantively similar. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 11 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above and the ’421 Patent claim 2 analysis in Ground 4, which I incorporate here.

640. For the reasons stated in my analyses of ’757 claim 11 and ’421 claim 2, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 12 of the ’421 Patent.

12. Claim 13

641. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 13 of the ’421 Patent. Claim 13 is the system counterpart to claim 3 and corresponds to claim 12 of the ’757 Patent. I have compared these claims limitation by limitation. They are substantively similar. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 3 and claim 12 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here.

642. For the reasons stated in my analysis of ’421 Patent claim 3 and ’757 claim 12, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 13 of the ’421 Patent.

13. Claim 14

643. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 14 of the ’421 Patent. Claim 14 is the system counterpart to claim 4 and corresponds to claim 13 of the ’757 Patent. I have compared these claims limitation by limitation. They are substantively similar. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 4 of the ’421 Patent and claim 13 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here.

644. For the reasons stated in my analysis of ’421 claim 4 and ’757 claim 13, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 14 of the ’421 Patent.

14. Claim 16

645. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 16 of the ’421 Patent. Claim 16 is the system counterpart to claim 6 and corresponds to claim 15 of the ’757 Patent. I have compared these claims limitation by limitation. They are substantively similar. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 6 of the ’421 and claim 15 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here.

646. For the reasons stated in my analyses of ’241 claim 6 and ’757 claim 15, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 16 of the ’421 Patent.

15. Claim 17

647. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 17 of the ’421 Patent. Claim 17 is the system counterpart to claim 7 and corresponds to claim 16 of the ’757 Patent. I have compared these claims limitation by limitation. They are substantively similar. Limitation 17[a] corresponds to claim 7[a] and to ’757 claim 16[a]. Limitation 17[b]

RAVE/MSI, EX1005, p. 350

corresponds to claim 7[b] and to ’757 claim 16[b]. Limitation 17[c] corresponds to claim 7[c] and to ’757 claim 16[c]. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 7 of the ’421 Patent and claim 16 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here.

648. For the reasons stated in my analyses of ’421 Patent claim 7 and ’757 claim 16, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 17 of the ’421 Patent.

16. Claim 18

649. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 18 of the ’421 Patent. Claim 18 is the system counterpart to claim 8 and corresponds to claim 17 of the ’757 Patent. I have compared these claims limitation by limitation. They are substantively similar. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 8 and claim 17 of the ’757 Patent in my Ground 3 analysis in Section [IX.C] above, which I incorporate here.

650. For the reasons stated in my analyses of ’421 claim 8 and ’757 claim 17, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 18 of the ’421 Patent.

RAVE/MSI, EX1005, p. 351

17. Claim 19

651. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 19 of the '421 Patent.

a. ***19[a]: The system of claim 18, wherein: the at least one signal made by the supervisee comprises shaking the supervisee device abruptly, pressing a button, or speaking a specific phrase, wherein: the at least one sensor is configured for detecting the at least one signal,***

652. For limitation 19[a], as discussed in my '421 Patent Ground 4 claim 8 analysis, Rauner's input device 132 includes a microphone that the user can use to "record the emergency trigger message using input device 132." Ex.1009 ¶[0105]. The recorded utterance is a signal the supervisee makes by speaking a phrase. Additionally, the user initiates an Emergency Communication Event by pushing a panic button, thereby disclosing "pressing a button." Ex.1009, ¶¶[0061], [0110].

653. The spoken phrase is a specific one because Rauner's analyzing module 163 "is configured to analyze two or more emergency trigger messages to determine if the emergency trigger messages contain one or more predetermined trigger words," and that those "predetermined trigger words can be word or phrases that indicate that a high-risk emergency is occurring or has occurred." *Id.* ¶[0076]. Rauner enumerates them, listing among others "homicide, murder, slaughter, rape, assault, arson, fire, weapon, gun, shoot, shooting, rifle, pistol, kill, handgun, bomb, explosion, gas, flood, earthquake." *Id.* Rauner then applies that vocabulary to the

spoken recording directly, stating that where "the emergency trigger message can be a sound recording," analyzing module 163 "can automatically transcribe the telephone call into text and determine if the telephone call included any of the predetermined trigger words." *Id.* ¶[0077].

654. Limitation 19[a] also requires that the sensor be configured for detecting that signal, and it is. The microphone and button are components of input device 132 through which Rauner's remote computing device detects the input. *Id.* ¶[0105]. Rauner confirms that the captured recording travels onward as the operative message, stating that "receiving the two or more emergency trigger messages further can include receiving an audio recording," that "the audio recording can be a recording made by a user of a remote computing device," and that "a device communications module can convert the audio recording into text." Ex.1009 ¶[0113]. Server-side transcription of the captured audio confirms that the microphone's output is what the system detects and processes. Similarly, the panic button is configured for detecting the pressing signal because upon being activated an emergency message is generated and sent.

b. ***19[b]: and the supervisee device is configured to optionally make an emergency call when the at least one sensor detects the at least one signal;***

655. For limitation 19[b], the supervisee device is configured to optionally make an emergency call when the sensor detects the signal. Rauner's remote

computing device presents emergency numbers as dialing controls on its own interface, stating that "[n]umbers are displayed as buttons on mobile device emergency call screen 120" and that "[u]sing buttons on the emergency call screen initiates an autodial for the emergency number selected." *Id.* ¶[0225]. The device is therefore configured to place an emergency call. The call is optional in the sense the claim requires because the autodial occurs only if the supervisee selects the presented number, so the emergency report and the emergency call are separate and independently available actions that the device is configured for.

c. 19[c]: wherein a phone number dialed in the emergency call is determined based on the geofence.

656. For limitation 19[c], the phone number dialed in the emergency call is determined based on the geofence. Rauner discloses this and states that "the System allows definition of a geographic area to be associated with a telephone number to display the number on the user's emergency call interface when the user's location is within the area defined for the number," and gives the worked example that "a City defines the service area for a local poison control call center as a geofence in the system Community," after which "[a]s a user enters the service area for the local poison control call center, the local poison control telephone number appears as a button on the emergency call interface." *Id.* ¶[0228]. The geofence is the data structure that determines which number is presented, and limitation 19[b] establishes that pressing the presented button autodials that number. *Id.* ¶[0225].

657. Rauner discloses the same geofence-driven selection for the proper emergency numbers. It states that "the system maintains local emergency calling numbers for every country in the world," that in the United States "the numbers 116a for emergency calling for Fire Service, Ambulance, and Police are all 911," and that upon the device's arrival in Egypt "[t]he system updates the emergency calling numbers on the emergency call screen to '180', '123', and '122.'" *Id.* ¶[0226]. Rauner further discloses sub-national selection, stating that the system "can also use defined geographic reference locations for increased granularity below the national level to provide local numbers," *id.*, and that it "uses geographic definition of areas where no national number is available to populate alternative numbers to the emergency call screen," including "local ten digit numbers" for an area of rural Missouri "without 911 service." *Id.* ¶[0227]. Rauner also discloses ordering numbers by the user's position relative to multiple defined areas, describing entities whose Communities have "concentric overlapping geofences that define their respective geographic boundaries" and stating that the resulting buttons "appear in order of proximity by comparing the current location of the user and the locations associated with each of the motorist assistance numbers." *Id.* ¶[0229]. In each of these disclosures the dialed number is determined by comparing the supervisee's position to a defined geographic area, which is the determination limitation 19[c] recites.

658. Accordingly, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 19 of the '421 Patent.

18. Claim 20

659. In my opinion, Rauner in view of Azmoodeh discloses or renders obvious every limitation of claim 20 of the '421 Patent.

a. ***20[a]: The system of claim 11, wherein the supervisee is associated with at least one identification,***

660. For limitation 20[a], the identification is the unique user ID carried in the stored user profile, for the reasons I gave for limitation 10[a]. Ex.1009 ¶¶[0050], [0037].

b. ***20[b]: wherein the communication device is further configured for receiving at least one indication corresponding to the at least one identification from the at least one supervisee device,***

661. For limitation 20[b], the communication device is configured for receiving the corresponding indication because device communications module 151 receives the emergency trigger message and location information sent from the supervisee's own device by emergency sending module 111, and the system associates the caller's stored emergency information profile with the resulting event, as explained for claim 10[b]. *Id.* ¶¶[0111], [0110].

c. ***20[c]: wherein the processing device is further configured for identifying the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying.***

662. For limitation 20[c], which corresponds to 10[c], the processing device is configured for identifying the supervisee from that indication because processing module 1652 and determination module 1666 run on processing unit 161 and process the incoming message and location, and because the resulting notice message carries the resolved "unique user ID" and "user name from profile" as its output. *Id.* ¶¶[0167]-[0168], [0050]. The notification being based on the identifying is disclosed because that notice message is composed of the identified user's stored data before it is transmitted to the system administrator contact, and because Rauner's reports carry the identified user's name and phone number. *Id.* ¶[0050]; Ex.1009, claim 6. Because Rauner's system performs each of these functions, its communication device and processing device are configured for them.

663. Accordingly, it is my opinion that Rauner in view of Azmoodeh discloses or renders obvious each limitation of claim 20 of the '421 Patent for the reasons above and those provided for claim 10[c].

19. Claim 21

664. In my opinion, Rauner in view of Azmoodeh renders obvious every limitation of claim 21 of the '421 Patent.

RAVE/MSI, EX1005, p. 357

a. ***21[a]: The system of claim 11, wherein each geofence grid box is further characterized by: a) storing at least one emergency contact number associated with the geographical area represented by the grid box geofence area;***

665. For limitation 21[a], the system stores an emergency contact number associated with the geographical area represented by the subdivision. Rauner stores emergency contacts against defined geographic areas as a matter of its ordinary operation. It recites "storing in a database of the emergency response computer system a plurality of geographic areas and a plurality of emergency groups having responsibility for the geographic areas." Ex.1009, claim 16. It states that "information can be stored in storage device 162 that identifies the appropriate first and second level response units to notify if an emergency occurs at a specific location," and that response module 154 accesses that stored information to select the units for the event. Ex.1009 ¶[0136]. At the level of individual telephone numbers, Rauner describes a City that "enables a telephone number for the local poison control call center on the system" after defining that center's service area "as a geofence in the system Community." *Id.* ¶[0228]. The stored association is therefore between a telephone number and a defined geographic area.

666. The association operates at the level of the subdivision because Azmoodeh's cells are the defined portions of the fenced area in the combined system. Azmoodeh states that its cells each represent "portions (in some instances

the portions are equal) of the physical location within the geo-fenced area," and that "the set of cells sum to make up the whole physical location encompassed by the geo-fence." Ex.1010 ¶[0022]. Each cell is accordingly a defined geographical area to which Rauner's stored number can be keyed, and that is the combined system's level of geographic resolution or subdivision.

667. . Rauner further refines emergency-number selection below the level of the national or regional area, stating that the system "can also use defined geographic reference locations for increased granularity below the national level to provide local numbers and to corroborate national identification," (*id.* ¶[0226]), and that it "uses geographic definition of areas where no national number is available to populate alternative numbers to the emergency call screen." *Id*. ¶[0227]. Rauner thus treats sub-area granularity as the means of reaching the correct local number. A single Rauner geofence, however, can span more than one answering jurisdiction, as Rauner itself illustrates in describing "three police municipalities 1822a, 1822b, 1822c within a single fire protection district 1820," each municipality having "their own law enforcement services." *Id.* ¶[0176]. Holding one number for the whole fenced area could therefore misroute an event occurring in the portion of the area outside that number's jurisdiction, whereas holding it per cell routes each event to the service that answers for the cell in which the event occurred. A POSITA would have had a reasonable expectation of success because the combined system stores

an additional field on a data structure the combined system already maintains per cell, and supplies that field to a location-driven selection step Rauner already performs. *Id.* ¶[0136].

b. ***21[b]: b) wherein the emergency contact number includes a 911 service or equivalent emergency service specific to then geographical area of the grid box; and***

668. For limitation 21[b], the stored number includes a 911 service or an equivalent emergency service specific to the area. Rauner states that "the system maintains local emergency calling numbers for every country in the world," and that in the United States the device is populated with "911" for Fire Service, Ambulance, and Police. *Id.* ¶[0226]. It discloses the equivalent-service alternative in the same passage, stating that upon the device's arrival in Egypt the system updates those numbers to "180," "123," and "122." *Id.* Rauner discloses the sub-national equivalent as well, describing an area of rural Missouri "without 911 service" in which "the numbers for Fire Service, Fire Service [*sic*] and Police are limited to local ten digit numbers." *Id.* ¶[0227]. The number is specific to the area because Rauner selects it by comparing the device's position to the defined area, which is the same operation the Rauner-Azmoodeh system performs at cell granularity in the combination. *Id.* ¶[0226]; Ex.1010 ¶[0047].

c. ***21[c]: c) wherein the processing device is configured to automatically select and transmit supervisee data to the stored emergency contact number upon detecting an emergency situation within the corresponding grid box geofence area.***

669. For limitation 21[c], the processing device is configured to automatically select and transmit supervisee data to the stored number upon detecting an emergency situation within the corresponding subdivision. Rauner performs the selection from the event's location: determination module 1666 is "configured to use the location of the remote computing device sending the emergency trigger message to determine an appropriate emergency response unit to notify," and notification module 1655 "can forward the emergency trigger message and the location information to the appropriate emergency response unit." Ex.1009 ¶¶[0167], [0168]. The data so forwarded is supervisee data, because the notice Rauner composes carries the supervisee's "unique user ID, user name from profile, user location, time, date." *Id.* ¶[0050].

670. The selection and transmission are automatic, and Rauner draws that distinction itself. It states that its automatic notification "differs from prior art PSAP systems and other emergency response systems which require the emergency information to be first routed to a human dispatcher before the information is made available to the emergency responders," and that under its own approach "the emergency system's computer processor performs the analyses to determine the

appropriate types of emergency response groups and also determine the appropriate emergency response unit that should be notified about the emergency with the corresponding location of the mobile computing device that sent the emergency request." *Id.* ¶[0169].

671. The emergency is detected within the corresponding subdivision because Azmoodeh localizes events to the cell. Azmoodeh states that the collected usage data "may include corresponding geo-location data indicating a cell from among the set of cells in which the usage data originated (*i.e.*, indicating a location of a device within the geo-fenced area)." Ex.1010 ¶[0047]. In the combined system the event's reported position resolves to a cell, and the number stored for that cell is the number to which the supervisee data is sent. A POSITA would have expected success because this uses the location-driven selection Rauner already performs and the cell-level localization Azmoodeh already supplies, with no change to either operation.

672. Accordingly, it is my opinion that Rauner in view of Azmoodeh renders obvious each limitation of claim 21 of the '421 Patent.

E. Ground 5: Claims 5, 15, and 22-24 of the '421 Patent Are Rendered Obvious By Rauner (Ex.1009) In View Of Azmoodeh (Ex.1010) And Further In View Of Noland (Ex.1008) + Knowledge Of A POSITA

673. Claim 5 depends from claim 1 and claim 15 depends from claim 11. I explained in Ground 4 why Rauner in view of Azmoodeh discloses or renders

obvious claims 1 and 11, and I incorporate that analysis here. Claim 22 is a separate independent method claim, and claims 23 and 24 depend from it. For the additional limitations of all five claims, I rely on the Rauner-Azmoodeh combination further in view of Noland, because Noland supplies the weapon-identification and threat-assessment functions and the distributed-sensor functions.

1. A POSITA would have combined the Rauner-Azmoodeh system with Noland

674. I set out the rationale for adding Noland to the already-combined Rauner-Azmoodeh system in my ’757 Ground 4 analysis in Section [IX.D.1] above, and I incorporate it here in full. That analysis establishes that Noland is analogous art, both because all three references are in the same field of endeavor as the Asserted Patents, facilitating supervision of individuals based on geofencing, and because Noland is reasonably pertinent to the problem addressed by the inventor of the ’421 patent; that Rauner itself invites the addition, because Rauner states that its geofence-based distribution model may be used to integrate external sensors, systems, and resources into its emergency work-flow, names gunshot detection specifically among the external sources that may serve as trigger events, and supplies a worked example in which a gunshot detection system indicates a firearm discharge at a location that is then distributed by cross-referencing the event location against stakeholder-defined geographic areas; that Rauner nevertheless names that capability only generally, as a category of external trigger source, and Noland

improves on that generalized reference by supplying the specific acoustic and image classification logic that resolves a detection into weapon type, caliber, attachments, shot count, and shooter location; that Noland's statement of the operational benefit of weapon classification supplies the motivation rather than hindsight; and that a POSITA would have expected success because Rauner's existing event-processing pipeline already compares georeferenced event location information against the locations of available sensors and distributes the resulting data according to an administrator-defined distribution list, so integrating Noland requires only directing its output into a pipeline that already exists, and because Noland's system gateway 110 and Rauner's processing unit 161 are both server-side processors that receive, analyze, and act on incoming sensor data, so Noland's structured georeferenced event output is the same kind of data Rauner's pipeline already consumes. Ex.1009 ¶¶[0211]-[0214], [0216], [0223]; Ex.1008 ¶¶[0096], [0100], [0107]-[0108], [0111], [0127], [0129], [0156]. I do not repeat that analysis here, and nothing in this section modifies it.

675. The analogous-art analysis applies to the '421 Patent for the same reason it applies to the '757 Patent, because the '421 Patent carries largely the same specification. The field and problem analyses rest on Rauner's and Noland's own subject matter and on the specification of the'421 Patent, so my conclusion that Noland is analogous art is the same for the '421 claims.

RAVE/MSI, EX1005, p. 364

676. One point requires statement in the ’421 context, because claims 22 through 24 recite subject matter with no direct counterpart in the ’757 Patent. Those claims require audio and video recordings, selection of a sensor from among nearby sensors by proximity, sensor-to-sensor tracking of the supervisee, and role-differentiated recipient groups. In my opinion a POSITA would have been motivated to add Noland’s distributed sensor network to the Rauner-Azmoodeh system for those functions. Rauner’s own sensor and camera architecture is geographically distributed and already selected by position: Rauner correlates video cameras to footprint view locations within a geographic area and determines the subset of cameras whose footprints are proximate to the reported mobile-device locations, and it cross-references the location of an emergency event against the geofences defining each camera’s viewing area in order to select the appropriate feed for distribution. Ex.1009, claims 15, 16, ¶[0211]. Noland’s threat sensing devices are deployed on the same pattern, distributed room by room through a facility with each unit’s installed location recorded, and Noland supplies the selection and hand-off logic that resolves an event to the nearest unit and follows a person from one unit’s coverage to the next. Ex.1008 ¶¶[0091], [0113], [0111], [0124]. Adding Noland’s network therefore supplies facility-level granularity to a system already built to select among position-referenced sensors, which is the granularity Rauner’s emergency-response

RAVE/MSI, EX1005, p. 365

objectives call for and which Rauner's existing distribution model can consume without redesign.

677. I note that the reasonable expectation of success I incorporate from the '757 analysis rests in part on Noland's weapon-identification output, which is the function the '757 Ground 4 claims required. It applies equally to the sensor functions at issue in '421 claims 22 through 24, because the data path is the same one: Noland's sensors report to its system gateway, and the gateway's georeferenced output enters Rauner's event-processing pipeline through the same interface. Ex.1008 ¶[0091]; Ex.1009 ¶[0212].

2. Claim 5

678. In my opinion the Rauner-Azmoodeh combination in view of Noland renders obvious every limitation of claim 5 of the '421 Patent. Claim 5 depends from claim 1 and corresponds to claim 5 of the '757 Patent. I have compared these claims limitation by limitation. They are substantively similar in wording. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 5 of the '757 Patent in my Ground 4 analysis in Section [IX.D] above, which I incorporate here.

3. Claim 15

679. In my opinion the Rauner-Azmoodeh combination in view of Noland renders obvious every limitation of claim 15 of the '421 Patent. Claim 15 is the

system counterpart to claim 5 and corresponds to claim 14 of the ’757 Patent. I have compared these claims limitation by limitation. They are substantively similar. Therefore, I reach that conclusion for the same reasons, and on the same disclosures, that I set out for claim 14 of the ’757 Patent in my Ground 4 analysis in Section [IX.D] above, which I incorporate here.

680. In the combined system the processing device includes Rauner’s processing unit 161 with Noland’s system gateway 110 integrated into its processing modules, and because that integrated server-side processing performs the weapon identification, the lethality assessment, and the generation of the resulting notification, the claim 11 processing device is configured for those functions.

681. For the reasons stated in my analysis of ’757 claim 14, which I incorporate here, it is my opinion that Rauner in view of Azmoodeh and further in view of Noland renders obvious each limitation of claim 15 of the ’421 Patent.

4. Claim 22

682. In my opinion the Rauner-Azmoodeh combination in view of Noland renders obvious every limitation of claim 22 of the ’421 Patent.

683. Limitations 22[pre] through 22[h] recite the same method steps I addressed for limitations 1[pre] through 1[i] of claim 1, with two exceptions: claim 22 omits the step of generating a geofence, and limitation 22[e] analyzes the supervisee data “based on the geographical location” rather than based on the

RAVE/MSI, EX1005, p. 367

geofence. For the steps common to both claims I apply the Ground 4 claim 1 mappings and incorporate that analysis here.

684. The wording difference in limitation 22[e] does not change the result, and the same Rauner disclosures satisfy both recitations. Rauner's processing device analyzes the reported locations of the supervisee devices against the geographic area the administrator selected: mapping module 158 calculates the coordinate range for the space inside the selected map feature and associates that range with the feature, and determination module 156 uses the stored location information of the remote computing devices to determine which of them fall within a given distance of the event. Ex.1009 ¶[0094], [0139]. That evaluation is an analysis of supervisee data based on the geographical location received from the supervisor device in limitation 22[b], and it is the same operation I relied on for limitation 1[f], where the geofence is the representation Rauner derives from that same selected area. Claim 22 recites no geofence, so limitation 22[e] does not require the analysis to be derived from a generated boundary. Accordingly, limitations 22[pre] through 22[h] are met for the reasons I gave for limitations 1[pre] through 1[i].

685. Limitations 22[i] through 22[k] recite the same three sensor requirements as limitations 8[a] through 8[c]. I apply the mapping I set out for claim 8 in Ground 4, which I incorporate here. Ex.1009 ¶[0061], [0180].

RAVE/MSI, EX1005, p. 368

a. ***22[l]: wherein the supervisee data comprises audio and video recordings;***

686. For limitation 22[l], the supervisee data comprises audio and video recordings. Noland's image-based sensors comprise a built-in communication module configured to transmit live video and audio to the system gateway 110 for storage or dissemination, and Noland confirms that the captured image and acoustic data is transmitted to and stored in a physical computer-readable storage medium, which is what makes the two modalities recordings. Ex.1008 ¶[0126], [0130]. Rauner independently supplies each modality within its own architecture, because the emergency trigger message may be a sound recording the user records through input device 132, and because Rauner correlates video cameras to footprint view locations and relays their live feeds to the responding units. Ex.1009 ¶[0180], claims 15, 16. In my opinion a POSITA would have combined Noland's audio-and-video sensor feeds with Rauner's supervision architecture because Rauner already ingests third-party sensor and camera feeds keyed to the event location and already stores and distributes them with the event, so Noland's combined feed enters an existing ingress and storage path rather than requiring a new one. Ex.1009 ¶[0212], [0134].

b. ***22[m]: wherein the at least one sensor is selected from one or more nearby sensors based on the most proximal nearby sensor by geographical location in real-time; and***

687. For limitation 22[m], the sensor is selected from one or more nearby sensors based on the most proximal nearby sensor by geographical location in real time. Rauner performs proximity-based selection among a population of position-referenced sensors as a matter of its ordinary operation, but it does not expressly state it does so in real-time. Rauner correlates in its database a set of video cameras according to their footprint view locations within the geographic area and determines in the processor the subset of those cameras whose footprint view locations are proximate to the reported mobile computing device locations, and it separately recites determining at least one camera with a footprint field of view proximate to the reported device location. Ex.1009, claims 15, 16. Rauner describes the same operation in its specification, selecting the appropriate camera feed by cross-referencing the location of the emergency event against the geofences that define each available camera's viewing area. *Id.* ¶[0211]. Noland resolves the event to the closest unit from the arriving sensor reports themselves in real-time, stating that the sound waveform determined to have the greatest amplitude is the threat sensing device closest to the gunshot and that the system gateway 110 correlates the known location of that closest device, and that the gateway can use the highest-rating reporting sensor device to determine the location of the shooter. Ex.1008 ¶[0111],

[0205]. Noland performs that resolution as the event unfolds, in real-time, because its gateway has an internal clock and emits multiple pulses per second to receive information sequentially from each connected threat sensing device, using the resulting time stamps and times of arrival to fix the event location. *Id.* ¶[0145]. Each candidate sensor's geographical location is already known to the system, because the geometry and location of each room in which a device is installed is entered into the system along with the device's location, height, and orientation, and each device carries a unique hardware address recognized by the gateway. *Id.* ¶[0113], [0095]. In my opinion a POSITA would have applied Noland's nearest-sensor logic to the Rauner-Azmoodeh system because Rauner already maintains stored positions for its distributed sensors and cameras and already selects among them by comparing those positions to the event location, so Noland's contribution is the criterion by which the comparison resolves to the single nearest unit as the reports arrive in real-time.

c. 22[n]: wherein the at least one sensor tracks the supervisee as the supervisee moves between the one or more nearby sensors.

688. For limitation 22[n], the sensor tracks the supervisee as the supervisee moves between the nearby sensors. Noland's sensors hand tracking off from one unit to the next. Noland states that the images its image-based sensors record enable facial recognition software and hardware to operate and to track within a room and from room to room, and that after facial identification images have been obtained by

one threat sensing device the system can report facial recognition information to the other threat sensing devices located throughout the facility in order to track more quickly and accurately. Ex.1008 ¶[0116], [0124]. Noland also discloses a time-based algorithm that distinguishes one individual moving between rooms from two individuals in separate rooms. *Id.* ¶[0229]. Rauner supplies complementary device-side tracking of the same individual across monitored areas. Rauner simultaneously tracks mobile devices into a mapping tool to provide a real-time depiction of location, movement, and relative position, with the map updating and the pin drops moving to track participants' movements. Ex.1009 ¶[0248]. Its dynamic tracking maintains a current location for all selected users and shortens the update interval when a user moves more quickly. *Id.* ¶[0249]. Rauner also discloses hand-off between adjacent defined areas, removing a user from one geographically defined Community and adding that user to the adjacent one as the user crosses the boundary. *Id.* ¶¶[0233]-[0234].

689. Noland's tracking disclosures describe tracking individuals between sensors. In my opinion a POSITA would understand this to be applicable to tracking any individual, including "the supervisee." The technique is indifferent to the role of the person tracked: facial recognition applied to captured images, reported from one device to the others and resolved by a time-based algorithm, operates on whatever face the sensors capture. Ex.1008 ¶[0116], [0124], [0229]. Noland

disclosing pre-programming the sensors to look for a particular person of interest even in the absence of any threat, with the example of a suspended student whose images are added to an alert database so the system can report the student's unexpected arrival and point of entry, and disclosing the use of its geo-fence and near field sensors to monitor the arrival and departure of identified device owners from the fenced area. *Id.* ¶[0125], [0148]. The supervisee in the combined system is the person carrying the Rauner remote computing device the system is deployed to monitor, and Rauner already reports that person's position continuously to the backend, so the person the combined system tracks is the supervisee. Ex.1009 ¶[0248]. For these reasons a POSITA would have understood Noland's sensor-to-sensor tracking to track the supervisee, and would have had a reasonable expectation of success in applying it to the monitored individual, because doing so requires no change to the technique. Ex.1008 ¶[0125].

690. Limitation 22[i] requires that the supervisee device comprise at least one sensor. Limitations 22[m] and 22[n] then recite selection among nearby sensors by proximity and tracking between those sensors. In my opinion the claim does not require that the sensor selected by proximity in 22[m] be the same sensor recited in 22[i]: 22[m] and 22[n] speak to the sensor population from which the system draws and through which it follows the supervisee, and in the combined system that population comprises Rauner's position-referenced cameras and Noland's

distributed threat sensing devices alongside the supervisee device's own microphone. Ex.1009, claim 15; Ex.1008 ¶[0091]. Even where every one of limitations 22[i] through 22[n] refers to a single sensor, the distributed threat sensing devices supply that sensor, reporting through the supervisee device for the reasons I gave in addressing the corresponding limitation in my Ground 2 analysis, and the conclusion is the same under either reading.

691. Accordingly, it is my opinion that Rauner in view of Azmoodeh and further in view of Noland renders obvious each limitation of claim 22 of the '421 Patent.

5. Claim 23

692. In my opinion the Rauner-Azmoodeh combination in view of Noland renders obvious every limitation of claim 23 of the '421 Patent.

a. ***23[a]: The method of claim 22, wherein: the supervision notification is sent to a first distinct group of one or more supervisor devices correlated with the geographical location;***

693. For limitation 23[a], the notification is sent to a first distinct group of supervisor devices correlated with the geographical location. Rauner determines the recipient group from the event's location and notifies it. Rauner states that information can be stored in storage device 162 identifying the appropriate first and second level response units to notify if an emergency occurs at a specific location, that response module 154 accesses that stored information to determine the

appropriate units, and that device communications module 151 then notifies those units. Ex.1009 ¶[0136], [0137]. The resulting recipient set is a distinct group of devices, and it is correlated with the geographical location because Rauner builds the association between locations and response units from the administrator's own mapped areas: a user loads the association information into the system and association module 1667 creates associations between various locations and various emergency response units, using a visual mapping tool to load the association data. *Id.* ¶[0177]. Rauner illustrates the resulting correlation with overlapping geofences that deliver an emergency event to one or more agencies based on the location of the mobile device, describing three police municipalities 1822a, 1822b, and 1822c within a single fire protection district 1820, each municipality having its own law enforcement services. *Id.* ¶[0176]. The group notified is therefore the group whose stored area encompasses the location of the event.

b. ***23[b]: the first distinct group of one or more supervisor devices is comprised of nearby first responders and dispatchers; and***

694. For limitation 23[b], the first distinct group comprises nearby first responders and dispatchers. Rauner identifies both categories as recipients. Its first and second level response units are the units responsible for responding to an emergency in the geographic area, whether associated with a city, county, state, another political subdivision, a university or college, or a business. Ex.1009 ¶[0165].

Rauner's architecture is accessed by PSAP computers, and Rauner describes the emergency work-flow as placing the caller together with the dispatcher and the responders into a group messaging session in which each participant sees the shared communications, so that the reporting individual can dialogue with the emergency dispatcher and the emergency responders. *Id.* ¶[0110]. Those recipients are nearby in the sense the claim requires because Rauner selects and displays them by proximity to the event: it cross-references capabilities and location to search for the nearest desired asset, and highlights the pin drops showing the locations of the qualifying officers in proximity to the location of the Emergency Call event. *Id.* ¶[0251]. Rauner's automatic notification is directed to the units associated with the emergency location rather than to a general roster. *Id.* ¶[0136].

c. ***23[c]: the supervision notification may be sent to a second distinct group of one or more supervisor devices based on the location and expertise of the second distinct group.***

695. For limitation 23[c], the notification may be sent to a second distinct group of supervisor devices based on the location and expertise of that group. The claim recites this permissively, so the system need only be capable of the second transmission. Rauner discloses that capability expressly, and it selects the second group on both of the recited bases. Rauner states that the system combines the capability to auto-generate participants based on location, capabilities, and role, and automatically initiates communications in response to a trigger event; in its worked

example, an Emergency Call event indicates that the caller's primary language is Spanish, and the system builds a recipient list of law enforcement first responders with Spanish language proficiency and automatically sends them a multimodal communication requesting participation. Ex.1009 ¶[0252]. Rauner selects those officers by position as well as capability, filtering for the qualifying responders in proximity to the location of the Emergency Call event. *Id.* ¶[0251]. In my opinion that recipient list is a second distinct group within the meaning of the limitation because it is built separately from the location-correlated group of limitation 23[a] by applying an added capability filter to the population, and the two selection criteria Rauner applies to it, proximity and language proficiency, are the location and expertise the claim recites. Rauner separately discloses a distinct second tier of recipients defined by role rather than by proximity alone, comprising its second level response units. *Id.* ¶[0165].

696. Accordingly, it is my opinion that Rauner in view of Azmoodeh and further in view of Noland renders obvious each limitation of claim 23 of the '421 Patent.

6. Claim 24: The method of claim 22, wherein: wherein the supervisee is associated with at least one identification, wherein the communication device is further configured for receiving at least one indication corresponding to the at least one identification from the at least one supervisee device, wherein the processing device is further configured for identifying the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying.

697. In my opinion the Rauner-Azmoodeh combination in view of Noland renders obvious every limitation of claim 24 of the '421 Patent.

698. Claim 24[a]-[c] are the same three requirements recited in claim 10[a]-[c], which I addressed in my Ground 4 analysis above, which I incorporate here. Ex.1009 ¶[0050], [0037], [0111], [0110].

699. Claim 24 depends from claim 22, therefore the reasons I gave for claim 22 are also incorporated here. The added identification limitations themselves rest on the Rauner disclosures I identified for claim 10 which I incorporate here as well.

700. Accordingly, it is my opinion that Rauner in view of Azmoodeh and further in view of Noland renders obvious each limitation of claim 24 of the '421 Patent.

F. Ground 6: Claim 9 of the '421 Patent Is Rendered Obvious By Rauner (Ex.1009) In View Of Azmoodeh (Ex.1010) And Further In View Of Smith (Ex.1011) + Knowledge Of A POSITA

701. Claim 9 depends from claim 1. I explained in Ground 4 why Rauner in view of Azmoodeh discloses or renders obvious claim 1, and I incorporate that

analysis here. For claim 9, I rely on the Rauner-Azmoodeh combination further in view of Smith.

1. A POSITA would have combined the Rauner-Azmoodeh system with Smith

702. All three references are directed to the same field of endeavor as the '421 Patent: facilitating supervision of individuals based on geofencing. Ex.1003, 1:7-18. They are also reasonably pertinent to the problem the named inventor addressed. Rauner in combination with Azmoodeh monitors individuals within geofenced areas subdivided into cells and coordinates emergency response, for the reasons I set out in Ground 4. Smith is in that same field, and specifically concerns three-dimensional, altitude-based geofencing. Smith defines virtual boundaries in a geographical space and triggers actions based on the position of a tracked device relative to those boundaries, stating that it provides "a method of three-dimensional geofencing" in which "[a] boundary-related event and an action to be triggered based on the position of a trackable object is defined with respect to the virtual boundary." Ex.1011, Abstract. In my opinion, the fact that Smith's geofences add a vertical dimension does not place Smith in a different field of endeavor; it is the same geofence-based supervision technology applied in three dimensions rather than two.

703. A POSITA would have been motivated to incorporate Smith's altitude-based boundary definition into the Rauner-Azmoodeh system, and Rauner's own disclosures identify the gap. Rauner already operates in multi-story environments

and already treats the floor as a unit of interest: its mapping module 158 allows "[s]elected areas of the target geographic area (*e.g.*, selected buildings, floors, parks, zones, etc.)" to be selected through the administrative interface, Ex.1009 ¶[0093], and Rauner describes the selectable subset of a target geographic area as including "a select number of floors of an office building." *Id*. ¶[0140]. Rauner also already carries position in three dimensions into its emergency-response output, because structure module 1657 overlays a building's three-dimensional schematic "with locations of individuals plotted into the schematic using the appropriate X, Y, and Z axis information." *Id.* ¶[0198]. What Rauner does not disclose is how that vertical value is derived or how a boundary is defined in the vertical dimension, and that is what Smith supplies. Smith identifies the two-dimensional character of prior geofencing as a specific technical shortcoming, stating that "prior art geofencing techniques are generally two-dimensional (*i.e.*, are defined within a planar map) and thus do not comprehend an altitude, height, or 'z-axis' attribute," with the consequence that such systems "are not able to determine whether a user has changed floors within a home." Ex.1011, 1:27-36. Smith states the emergency-response benefit directly, disclosing that "first responders may use altitude data to determine which floor (*e.g.*, 981 or 982) the user is on during an emergency situation, such as during a fire." *Id.,* 5:62-65. That is the same purpose Rauner's system serves, because Rauner's structure module exists to tell responders where within a structure

the monitored individuals are. Ex.1009 ¶¶[0174], [0198]. In my opinion a POSITA would therefore have recognized that supplying the vertical boundary input Smith describes would complete a capability Rauner already reaches toward, and would do so because Rauner already selects floors as areas of interest and already plots a Z value, so without a vertical boundary definition the system can display a device's elevation but without a technique for testing it against a supervisor-defined limit.

704. A POSITA would also have had a reasonable expectation of success. Rauner already plots mobile-device location data in three dimensions, so the combination does not require the system to acquire any new category of position data. *Id.* ¶[0198]. Azmoodeh's geo-location data likewise already includes the vertical coordinate, because Azmoodeh states that "[t]he geo-location data may include a set of coordinates that define a point (*e.g.*, longitude, latitude, and altitude)." Ex.1010 ¶[0018]. Azmoodeh further states that its own subdivision technique is not limited to the plane, disclosing that "[a]lthough FIGS. 3, 4, 5, and 6 depict two-dimensional geo-fences, the techniques described in this specification can be applied to three-dimensional space with geo-fences defined in three dimensions (*e.g.*, different media content is available at the base of the Empire State Building than at the observation deck)." *Id.* ¶[0041]. That vertical extension is applied to the very subdivision logic on which my Ground 4 grid-box mapping rests, so the extension operates within the combination's existing framework. Smith

confirms that the necessary sensing is conventional, disclosing that the altitude value may be estimated using "an altimeter module 520, an altimeter module 521, and or an accelerometer module 522," Ex.1011, 3:58-62, and claiming estimation "via at least one of a barometer, an altimeter, and an accelerometer located within the trackable object." *Id.,* claim 13. Extending the combined system's boundary and grid definition by one axis therefore uses position data the combination already handles and sensors a POSITA would have recognized as standard, and it leaves Rauner's geofence generation, Azmoodeh's cell subdivision, and Rauner's event-processing framework otherwise intact. Adding Smith's technique of using altitude/z-axis attribute information to define a boundary in the Rauner + Azmoodeh system would therefore been within the level of skill in the art, and would require nothing more than a straightforward software implementation of Smith's disclosures.

705. Rauner's "Z axis information" is reported position data describing where a device is, used to place a plotted icon within a schematic. Ex.1009 ¶[0198]. Azmoodeh's altitude coordinate is likewise a component of the geo-location data the system receives and stores. Ex.1010 ¶[0018]. Smith's altitude parameter, by contrast, is an input the supervisor supplies in order to define the boundary itself: Smith's method recites "receiving, via the user-carried mobile device, user input defining a virtual boundary in a three-dimensional geographical space, the virtual boundary including lateral position parameters and an altitude parameter," Ex.1011,

claim 1, and Smith confirms that "[d]efining the boundary may be accomplished by a user (using an appropriate user interface)" and that "the user defines the boundary explicitly using position and range values." *Id.,* 4:63-67. I rely on Smith for limitation 9[a]. I rely on the Rauner and Azmoodeh disclosures for the reasonable expectation of success described above.

2. Claim 9

706. In my opinion the Rauner-Azmoodeh combination in view of Smith renders obvious every limitation of claim 9 of the '421 Patent.

a. ***9[a]: The method of claim 1, wherein: the at least one security parameter comprises an altitude,***

707. For limitation 9[a], the at least one security parameter comprises an altitude. The altitude is Smith's supervisor-supplied altitude parameter, which defines the boundary rather than reporting a position, for the reasons I set out in my analysis of claim 9 in Section [X.C.2] above, which I incorporate here. In the combined system the supervisor supplies that altitude through the same administrative interface through which the administrator already configures the properties I mapped as the security parameter in Ground 4, including the trigger words and thresholds the administrator designates and the map features and geographic areas the administrator selects. Ex.1009 ¶¶[0089], [0091], [0093]-[0094]. Smith's altitude parameter is a property of the same kind, supplied by the same actor through the same interface, and serving the same function of determining

what the resulting boundary covers. Adding it to that existing property set makes the security parameter comprise an altitude.

b. ***9[b]: the at least one grid parameter comprises a building floor, and***

708. For limitation 9[b], the at least one grid parameter comprises a building floor. In Ground 4 I mapped the grid parameter to the administrator-supplied input that sets the number of cells into which the fenced region is divided, which Azmoodeh makes user-configurable: "the number of cells within the region may be defined based on a size of the geo-fence, or based on user input." Ex.1010 ¶[0046]. The building floor is a different input, and in my opinion both are grid parameters in the combined system. The limitation recites that the grid parameter "comprises" a building floor, and "comprises" is open-ended: a grid parameter that includes both a horizontal cell count and a vertical floor designation satisfies a requirement that the grid parameter comprise a building floor. My Ground 4 mapping therefore applies, and claim 9 adds an additional component to the same parameter. I set out the same construction in my analysis of '421 claim 9 in Section [X.C.2] above, which I incorporate here.

709. The building floor functions as a grid parameter in this combination. Azmoodeh's cell count performs function of the grid parameter horizontally: the administrator's input sets how many cells divide the region, each cell "represent[s] portions (in some instances the portions are equal) of the physical location within

the geo-fenced area," and "the set of cells sum to make up the whole physical location encompassed by the geo-fence," so the count supplied determines both how many cells exist and how much area each one covers. Ex.1010 ¶[0022], [0046]. A floor designation performs the same function vertically. Each floor is a defined slice of the structure, the set of floors partitions the structure's vertical extent, and the number of floors the supervisor designates determines how many such slices exist and how much of the building each one spans. Smith discloses the structure so divided, describing a building that "includes multiple (*i.e.*, 3) stories, or 'floors', including a first floor, a second floor 982, and a third floor 981," and a system that determines "whether a trackable object 504 (carried by a user, not illustrated) is on the third floor 981 or 982, and act[s] accordingly." Ex.1011, 5:32-48. Smith further confirms that the floor is the frame of reference in which the supervisor sets the boundary's vertical extent, stating that "the current location of the trackable object is set as the z-distance for a boundary (*e.g.*, first floor, second floor, etc.)." *Id.,* 5:3-6.

710. In the combined system, therefore, the supervisor's input defines a grid in both dimensions: the cell count determines how finely the fenced region is subdivided in plan, and the floor designation determines how the resulting column is subdivided in elevation. Each resulting cell is a geofence grid box characterized by a grid box geofence area, consistent with limitation 1[j]. A POSITA would have

RAVE/MSI, EX1005, p. 385

expected success in making that extension because Azmoodeh's subdivision logic is already parameter-driven and already converts an administrator-supplied granularity value into a count and extent of subdivisions, Ex.1010 ¶[0046], the floor designation supplies the same kind of value along a different axis, and Azmoodeh itself states that its technique applies to "three-dimensional space with geo-fences defined in three dimensions." *Id*. ¶[0041]. Rauner's own interface already accepts floors as selectable areas, so the input requires no new configuration mechanism. Ex.1009 ¶¶[0093], [0140].

c. ***9[c]: the building floor is estimated from the altitude.***

711. For limitation 9[c], the building floor is estimated from the altitude. Smith discloses the estimation as a two-stage operation, in which available altitude information is "provided to an altitude estimation module 1002, which determines an altitude (z-value) estimate 1004," and that estimate is then supplied with the lateral position data to decision module 1005, which "determines which, if any, action 1008 should occur." Ex.1011, 4:37-50. Smith states the floor-level output of that operation in terms, disclosing that the system "might determine whether a trackable object 504 . . . is on the third floor 981 or 982, and act accordingly," and that "first responders may use altitude data to determine which floor (*e.g.*, 981 or 982) the user is on during an emergency situation." *Id.,* 5:46-48, 5:62-65. Determining which floor the user is on from the altitude estimate is the estimation

of a building floor from an altitude that limitation 9[c] recites. I set out this analysis more fully in Section [IX.C.2] above, which I incorporate here.

712. The estimated floor is resolved within the combined system's own architecture. Rauner already receives the vertical component of device position and already places the device within a structure using X, Y, and Z axis information, Ex.1009 ¶[0198], and Azmoodeh already resolves a device's reported position to the particular cell in which it sits, stating that the collected usage data "may include corresponding geo-location data indicating a cell from among the set of cells in which the usage data originated (*i.e.*, indicating a location of a device within the geo-fenced area)." Ex.1010 ¶[0047]. Smith's altitude-to-floor estimation supplies the vertical counterpart of that resolution, and a POSITA would have expected success in adding it because it operates on a value the combined system already receives.

713. Accordingly, it is my opinion that Rauner in view of Azmoodeh and further in view of Smith renders obvious each limitation of claim 9 of the '421 Patent, including limitations 9[a] through 9[c].

XI. CONCLUSION

714. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the

like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: October 7, 2026

By: 
David H. Williams

RAVE/MSI, EX1005, p. 388

Appendix I: Claim Listing

XII. '757 Patent Claims

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.
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.
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.
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.
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.
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
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.
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.
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.
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.
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 at 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.
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.
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.
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.
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.
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.
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.
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.

XIII. ’421 Patent Claims

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;
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.
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.
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.
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.
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.
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.
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.
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.
Claim 9	
9[a]	The method of claim 1, wherein: the at least one security parameter comprises an altitude
9[b]	the at least one grid parameter comprises a building floor, and
9[c]	the building floor is estimated from the altitude.
Claim 10	
10[a]	The method of claim 1, wherein the supervisee is associated with at least one identification, wherein the method comprises:
10[b]	receiving, using the communication device, at least one indication corresponding to the at least one identification from the at least one supervisee device; and

10[c]	identifying, using the processing device, the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying.
Claim 11	
11[pre]	A system for facilitating supervision of individuals based on geofencing, the system comprising:
11[a]	a communication device configured for:
11[a][1]	receiving at least one security parameter from at least one supervisor device associated with at least one supervisor;
11[a][2]	receiving a geographical location from the at least one supervisor device;
11[a][3]	receiving at least one supervisee data associated with a supervisee from at least one supervisee device; and
11[a][4]	transmitting a supervision notification to the at least one supervisor device;
11[b]	a processing device configured for:
11[b][1]	analyzing the geographical location based on the at least one security parameter;
11[b][2]	generating a geofence corresponding to a geographical area based on the analyzing;
11[b][3]	analyzing the at least one supervisee data based on the geofence; and
11[b][4]	generating the supervision notification based on the analyzing of the at least one supervisee data; and
11[c]	a storage device configured for storing the at least one supervisee data and the supervision notification, wherein:
11[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,
11[d][1]	wherein the communication device is further configured for receiving at least one grid parameter from the at least one supervisor device,
11[d][2]	wherein the processing device is further configured for: analyzing the at least one grid parameter;
11[d][3]	determining the grid box geofence area based on the analyzing of the at least one grid parameter; and
11[d][4]	generating a number of geofence grid boxes based on the determining.
Claim 12	
12[a]	The system of claim 11, 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:
12[b]	identifying at least one location corresponding to the at least one location indication;
12[c]	analyzing the at least one supervisee data based on the at least one location; and
12[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.
Claim 13	
13[a]	The system of claim 11, 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:

13[b]	determining the at least one action based on the supervision notification; and
13[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.
Claim 14	
14[a]	The system of claim 11, wherein the processing device is further configured for identifying the supervisee based on the analyzing of the at least one supervisee data,
14[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.
Claim 15	
15[a]	The system of claim 11, 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
15[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.
Claim 16	
16[a]	The system of claim 11, 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:
16[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.
Claim 17	

17[a]	The system of claim 11, wherein the storage device is further configured for retrieving a blueprint associated with the geographical area corresponding to the geofence,
17[b]	wherein the processing device is further configured for analyzing the blueprint and the at least one supervisee data; and
17[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.
Claim 18	
18[a]	The system of claim 11, wherein the at least one supervisee device comprises at least one sensor,
18[b]	wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,
18[c]	wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting.
Claim 19	
19[a]	The system of claim 18, wherein: the at least one signal made by the supervisee comprises shaking the supervisee device abruptly, pressing a button, or speaking a specific phrase, wherein: the at least one sensor is configured for detecting the at least one signal,
19[b]	and the supervisee device is configured to optionally make an emergency call when the at least one sensor detects the at least one signal;
19[c]	wherein a phone number dialed in the emergency call is determined based on the geofence.
Claim 20	
20[a]	The system of claim 11, wherein the supervisee is associated with at least one identification,

20[b]	wherein the communication device is further configured for receiving at least one indication corresponding to the at least one identification from the at least one supervisee device,
20[c]	wherein the processing device is further configured for identifying the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying.
Claim 21	
21[a]	The system of claim 11, wherein each geofence grid box is further characterized by: a) storing at least one emergency contact number associated with the geographical area represented by the grid box geofence area;
21[b]	b) wherein the emergency contact number includes a 911 service or equivalent emergency service specific to then geographical area of the grid box; and
21[c]	c) wherein the processing device is configured to automatically select and transmit supervisee data to the stored emergency contact number upon detecting an emergency situation within the corresponding grid box geofence area.
Claim 22	
22[pre]	A method for facilitating supervision of individuals based on geofencing, the method comprising:
22[a]	receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor;
22[b]	receiving, using the communication device, a geographical location from the at least one supervisor device;
22[c]	analyzing, using a processing device, the geographical location based on the at least one security parameter;
22[d]	receiving, using the communication device, at least one supervisee data associated with a supervisee from at least one supervisee device;

22[e]	analyzing, using the processing device, the at least one supervisee data based on the geographical location;
22[f]	generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data;
22[g]	transmitting, using the communication device, the supervision notification to the at least one supervisor device; and
22[h]	storing, using a storage device, the at least one supervisee data and the supervision notification; wherein:
22[i]	the at least one supervisee device comprises at least one sensor,
22[j]	wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,
22[k]	wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting,
22[l]	wherein the supervisee data comprises audio and video recordings;
22[m]	wherein the at least one sensor is selected from one or more nearby sensors based on the most proximal nearby sensor by geographical location in real-time; and
22[n]	wherein the at least one sensor tracks the supervisee as the supervisee moves between the one or more nearby sensors.
Claim 23	
23[a]	The method of claim 22**,** wherein: the supervision notification is sent to a first distinct group of one or more supervisor devices correlated with the geographical location;
23[b]	the first distinct group of one or more supervisor devices is comprised of nearby first responders and dispatchers; and

23[c]	the supervision notification may be sent to a second distinct group of one or more supervisor devices based on the location and expertise of the second distinct group.
Claim 24	
24[a]	The method of claim 22**,** wherein: wherein the supervisee is associated with at least one identification,
24[b]	wherein the communication device is further configured for receiving at least one indication corresponding to the at least one identification from the at least one supervisee device,
24[c]	wherein the processing device is further configured for identifying the supervisee based on the at least one indication, wherein the generating of the supervision notification is based on the identifying.