Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2607236 A1 2006/11/16

(21) 2 607 236

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2006/05/08
(87) Date publication PCT/PCT Publication Date: 2006/11/16
(85) Entrée phase nationale/National Entry: 2007/11/05
(86) N° demande PCT/PCT Application No.: US 2006/017678
(87) N° publication PCT/PCT Publication No.: 2006/122004
(30) Priorités/Priorities: 2005/05/06 (US60/678,823);
2006/04/06 (USPCT/US06/012754)

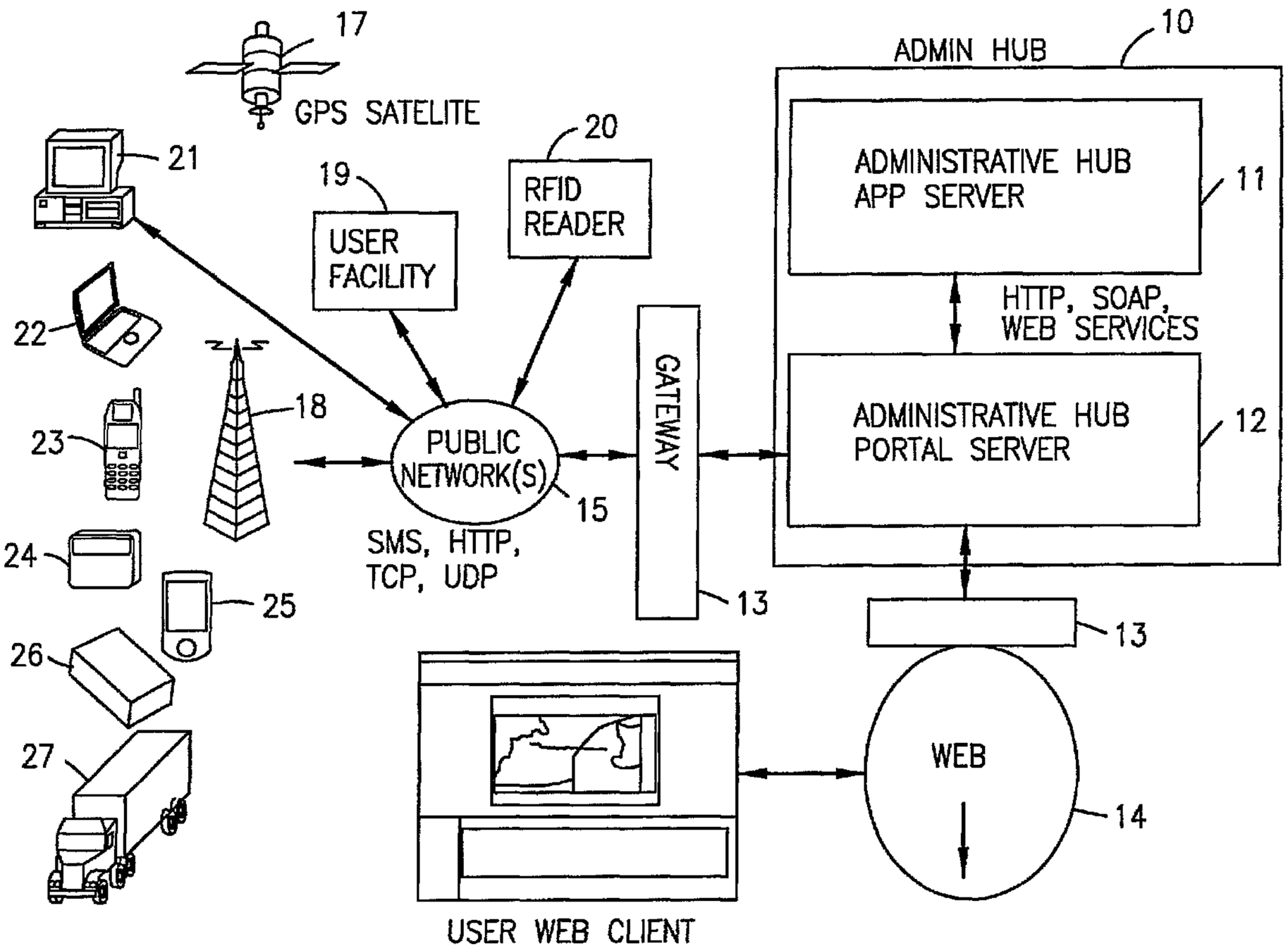
(51) Cl.Int./Int.Cl. *G08B 23/00* (2006.01),
G08B 1/08 (2006.01), *G08B 21/00* (2006.01),
G08B 21/02 (2006.01)

(71) Demandeur/Applicant:
OMNILINK SYSTEMS, INC., US

(72) Inventeurs/Inventors:
ANINYE, STEVE, US;
RAJALA, YOGANAND, US

(74) Agent: GOUDREAU GAGE DUBUC

(54) Titre : SYSTEME ET PROCEDE DE SUIVI DU MOUVEMENT D'INDIVIDUS ET DE BIENS
(54) Title: SYSTEM AND METHOD OF TRACKING THE MOVEMENT OF INDIVIDUALS AND ASSETS



(57) Abrégé/Abstract:
A monitoring system is provided, by which location data and possibly other information from a wireless personal tracking device carried by an individual is transmitted to an administrative hub for processing and action according to defined rules. Simultaneous monitoring of a plurality of individuals with diverse tracking units and effective event recording and reporting can be implemented.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 November 2006 (16.11.2006)

PCT

(10) International Publication Number
WO 2006/122004 A1

(51) International Patent Classification:
G08B 23/00 (2006.01) *G08B 1/08* (2006.01)
G08B 21/00 (2006.01) *G08B 21/02* (2006.01)

(21) International Application Number:
PCT/US2006/017678

(22) International Filing Date: 8 May 2006 (08.05.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/678,823 6 May 2005 (06.05.2005) US
Not furnished 6 April 2006 (06.04.2006) US

(71) Applicant *(for all designated States except US)*: **OMNILINK SYSTEMS, INC.** [US/US]; 13010 Morris Road 6th Floor, Alpharetta, GA 30004 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **ANINYE, Steve** [US/US]; 13010 Morris Road 6th Floor, Alpharetta, GA 30004 (US). **RAJALA, Yoganand** [US/US]; 13010 Morris Road 6th Floor, Alpharetta, GA 30004 (US).

(74) Agent: **JOHNSON, Douglas, T.**; MILLER & MARTIN PLLC, Suite 1000 Volunteer Building, 832 Georgia Avenue, Chattanooga, TN 37402 (US).

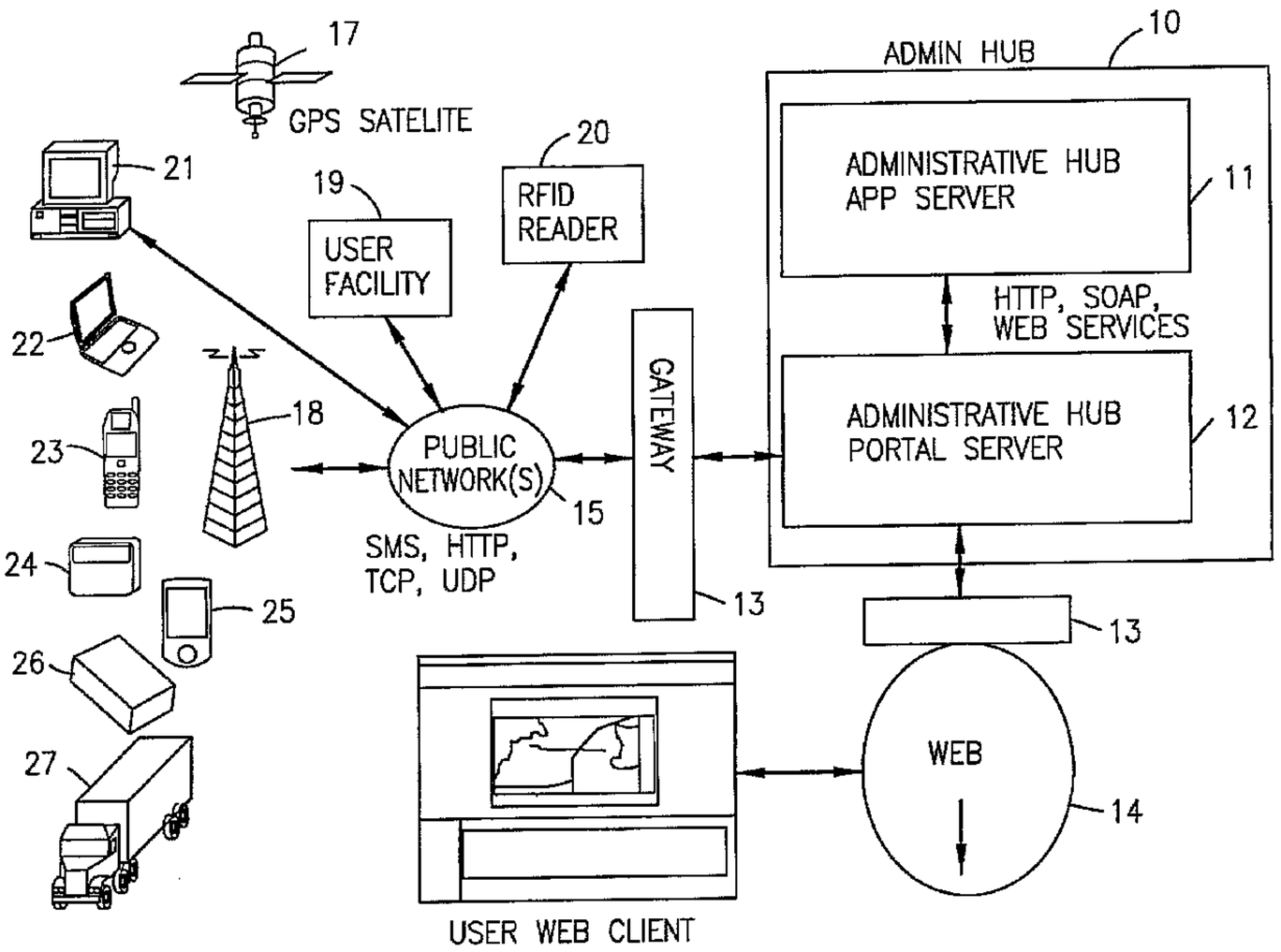
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** SYSTEM AND METHOD OF TRACKING THE MOVEMENT OF INDIVIDUALS AND ASSETS



(57) **Abstract:** A monitoring system is provided, by which location data and possibly other information from a wireless personal tracking device carried by an individual is transmitted to an administrative hub for processing and action according to defined rules. Simultaneous monitoring of a plurality of individuals with diverse tracking units and effective event recording and reporting can be implemented.

A1 WO 2006/122004

System and Method for Tracking, Monitoring, Communicating and Responding to the Movement of Individuals and Assets

Priority

The present application claims priority to the May 6, 2005 filing date of U.S. provisional patent application, Serial No. 60/678,823 and the April 6, 2006 filing date of PCT US06/12754, which are incorporated herein by reference.

Field of the Invention

[0001] The system and method of the present invention is utilized in determining the position of an individual using GPS signals and cell phone location technologies for both real time and later comparison with parameters and providing bidirectional communication capability with the tracking device associated with the individual, and providing a response network to address critical alarm conditions.

Background of the Invention

[0002] Many devices and systems are known to monitor the position and movements of individuals. Employers use devices to monitor employees against diversion from work-related locations, and such devices may be installed in work vehicles, attached to accessories such as computers, or comprise other GPS enabled devices. In addition, in the case of house arrest, the offender must often carry a body-worn device to permit position monitoring. The monitoring of individuals may take either active or passive forms. An active system will compare its location with ongoing restrictions to detect violations. Such a violation may occur by either coming into broadcast range of a prohibited zone, leaving broadcast range of a confinement zone, or by actual location determination and mapping against both permitted and exclusion zones. Alternatively, passive devices may simply record and transmit location information for later or real time comparison with permitted and excluded zones at a remote system.

PCT/US2006/017678 RO/US 28/08/06

[0003] Many devices have been proposed and employed for such uses. Among the most common are multi-component systems. Such systems typically include a wearable radio frequency (RF) bracelet that communicates with some type of base device. This may be a fixed base system with access to a telephone line that places a telephone call to a monitoring service anytime the RF signal is not detected. Alternatively, it may be a portable base equipped with GPS location technology that detects the presence of the bracelet RF signal and also tracks movements and periodically communicates, typically through wireless phone technology, to report those locations. These devices may also have the capability of displaying text messages from the monitoring officer or agency on an LCD screen. Some base attachments have attempted to utilize voice recognition technology to provide verification of the identity of a person present and responding to a phone call placed through the base unit.

[0004] Generally absent from these systems is the ability for real time or near real time communication directly between a remote system and the locator device associated with the individual. In addition, the component costs of custom devices is unnecessarily high compared to the prices available for mass market cellular telephone and GPS technology. Many systems require dedicated phone lines, require the monitored individual to wear or carry obtrusive hardware, require additional hardware for monitoring personnel, lack adequate battery life for multi-day usage, are subject to drift due to GPS signal errors, and lack a method for confirming receipt of messages sent between monitoring personnel and a monitored individual.

[0005] Accordingly, there is a need for an individual tracking system that can be deployed with software capable of running on a wide variety of devices and is therefore largely device agnostic.

PCT/US06/17678 RO/US 28/08/06

[0006] There is also a need for an individual tracking system that does not require the use of dedicated phone lines or obtrusive hardware. There is also a need to provide real time or active tracking and active notification to monitoring personnel.

[0007] There is a further need for a system with easily configurable rules and with easily updated and connected location data.

[0008] There is an additional need to provide a method for shorter response times to alarm conditions than can be economically provided by municipal police and private security services.

Summary of the Invention

[0009] Accordingly, it is an object of the invention to provide a largely device agnostic system for monitoring of individuals.

[00010] It is further an object of the invention to implement individual tracking capability without the necessity of obtrusive hardware or dedicated phone lines.

[00011] It is yet another object of the invention to provide an individual tracking system that does not require specialized hardware for monitoring personnel.

[00012] It is a further object of the invention to provide active or real time location information concerning monitored individuals and to provide active notification to monitoring personnel.

[00013] It is another object of the invention to provide a method for confirmed communications between monitoring personnel and a monitored individual.

[00014] It is yet a further object of the invention to provide an easily adjustable and tamper resistant wearable tracking device.

[00015] It is an additional object of the invention to provide a system that allows the implementation of many rules, and which is easily updated with location data, and can self correct location data.

SUBSTITUTE SHEET (RULE 26)

PCT/US2006/017678 RO/US 28/08/06

[00016] It is a further additional object of the invention to provide a responsive network to provide assistance to monitored individuals signaling an alarm condition.

Brief Description of the Drawings

[00017] Figure 1 is a schematic diagram showing the communication paths of components utilized in the invention.

[00018] Figure 2 is a block diagram of the functional architecture of an administrative hub server.

[00019] Figure 3 is a functional architecture diagram of an administrative hub portal server.

[00020] Figure 4 is a schematic diagram reflecting the processing of communications by a portable device according to the present invention.

[00021] Figure 5 is a functional architecture diagram of a wearable tracking device according to the present invention.

[00022] Figure 6 is a high level electrical block diagram of a wearable tracking device according to the present invention.

[00023] Figure 7A is a perspective view of a tamper resistant strap for use with a wearable tracking device according to the present invention.

[00024] Figure 7B is a perspective view of a wearable device according to the invention with strap affixed.

[00025] Figure 7C is a perspective view of a locking pin utilized to hold the strap of Figure 7B in place.

[00026] Figure 7D is a rear perspective view of a monitoring device according to the present invention.

[00027] Figure 7E is a perspective view showing the method of attaching a monitoring device of the present invention to the wearer's leg with the device, attached strap and lock bracket.

SUBSTITUTE SHEET (RULE 26)

[00028] Figure 7F is a perspective view of a lock bracket base according to the present invention in isolation.

[00029] Figure 8 is a schematic and flow chart reflecting a confirmed communication protocol that may be implemented according to the invention.

[00030] Figure 9A is a screen display of a graphical location history map that may be generated with location data provided by the invention.

[00031] Figure 9B is a pop up text window reflecting the graphical data of Figure 9A.

[00032] Figure 10A is a screen display of graphical map of an inclusion zone defined according to the present invention.

[00033] Figure 10B is a schematic representation of inclusion and exclusion zones.

[00034] Figure 11 is a screen display of a status report for individuals being monitored according to the present invention.

[00035] Figure 12 shows a screen display of a data entry template for a new individual to be monitored according to the present invention.

[00036] Figure 13 is a screen display of a representative violation report that may be generated when utilizing the invention of the present system to monitor offenders subject to restrictions.

[00037] Figure 14 is a screen display of a representative device report for devices being monitored according to the present invention.

[00038] Figure 15 shows a screen display of a management function template for editing schedules.

[00039] Figure 16 depicts a screen display of a management schedule for automatic notification procedures.

SUBSTITUTE SHEET (RULE 26)

RO/US 28/08/06

[00040] Figure 17 shows a screen display of an administrative data entry form for establishing a new user on the system.

[00041] Figure 18 is a schematic illustration of the implementation of a response network.

[00042] Figure 19 is a schematic illustration of communication paths of users of a system implementing the invention.

[00043] Figure 20 is a flow chart of a method of adding and removing sensors to report alarm conditions at a physical location.

[00044] Figure 21 is a flow chart of a process of arming and disarming sensors at a physical location.

[00045] Figure 22 is a flow chart of a process of implementing a response to a monitored individual's alarm condition.

Detailed Description of the Invention

[00046] Turning then to Figure 1, a schematic overview of the communication path utilized in the present invention is illustrated. Control of the invention is preferably maintained at one or more administrative hubs **10** running application server **11** functionality and portal server **12** functionality. The portal server **12** will communicate through gateways **13**, generally routers or a location aggregator, with the Internet **14** or some combination of public networks **15**, possibly including the Internet, and telephone networks. Communications are then directed to and/or from a wide variety of devices with respect to the administrative hub **10**. For instance, an RFID reader **20** may detect and report the presence of an RFID tag. The administrative hub **10** may generate a message to a controllable device user at facility **19** and receive a confirming acknowledgement. A user of the invention may obtain information via personal computer **21**, laptop computer **22**, cell phone **23**, Blackberry **24**, Palm Pilot **25** or other digital communication device. The tracking device may be in a wearable ankle bracelet box **26**, installed in a vehicle

SUBSTITUTE SHEET (RULE 26)

27, or operated on GPS enabled mobile communications devices such as Palm Pilots **25**, Blackberrys **24**, cell phones **23**, or even on appropriately configured laptop computers **22**. If the tracking software is installed on these or similar devices, then location information generated from GPS satellite **17** and confirmed by assisted GPS location data for cell tower triangulation, together with any other types of data collected by the mobile communication device, is periodically transmitted to the administrative hub **10**. A user of the system with access via a web enabled device is able to graphically display a variety of tracking device information utilizing web client **16**. In addition, the user may generate messages to the administrative hub **10** or to any of the described communication enabled devices. Because the system is implemented in a device agnostic fashion, it is contemplated that the system will operate with a plurality of types of devices employed by both users who access data and by monitored persons.

[00047] Turning then to an examination of the system components in greater detail, the logical architecture of a representative administrative hub application server **11** is shown in Figure 2. This server has a standard administration **41** and security **42** functionality. The three principal categories of the services provided by the application server **11** are data services **43**, core services **46**, and communications services **55**. Data services **43** include data housed in OLTP (Online Transaction Processing) or OLAP (Online Analytical Processing) relational or multidimensional databases **45** and data access objects (DAO) **44** to allow data access mechanisms to change independently of the code that uses the data. Core services **46** principally comprise message processor **47** for parsing and either acting upon or forwarding incoming messages for action and building and formatting outgoing messages in appropriate packet format; reporting services **48** for building reports from event logs stored in data services **43** and organizing the data for transmission to portal server **12**; remote parameters management **49** for

EC'd US/US 28/08/06 RO/US 28/08/06

storing and managing parameters such as time intervals for a mobile unit to take location fixes and for initiating communications with administrative hub **10**, and intervals for battery charge testing and reporting and battery charge requirements; notification/alerts **50** for configuring conditions that will generate alerts and reports, including persons to be notified for types of events, immediate or delayed timing for those notifications, and the communication methods to be employed in notifications; system configuration services **51** to hold parameters defining the system and user preferences which may include language choice, time zone, and the like; location services **54** to convert data from mobile units to position, and geocoding to or from a particular address, as well as performing assisted GPS location calculations and any necessary drift correction; scheduling services **53** for managing times including regular schedules for exclusion and inclusion zones, as well as special permissions or allowed variations from usual schedule, and required appointments at particular addresses; and monitoring services **52** for comparing reported locations against rules for the monitored individual's locations and generating appropriate information to the notification/alerts module **50** in the event of violations. The communication services component **55** includes inbound and outbound message queues **57, 58;** communication adapters **56** to allow messaging with a variety of devices; data bridge **59** to permit data from core services to be formatted into outbound messages, and inbound messages to be formatted for access by core services **46**; and personalization **68** to permit users to specify custom reports and preferred screen displays. Finally, an interface **61** such as XML protocol for accessing web services is provided.

[00048] Figure 3 shows a similar logical architecture of an administrative hub portal server **12** which once more has standard administrative **70**, security **71** and interface **99** modules. The principal functionality of portal server **12** may be divided into data services **72**, system services

RECTIFIED SHEET (RULE 91)
RO/US 28/08/06

76, application services 85 and a browser 98. Data services 72 principally comprise a repository for data needed to reply to inquiries from users accessing the system using their web client 16 (shown in Figure 1).

[00049] Principal components of data services 72 include system metadata repository 73 holding information with respect to the system components so that they may be accessed when needed to carry out actions; workflow repository 74 queuing the actions to be carried out; and OLTP/OLAP storage 75. System services provide a number of modules corresponding to core services on the application server including reporting services 80, notification alerts 84, and location services 82. In addition, system services provide mapping services 83 for rendering locations on graphical maps, workflow executive 72 for parsing actions in the workflow repository 74 and commencing execution of those actions, data integration 78 for merging structured and unstructured data into a useful form such as XML for use by the system, and digital business identity 79 for holding user management information utilized by the system's access control logic. The application services 85 include display related personalization 92; search functionality 87; reporting 86; points of interest 89 for assigning descriptive names to physical locations in lieu of addresses; subscriptions 90 for allowing users to specify types of information to receive, such as whenever a new subscriber or offender is added for monitoring, whenever a mobile unit is disabled, or other types of events separate from the violation type notification/alerts; directions 88 for facilitating navigation to locations; and calendaring/scheduling 91 to communicate schedule information with scheduling services 53 on application server 11. Presentation services 93, principally comprising templates 94, themes 95, and rendering 97, provide for enhanced screen displays presented in browser 98. Events 96 translates user keystrokes and mouse clicks into workflow actions.

SUBSTITUTE SHEET (RULE 26)

RECTIFIED SHEET - EXCLUDED
RO/US 28/08/06

[00050] Figure 4 shows an overview of messaging between application hub **10** and user device **100**. A message may be generated by application server **12** and then communicated via Internet and typically public cellular network **15** to device **100** where it is inserted in the inbound message queue **104**. Messages are then read into the messaging hub **102** which corresponds to communication services **114** shown in Figure 5 and deleted from the inbound queue **104**. Received messages are then processed for message type and appropriate message data is transmitted to embedded application **101** in the device **100**. Similarly, the embedded application **101** may generate acknowledgement for messages which are transmitted to messaging hub **102**, formatted and inserted in outbound message queue **103**.

[00051] The logical architecture of a representative device utilized in the invention is reflected in Figure 5. A preferred device uses a real time operating system (RTOS) or a virtual machine software implementation of a desired CPU and native device drivers **111** to permit operation of the system with a wide variety of devices **100**. In even the more basic tracking devices typified by vehicle tracking **27** or offender tracking **26** devices, there are device drivers **115** to interface with much of the hardware shown in Figure 6, systems services **113** to monitor device status **112** or to generate alerts, and communication services **114** to transmit stored data and alerts as described in connection with Figure 8. Wireless business framework **116** implements the confirmed delivery of messages, as also explained in connection with Figure 8, while presentation framework **117** contains dispatch module **118**, which effectively is a calendaring or scheduling functionality, and messaging **119** which is only available on more advanced devices such as handhelds, phones with LED displays, or computers. Monitoring rules and constraints **120** are implemented to generate active monitoring notifications while location tracking **121** generates GPS and assisted GPS location data.

RO/US 28/08/06

[00052] Figure 6 is a high level block diagram of a device **100** used in the invention. Typically, the device is based upon a GPS enabled cell phone, principal components of which are flash memory **129**, CPU **130**, data bus **131**, cellular modem **132**, antenna **133**, GPS receiver **134**, display driver **136**, speaker **140**, and microphone **141**. The operating system or virtual machine software, as appropriate to the device, may be installed in flash memory **129** and operates in connection with CPU **130** to present a standard device profile to the system. Communications are transmitted from the CPU through the data bus **131** to cellular modem **132** and broadcast in the form of digital packets via antenna **133**. Similarly, incoming messages travel in the reverse sequence.

[00053] The GPS receiver **134** is utilized to generate location information. Because GPS location requires line of sight access to GPS satellites **17**, and because GPS location is sometimes subject to erroneous results due to drift or temporary satellite misorientation, GPS assist **135** may be added to the device or the cellular network. Assisted GPS generates location information based upon signals received from nearby cellular communication towers **18** and without correction is often only accurate to within several hundred feet rather than the GPS location accuracy of only several feet. Nonetheless, assisted GPS provides valuable location confirming information as well as at least general location information when line of sight access to GPS satellites is unavailable.

[00054] Alternatively, location information may be provided by a location aggregator. The location aggregation service may be provided by a cellular network provider or an entity operating a gateway in connection with the cellular network or other broadcast communication provider. Many cellular networks are now capable of determining the location of GPS enabled cellular handsets with some degree of accuracy, particularly handsets that facilitate assisted GPS

PCT/US06/17678 RO/US 28/08/06

such as those using Qualcomm 6050 or 6250 microprocessors which permits the network to use AFLT. While the 6250 microprocessor can operate autonomously to determine the co-ordinates of the handset, both of the Qualcomm processors can also operate in response to a cellular network query, or by generating a their own location query, to cause the network to acquire the GPS data received by the cellular handset, and to utilize Advanced Forward Link Triangulation (AFLT) or other cellular network information, to produce an assisted GPS geolocation for the handset.

[00055] In a further refinement, the GPS and cellular network data may be processed by the location aggregation service for accuracy. For instance, location information data may be processed utilizing noise processing theorems to correct for bad data such as drift caused by a GPS satellite wobble, or the effects of changes in signal reflection and absorption caused by varying conditions such as locations in urban canyons, the woods, or beneath heavy cloud cover, and atmospheric ionization changes from day and night. Information as to the geolocation of the handset is then communicated by the location aggregator to the administrative hub, and in appropriate instances may also be communicated to the handset.

[00056] While the display driver **136**, microphone **141** and speaker **140** may be disabled or removed from vehicle location **27** or offender bracelet **26** constructions, other hardware may be added. For instance, in the case of an offender bracelet **26**, tamper detector **139** and LED driver **137** and LED emitter receiver **138** are added to provide redundant tamper indicators as explained below in connection with Figure 7.

[00057] A preferred offender tracking device **26** is illustrated in Figures 7A – 7F. The principal components of tracking device **26** are lock bracket **144** as shown in isolation in Figure 7F, a strap **150** shown in isolation in Figure 7A, and main housing **170** shown in bottom view in

SUBSTITUTE SHEET (RULE 26)

Figure 7D and top phantom view in Figure 7B. Turning first to the strap **150** of Figure 7A, a representative strap **150** might be manufactured from plastic molded over optical cable **151** and light guide **153**. The strap will preferably have a light guide/connector **152**, apertures **154** to accept fasteners, and apertures **155** to receive locking posts. An alternative strap design includes a flexible battery within the strap. Optical cable **151** may still be included in the strap **150**, and significant power resources for the device can be located within the strap. This results in the main housing **170** no longer having to contain the entire power supply, and by utilizing a smaller battery within the housing, the size of the housing may be reduced, resulting in a device that is more easily worn.

[00058] An exemplary battery technology that may be employed in such a strap is a thin flexible battery using NECs organic radial battery technology. Turning then to Figure 7D, it can be seen that fasteners **156** have been received through apertures **154** of strap **150** and thereby fasten the strap **150** to bottom of main housing **170**. As shown in Figure 7B, main housing **170** contains recharge connector **180**, tamper sensor switch **181**, battery **182**, antenna **183**, and generally the components **184** reflected in Figure 6. When used without a power strap, the battery **182** is preferably a long life battery which has a life of up to approximately 21 to 30 days when used for offender monitoring in monitoring units having current efficient circuitry and antenna design, and effective power management algorithms to minimize the number and duration of transmissions from the unit and the intensiveness of calculations carried out in the mobile unit. This permits monthly visits to a probation officer with the necessity of recharging the battery by the offender only once, if at all.

[00059] When used with a power strap, the battery in the strap **150** preferably has these long lived characteristics, and the battery **182** within the housing **170** may be simply a short term

PCT/US2006/017678 RO/US 28/08/06

back-up power supply, to operate the device temporarily if the power strap is damaged or disconnected. The storage in device **100** is sufficient to store messages and GPS location recordings for up to about two weeks depending upon the frequency with which GPS location readings are recorded.

[00060] The bottom of main housing **170** in Figure 7D shows a variety of features including opening **171** for tamper sensor **181**, opening **172** for recharge connector **180**, rearward facing hooks **173**, lens opening **174** to transmit light from a diode to the light guide connector **172** of strap **150** and forward lip **175** defining cavity **176**. The side walls for cavity **176** have apertures **177** to receive locking pin **160** shown in Figure 7C.

[00061] To attach the device **26** as shown in Figure 7E, the lock bracket **144** is placed on the offender **190**. Accordingly, the bottom surface of the lock bracket **144** is preferably made with comfortable to wear surface. The top surface of lock bracket **144** has an outer flange **146** to receive housing **170** and a plurality of upstanding pins. At one end are two relatively short pins **145** that interface in the strap openings **154** that receive fasteners **156**. At the opposite side of the face of lock bracket **144** are two taller pins **148** that are received in apertures **155** of strap **150** after it encircles the offender's arm or leg **190**. These taller pins **148** have lateral apertures **165** to receive the locking pin **160**. Also shown is pin **149** that is received in aperture **171** to activate the tamper sensor switch **181**.

[00062] Thus, to fit the device **26** to the offender, lock bracket **144** is placed on the offender's leg **190.** The light guide connector **152** end of the strap **150** is secured to the housing **170** as by screws **156**. The strap **150** is placed so that the unattached end is received over posts **145, 148.** The strap is then wrapped around the offender's leg **190**, and the main housing hooks **173** are received in flange recesses **147** on lock bracket **144**, while posts **148** extend upward into cavity

RECTIFIED SHEET (RULE 91) ISA/US RO/US 28/08/06

176. Then locking pin **160** is passed through openings **177** and pin holes **165** so that the pin head **163** extends from one side of front lip **175** and base **161** extends from the other side with lateral section **162** extending therebetween. In the event that the offender should attempt to remove the pin **160**, it will break at breakpoint **164** and the tamper detector will be activated. Similarly, if the optical cable **151** of strap **150** is cut, the tamper detector will be activated. Finally, if the main housing **170** is removed from lock bracket **144**, the tamper sensor switch **181** will be activated. In any of these instances, the device **26** will generate a message to the administrative hub **10** advising of the tampering event.

[00063] An effective tamper detector to ascertain whether there has been a breach of the housing **170** may combine a light sensor that is activated when light enters the housing and an electromagnetic field sensor that is activated if metal components of the housing are dislocated. A sophisticated tamper detector used with the optical cable may utilize an LED driver **137** and one or more LEDs to emit at least two different frequencies of light in alternating or random sequence through the lens opening **174** into the light guide connector **152** and outbound on a first length of optical cable **151** to light guide **152** and back inbound on the second length of optical cable **151**. Simultaneously, the LED receiver is informed of the frequency being emitted, and if either no light or the wrong frequency light is detected inbound, then a tamper alert is generated.

[00064] It will be appreciated that in securing the device **26** to an offender, it is not necessary to cut strap **150**. Instead, the strap will fit a substantial range of offender leg sizes and requires no special tools to secure the unit on the offender's leg. Prior art devices have generally required the strap be cut to length and in the event that optical cable is utilized for tamper indication, the difficulties of accurately splicing the cable not only requires special tools, but also is likely to be

PCT/US2006/017678 RO/US 28/08/06

sufficiently defective that false tamper alerts may be generated. Furthermore, when the device is removed from an offender, only the pin **160** is destroyed, so that the strap **150** may be reused.

[00065] Turning then to Figure 8, the messaging protocol providing for confirmed messaging is illustrated. First, a device **100** generates message **201**. This message may be generated as a result of an alarm condition such as tampering, low battery, or entry into an exclusion zone, or alternatively may be simply a regularly scheduled transmission of location data as the device will be configured to take location readings periodically, typically in intervals of about one to five minutes, and to transmit those readings in batches, typically about every thirty minutes, preferably in a proprietary data packet. Such a data packet preferably has a header identifying message type, a security token, and message data. After the device **100** generates message **201**, the message is transmitted **202** and received **203** by administrative hub **10**. The data packet is parsed **204** to confirm a message type, the sending device, that security protocols are satisfied, and to determine that the data is not corrupt. Administrative hub **10** then sends an acknowledgement **205** to device **100** which receives the acknowledgement **206** and deletes the message from its outbound message queue **207**. If the administrative hub determined the message was corrupt, it would request that the message be resent. If the device **100** did not receive an acknowledgement within a predetermined time period, it would resend the message.

[00066] It is also possible for messages to be generated at the administrative hub **10**. These messages might actually be entered by systems personnel at the administrative hub **10** or by monitoring personnel interfacing with the administrative hub via user web client **16** or other suitably enabled device. Accordingly, a typical message generated might be from a probation officer advising an offender with a display equipped monitoring device that he has a court date at a particular time and place; or a message from a dispatcher to a pickup/delivery vehicle advising

of an additional address to include on a route; or an administrative change to redefine an exclusion zone or alter a parameter of operation such intervals for taking and reporting location readings. Once the message is generated **210**, the messaging hub transmits **211** the message which is received **212** by device **100**. The device **100** parses **213** the message for message type and confirms appropriate security token is present and that the message is not corrupt. Then the device **100** generates an acknowledgement **214** which is sent to messaging hub and received **215**. The administrative hub **10** then records confirmation that the message was received by device **100**. The device **100** proceeds to process the message data **217**.

[00067] When the administrative hub **10** is messaging device **100** with user display means such as a LED screen, messages may be sent which request a response. For instance, probation officer might ask an offender if he needs a ride to a court hearing. A dispatcher might ask a delivery/pickup person if he can make an extra pickup or delivery, and in either case request a reply. In the event that the message is received by the device **100** but there has been no reply, it is possible for the administrative hub to issue a message recall **220**. When that recall is received **221** by device **100**, it parses recall message **222**, generates an appropriate acknowledgement **223**, and proceeds to delete the message. The administrative hub receives the acknowledgement **224** and records the deletion of the message **225**.

[00068] Alternatively, if the device user responds to the message **230**, the response is sent to the administrative hub **10** and received **231**. Then the response is parsed **232** and acknowledged **233**, and the administrative hub proceeds to process the data in the response, perhaps informing a dispatcher that the requested pickup or delivery has been accepted by the pickup/delivery driver. The device **100** receives the acknowledgement **234** and proceeds to delete the response from its messaging queue **235**. Thus, the invention provides for a robust two-way messaging system with

SUBSTITUTE SHEET (RULE 26)

PCT/US06/17678 RO/US 28/08/06

confirmed messaging delivery and message recall capability. The administrative hub **10** has the capability of sending inquiries to the device **100** in order to return information regarding device status and location information. The message confirmation protocols assure that a reliable audit trail can be maintained by the system.

[00069] The administrative hub **10** has the capability of sending alerts to a variety of devices. For instance, the hub **10** can provide graphic data and text messages to user devices with screen displays; it can send email messages to email accounts; it can send text messages; it can send fax reports or alerts; and it can generate voice alerts to be received by telephone or RF enabled devices. Thus, a probation officer can receive a voice alert generated by the system over a regular telephone when a high priority alarm warrants such communication.

[00070] Figures 9 and 10 display a user web client **16** such as would be available to a probation officer or dispatcher utilizing the invention. Figure 9A discloses a location history map **300** with indicators **301** showing the locations of a tracked individual over time. To utilize this reporting functionality, a location history is selected in the location menu **311**. The target entity is selected **302** and displayed **303**. Starting time **304** and ending time **305** are entered and display **306** generates the appropriate mapping. The location history can also be generated in a text popup screen **315** with text entries **316** corresponding to numbered indicators **301** on the map screen **300**. The location history may also be overlaid with the location history of one or more other monitored individuals for analysis, such as the enforcement of separation/non-association orders or to disclose behavioral patterns among offender groups. The locations and text route histories may be exported **317** into a digital file or document for use apart from the device management and interaction software. As shown in Figure 9A, additional types of reporting and functionality are also available. Report menu **307** provides for the creation of

SUBSTITUTE SHEET (RULE 26)

device reports that could include items such as battery power, battery charging events, device tampering attempts, and the like as reflected in greater detail in Figure 14. An event log may be created listing a variety of different types of events that may have transpired; a message report lists messages between a user and the device; an online/offline report lists the times that the device was not within a reporting area; and a proximity report provides data concerning the device's proximity to a particular location or another enabled device. A speeding report extrapolates the device speed between location reports and lists instances when the distance between way points indicates a speed in excess of a user designated limit. A stops report indicates locations where the device has remained stationary for a user-determined interval. A violation report as shown in Figure 13 lists instances in which the device wearer has entered exclusion zones or deviated from established routing. Additional menus **308**, **309**, **310** are provided for management and administration functions discussed below.

[00071] Figure 10A shows an inclusion/exclusion zone map **320** with defined inclusion zone **321**. In the manage entity menu **308**, new zones may be added and applied to target entities or existing zones may be edited. For a stationary zone such as inclusion zone **321**, an address is entered **323** and named **322**. Target entity is selected **324** and displayed **325**. The zone has a starting time **326** and ending time **327** as is appropriate for offenders with a probationary term. The zone may be made active on all or selected dates **328**, and the radius of the zone defined **330**. In addition, the zone may be defined as inclusion or exclusion type **329**.

[00072] Two particular advantages of the present invention are the ability to define buffer zones and mobile exclusion or inclusion zones. Relative to mobile zones for instance, inmates on a work crew may be assigned to an inclusion zone within a defined radius of a supervising corrections department official. The official will carry a device that is tracked by a

administrative hub **10** as the official moves about. Any inmate whose device leaves the inclusion zone about the official's device generally causes alerts to be sent with tracking data so that the inmate may be apprehended. Similarly, an offender subject to a restraining order not to come within a certain radius of a victim may be equipped with a location device **100** and the victim also equipped with a location device, preferably by simply installing the necessary software on a GPS enabled cellular phone. The system then tracks the mobile locations of both the offender and the victim and sends appropriate alerts to one or more of the victim, the offender, and monitoring officer. In addition, the present invention provides for the creation of reportable events that are not explicit violations of rules applicable to an offender, for instance by allowing the creation of buffer zones that are not strict inclusion or exclusion zones. As an example, an offender might be subject to a 500 foot exclusion order, that creates a 500 foot exclusion zone around the victim and the victim's home and place of work. The system permits the definition of a larger buffer zone, perhaps 1000 feet or a quarter mile in radius, and if the offender lingers in the expanded buffer zone beyond a user designated time period, perhaps thirty minutes or an hour, notification is sent to a monitoring officer or included in reports.

[00073] In an alternative mode of operation, when the system determines that an offender or subscriber is in close proximity to an exclusion zone or similar critical location, the system can order the device to operate autonomously to determine its location. In this mode of operation, the device becomes location aware by processing GPS coordinates and any assisted GPS information that it can obtain to determine its own geolocation, and it may also apply its own rule analysis to the determined location. This autonomous operating mode may also be implemented if the device loses contact with the system for a predetermined interval of time. As an alternative to switching a device to autonomous operation for performing onboard geolocation

SUBSTITUTE SHEET (RULE 26)

PCT/US2006/017678 RO/US 28/08/06

and rule analysis, the administrative hub might alternatively simply order the device to collect and transmit GPS and assisted GPS data with increased frequency.

[00074] Two optional features of the invention's geo coding databases also increase its effectiveness. The first of these is the ability of the geo coding database to allow the addition and publishing of custom information. So, for instance, as shown in Figure 10A, an address is added for an inclusion zone **321** which might be an offender's home address where he is required to remain throughout an evening curfew period. This information would typically be considered custom information to an offender monitoring service. However, if custom information is added by a subscriber to the system that would be of more widespread interest, such as the location of a probation office or a substance abuse treatment facility, or a roadway speed limit, the subscriber has the ability to publish that information so that those details will be available on the public geo coding databases available to all subscribers to the system. Of course, prior to allowing the publishing of information to the public database, there is a review for format compliance and accuracy. In addition, web crawlers are utilized to harvest information for additions to the public or master geo coding database. Web crawlers are directed to search for specified criteria and return a listing of proposed changes to existing geo coding data meeting the designated criteria, and potential additions to the geo coding data meeting the program criteria which are then reviewed and added by an efficient work process such as single click approval.

[00075] The second geo coding database feature that improves operability of the system is an auto correction aspect. Publicly available geo coding databases include numerous, usually minor, defects due to errors in data coding as well as the development of new subdivisions and new building construction. If the center point for an inclusion or exclusion zone or other critical location point is set incorrectly, it can lead to a number of false alerts. In prior art systems, when

a monitored offender generates an alert, the protocol has been for a call to be initiated to ask the offender to confirm his location and in the event of repeated erroneous alerts, to send a GPS reader out to the physical location to recalibrate the geo coding for that location. However, according to the invention, the administrative hub monitors new inclusion zones and other appropriate critical points for the first few days after their entry into the system. If it is determined that an offender's apparent inhome time is not centered within an inclusion zone, the inclusion zone can be automatically recentered or recalibrated to the real location. This auto configuration is particularly useful for offender monitoring when there is an incorrect geo coding or a coding of a mailbox location instead of a house location for a particular address. Similarly, new construction sites may have only estimated geolocations and may require correction once construction has proceeded sufficiently. In another situation benefiting from auto correction, deliveries of shipments of goods that are being tracked may take place at a loading dock 100 yards or more from the coded geolocation of a facility. The ability to accurately track the transportation and delivery of goods to provide exception based reporting of route deviations combined with the ability to proactively optimize supply channel efficiencies, such as loading dock utilization and minimized waiting times for delivery, will further the goal of logistics managers to achieve complete, audited, unattended delivery.

[00076] Figure 10B illustrates inclusion and exclusion zones in operation. Specifically, an offender **350** is equipped with tracking device **100**. An officer **351** is also equipped with a communication device **353** which might be sending communications to an enabled device ranging in sophistication from a cell phone **23** to a laptop computer **22**, or the officer **351** may even be within a corrections facility **356** equipped with a work station **21** running web client **16**. Generally, the corrections facility **356** would be within an inclusion zone **355** to permit the

PCT/US2006/017678 RO/US 28/08/06

offender **350** to report for monthly probation officer meetings. In addition, the offender **350** would frequently be provided an inclusion zone **360** on workdays during work hours for his place of work. In some instances, the offender **350** would be allowed an inclusion area **365** for some leisure activities during selected hours, inclusion zone **370** for his place of residence and shopping needs, and if attending classes an inclusion zone **375** to attend school. An exclusion zone **380** would be established around the victim's home and possibly the victim's place of work. In addition, according to the present invention, victim **352** may carry a GPS enabled cell phone or other device running software according to the present invention and have a mobile exclusion zone **381** that moves with the victim's location. Thus, if the victim **352** were in one of the offender's **350** inclusion zones, then the system may generate notices to any of: the victim **352** to advise of the proximity of offender **350**; the offender **350** to advise that the usual inclusion zone is not currently permitted; or the officer **351** to alert the officer to the developing situation so that corrective action may be taken.

[00077] Figure 11 shows a useful management report **400** for a probation officer or other corrections official with monitoring responsibility. The report lists offender status by user defined criteria, and in the illustrated case those criteria are of zone violations, battery status and recharge scheduling, failure to call in when required, and strap tampering events.

[00078] Figure 12 shows the new offender data entry template **405** which is generated by the new offender item or manage offender menu **308**. As shown, the new offender template has tabbed **406**, **407** pages to permit the entry of personal information, charges, additional offender details and notifications. Adding new offenders is typically a user administrative function that may be accomplished over user web client **16** shown in Figure 1. From this description, it will be appreciated that several databases are employed in the operation of the system. For instance,

there is a database of devices that are being monitored by the system for their locations; there is a database of offenders, subscribers or assets that are associated with devices and rules associated with those offenders, subscribers or assets; there is a database of clients of the system and the users and user rights for each client; and there is a GPS map or location database that may be supplemented with additional information by clients and by selective purchases of data such as registered sex offender residence data.

[00079] Figure 13 shows a violation report which is produced from report menu **307**. After violation report activity is selected, the user selects the entities or offenders upon which the report is to be generated **411** and those entities are displayed **412**. The user also selects the interval **413** over which the violations are to be displayed. When the report is run **417**, text report **415** is generated. The report may be exported **416** to a digital file or document for use outside the monitoring and tracking system.

[00080] The report menu **307** also permits generation of device report **420** shown in Figure 14. From this report, the user can select active or nonactive devices **421** or both, and a report is generated showing device ID and type, such as an offender ankle bracelet, cellular phone, or the like, and other pertinent device information. A text report **422** can be generated, and the data in the report may be exported **423** to a digital file or document for use outside the tracking system.

[00081] The manage entity or offender menu **308** permits entity schedules to be edited. Figure 15 shows the edit schedule template **425** whereby utilizing tabs **426**, **427**, **428** offenders and their schedules may be selected and entries for particular days may be edited with event types **429**, which may be appointments or particular time periods for application of inclusion or exclusion zones. In the administration menu **310**, authorized administrative personnel may perform necessary updates such as managing various agency accounts, authorizing new agency or

company users, editing existing user information, adding new agency or company accounts and editing account information, and adding new devices or editing device information

[00082] Figure 16 displays an edit company report showing company notification defaults **430**. This allows the agency, such as a probation department subscribing to the service to designated parameters to the administrative hub **10** specifying communications methods **432** to be employed upon the occurrence of selected events **436** with respect to the agency **431**, to a responsible officer for a particular offender **435** and to a victim or other interested third party. Illustrated communication methods include by fax, pager, e-mail, and SMS text messaging, and messages may be sent immediately **433** and/or provided in summary **434**.

[00083] Figure 17 shows another administrative menu **310** section, that of the new user template **440**. The template collects system identification information such as user name and login password **441**; the user's role **442** within the company or agency which will define to some extent the user's rights to access various aspects of the system, with a company administrator or supervisor having a greater rights than a monitoring officer or dispatcher. User contact information **443** is also collected, and user preferences **444a**, **444b** may also be input.

[00084] The system provides for the monitoring of a wide variety of criteria. A wearable device **100** may be equipped with a transdermal sensor for offender alcohol monitoring and with a thermometer for body temperature readings. In addition, stationary reporting devices such as active RFID readers **20**, intrusion or smoke alarms may be placed in facilities **19** and generate signals to administrative hub **10**. Upon obtaining a message from such a fixed reporting device, the administrative hub can automatically direct certain actions and make appropriate notifications. For instance, a smoke alarm message could lead the administrative hub **10** to seek confirmation from user facility staff, and in the absence of rapid confirmation that there is no

problem, the appropriate fire department may be notified. An intrusion alarm may generate a call to a response network as described below. Similarly, a RFID reader **20** may signal warning that an offender is entering a restricted area and cause appropriate action to be taken. Patients in assisted living facilities may also be equipped with RFID tags that are read and generate messages to the administrative hub **10** that may cause nearby doors to be locked to prevent patients from leaving the building or entering restricted areas such as kitchen and maintenance facilities, while avoiding the need to maintain the facility in a heavily supervised or lockdown mode.

[00085] With reference to Figures 18 – 22, the operation of a response network useful primarily outside the offender monitoring marketplace may be explained. For instance, Figure 18 reflects the operation of the system with administrative hub **510** in connection with an individual subscriber running appropriate software to communicate with the system on cell phone **523** and subscribing to a security service with administrative node **501**, where the security service is communication with police dispatch node **503** over a virtual private network. When the subscriber with cell phone **523** encounters an alarm condition, as by holding down the numeral 9 on the cell phone **523** (see step 530 in Figure 22), the cell phone transmits a panic signal **531** to the administrative hub **510**. The administrative hub **510** automatically responds by causing the cell phone **523** to increase the frequency of its location transmission **532**. Accordingly, rather than generating a signal to collect GPS data and assisted GPS data from GPS satellites **517** and cellular radio towers **518** about every two to five minutes, ephemeral location data may be collected every 30 seconds and transmitted to administrative hub **510**. The administrative hub **510** or a location aggregator **513** will calculate the geolocation of the subscriber **533**. If the location is successfully determined **534**, and if that location is also the

location wherein the subscriber previously had a confirmed location **535**, then the security service node **501** will respond by dispatching aid to that physical location **536**. The dispatch may be a private guard service employed by a security service, or in cooperation with police authorities the security service may communicate from node **501** to police dispatch node **503** and a police unit may be dispatched to the location. Indeed, the dispatch alternatives are not limited to private security guards and official police dispatch, but the security service may contract with an entire response network which may include off-duty police personnel, police authorities not merely from a particular municipality, but also both federal and state police authorities, and police authorities from nearby counties and municipalities. In addition, paramedic and medical personnel and even qualified volunteers may form part of a response network. When these resources, as on-duty police authorities, off-duty police authorities, private security, and medical personnel, are available for use by response network, they will activate their tracking devices and will be subject to being monitored and plotted on location maps in near real time. When an event occurs, the security service collecting the alarm event is then able to determine the nearest responder with the appropriate training for the type of alarm condition, and then attempt to contact that responder and inform the responder of the location of the event. If the responder accepts the engagement, a predetermined fee will be paid (unless an on-duty police authority) and the fastest possible response should be achieved. Thus, it will be appreciated that if the subscriber alarm in Figure 22 was determined to be a medical alarm, paramedic or medical personnel would be dispatched rather than police authorities.

[00086] Returning to Figure 22, however, if the location is determined for the alarm is not at the subscriber's previous confirmed location but it is near or inside a community protected by a security service **550**, then police authorities may be contacted and an agent responsible for

community protection may be contacted **551**. In addition, appropriate messages are sent to distribution lists appropriate to the type of event and the location **537, 552**. Messages may be sent as text messages, faxes, emails or voice calls, depending upon the urgency and device-types of the users to whom the messages are being sent. The subscriber is called or messaged when the appropriate action has been implemented **538, 553**. Logic also provides that if the location is not precisely determined, police or responders are dispatched to the best last known location **541, 544, 555**. Appropriate notifications are sent **542, 546**, and a subscriber is notified of the action being taken **543, 557**.

[00087] Figure 19 shows the integration of many users and services into the actions coordinated by administrative hub **510**. For a client or subscriber to services provided by administrative hub **510**, communication is by web enabled device **527** or cell phone **523**. Administrative users for a client define the authorized users, enroll devices and identify the rules and reporting protocols. In a real estate-centric application, survey information will be added to geo coding database, builders will add sensors to new buildings, real estate agents and contractors will be able to activate and deactivate alarm devices to suit their needs, and the administrative hub will maintain appropriate databases with a fully auditable record of events and produce appropriate billing information for clients.

[00088] Figure 20 shows a process for adding or removing sensors from a building, with a particular focus on new home building. First, builder will place a sensor at a home **560** and depress the 5 button on builder's cell phone **561**, that cell phone being a device enrolled with the administrative hub of the invention. The administrative hub receives the signal of the 5 button being depressed and location information is computed either autonomously by the cell phone or by a location aggregator or the administrative hub from ephemeral data. The administrative hub

first determines whether the location already has sensors installed **563** and allows the builder to elect **564** whether to disable existing sensors at the location **565**. If the builder is not at a geolocation that is identified as a home site **570**, then an option is provided to exit **571** or to proceed to establish a location **572** and enter a identifying number **573** for the home site. If the builder is authorized to place sensors at the site **575**, then the builder will need to provide the serial numbers of the sensors associated with the location **577**, and the sensors will be enabled **578**. If the builder is not in an area where he is authorized to enable sensors, he will be so notified **576**.

[00089] Figure 21 demonstrates steps by which a real estate arriving at an alarmed property to show the property to a prospective purchaser, or a tradesman arriving to perform work at an alarmed property, may disarm the alarm while necessary to work and then the alarm be reactivated upon departure of the real estate agent or tradesman. For instance, the agent may position themselves at the building where the alarm is to be disarmed, and the 3 button on the agent's cell phone is depressed. The phone transmits the disarm function together with data upon which the location aggregator or administrative hub may determine the location of the phone **601**. If the administrative hub determines that the geolocation is not at a alarm protected building **602**, a notification is sent to that effect **603**, and it is requested that the identifying number of the building be entered **604**. If the geolocation coordinates are at a protected building, the administrative hub determines whether the requester has access to disarm **610**, and failing appropriate authority, a notification is sent **611**, and an auditable history is created for future reporting **612**. If the agent has authority to disarm the alarm sensor, then the building is disarmed and an appropriate history record created. The administrative hub then signals the requesting phone to increase the frequency of transmission of data for location determination **621**

SUBSTITUTE SHEET (RULE 26)

so that the administrative hub may determine when the agent has left the home in order to rearm the alarm system. After the building is disarmed **620**, text message is sent verifying that the alarm was disarmed **622**, and the message recorded for future reporting **623**.

[00090] With the frequent reporting of location information **621**, the administrative hub actively monitors the agent's location **624**. So long as the agent is still at the location of the disarmed home **625**, the system takes no action **626**. However, once the agent is no longer at that location, the administrative hub rearms the sensors at the building **627**. Also at this time, the agent's phone is reset to original intervals for location reporting **626** and records are created of the time at which sensors were rearmed. If the agent or tradesperson remains in the building beyond a predetermined period of time, such as one or two hours, the administrative hub may request confirmation that the alarms be maintained in their disarmed status and failing confirmation of the need to maintain disarmed status, the alarms would then be reactivated.

[00091] Alternatively, the agent may depress another phone button such as 7 at the end of visit to an alarmed property, to create a signal back to the administrative hub to reactivate the home alarm system. Communication between the administrative hub and a home alarm system is typically over a POTS connection, however, an appropriately configured home system may be communicated with by wireless communications or a fixed line IP connection.

[00092] While the invention has been explained with respect to particular embodiments, numerous other location aware reporting applications exist, such as reporting to judges or judicial personnel if they are in proximity to monitored offenders, or if monitored offenders are in proximity to their residence, or reporting to parents proximity to residences or physical locations of monitored or registered sex offenders.

PCT/US06/17678 28 August 2006 (28.08.2006)
RO/US 28/08/06

[00093] All publications, patents, and patent documents are incorporated by reference herein as though individually incorporated by reference. Although preferred embodiments of the present invention have been disclosed in detail herein, it will be understood that various substitutions and modifications may be made to the disclosed embodiment described herein without departing from the scope and spirit of the present invention as recited in the appended claims.

SUBSTITUTE SHEET (RULE 26)

Claims

I claim:

1. A monitoring system for monitoring the compliance of an individual with a set of prescribed rules comprising:

(a) a wireless personal tracking device carried by the individual;

(b) an administrative hub monitoring locations of the individual based upon data reported by the wireless personal tracking device, and having a location database and a database containing the set of prescribed rules applicable to the individual;

wherein at least one of the rules applicable to the individual is a mobile exclusion zone that moves corresponding to the location of a second wireless tracking device that is monitored by the administrative hub.

2. A monitoring system for monitoring the compliance of an individual with a set of prescribed rules comprising:

(a) a wireless personal tracking device carried by the individual;

(b) an administrative hub monitoring locations of the individual based upon data reported by the wireless personal tracking device, and having a location database and a database containing the set of prescribed rules applicable to the individual;

wherein at least one of the rules applicable to the individual is a mobile inclusion zone that moves corresponding to the location of a second wireless tracking device that is monitored by the administrative hub.

3. The monitoring system of claims 1 or 2 wherein a user of the monitoring system is notified upon the administrative hub determining that one of the prescribed rules has been violated.

4. The monitoring system of claim 3 wherein the user notification is by a recorded or synthesized voice message.

5. A monitoring system for monitoring the compliance of an individual with a set of prescribed rules comprising:

(a) a wireless personal tracking device carried by the individual;

(b) an administrative hub monitoring locations of the individual based upon data reported by the wireless personal tracking device, and having a location database and a database containing the set of prescribed rules applicable to the individual in addition to reportable events applicable to the individual;

(c) an event log created by the administrative hub that contains both violations of the prescribed rules and reportable events applicable to the individual.

6. The monitoring system of claim 5 wherein a reportable event includes the presence of the individual in a buffer zone.

7. A monitoring system for monitoring the compliance of an individual with a set of prescribed rules comprising:

(a) a wireless personal tracking device carried by the individual;

(b) an administrative hub monitoring locations of the individual based upon data reported by the wireless personal tracking device, and having a location database and a database containing the set of prescribed rules applicable to the individual, at least one of said prescribed rules being an inclusion zone for the individual;

wherein when the location of the individual in the inclusion zone is initially monitored over a defined period the reported locations are predominantly near a perimeter location of the inclusion zone, then the co-ordinates of the inclusion zone are automatically selected for

recalibration to the predominantly reported location.

8. The monitoring system of claim 7 wherein an administrator can efficiently approve the selected recalibration.

9. The monitoring system of claims 1, 2, or 7 wherein the wireless personal tracking device does not determine its location, but only transmits location related data to the administrative hub.

10. The monitoring system of claim 9 wherein the administrative hub may direct the wireless personal tracking device to determine its location autonomously.

11. The monitoring system of claim 10 wherein the administrative hub may direct the wireless tracking device to autonomously apply at least one of the prescribed rules for the individual.

12. A monitoring system for monitoring the compliance of a plurality of individuals with a set of prescribed rules for said individuals comprising:

(a) a first wireless personal tracking device having a first CPU running a real time operating system carried by a first individual;

(b) a second wireless personal tracking device having a second CPU running a virtual machine implementation of the first CPU carried by a second individual;

(c) an administrative hub monitoring locations based upon data reported by the first and second wireless personal tracking devices, and having a location database and a database containing the set of prescribed rules applicable to each of the first and the second individuals.

13. The monitoring system of claim 12 wherein a third wireless personal tracking device having a third CPU running a virtual machine implementation of the first CPU is carried by a third individual, the location of said third wireless personal tracking device also being monitored by the administrative hub.

14. The monitoring system of claim 12 wherein the second individual is notified when the

SUBSTITUTE SHEET (RULE 26)

first individual is within a specified proximity.

15. A monitoring system for monitoring compliance of individuals with associated sets of prescribed rules comprising:

(a) a first group of individuals each carrying a wireless personal tracking device;

(b) a second group of individuals each carrying a wireless personal tracking device;

(c) an administrative hub monitoring locations of the individuals in the first and second groups based upon data reported by the wireless personal tracking devices, and having at least one location database and a database containing the sets of prescribed rules applicable to the individuals;

(d) a first user authorized to access the locations of and data stored by the administrative hub pertaining to the individuals in the first group;

(e) a second user authorized to access the locations of and data stored by the administrative hub pertaining to the individuals in the second group;

wherein the first user is not authorized to access the locations of and data stored by the administrative hub pertaining to the individuals in the second group.

16. The monitoring system of claim 15 wherein the first user is authorized to modify the location database used by the administrative hub for monitoring locations of the individuals in the first group and applying the sets of prescribed rules applicable to those individuals, to create a set of first modifications applied to the location database.

17. The monitoring system of claim 16 wherein an administrator of the system is authorized to accept the modifications entered by the first user for general inclusion in a location database at the administrative hub.

18. The monitoring system of claim 15 wherein a web crawler is directed to search for specified criteria and returns data proposed for inclusion in a location database.

19. A monitoring system for monitoring the compliance of an individual with a set of prescribed rules comprising:

(a) a wireless personal tracking device carried by the individual;

(b) an administrative hub monitoring locations of the individual based upon data reported by the wireless personal tracking device, and having a location database and a database containing the set of prescribed rules applicable to the individual;

wherein the location database includes speed limit data for at least selected road segments, and at least one of the prescribed rules is for the individual to abide by speed limits.

20. A monitoring system for monitoring compliance of individuals with associated sets of prescribed rules comprising:

(a) a group of individuals each carrying a wireless personal tracking device;

(b) an administrative hub monitoring locations of the individuals in the group based upon data reported by the wireless personal tracking devices, and having at least one location database and a database containing the sets of prescribed rules applicable to the individuals;

(c) a user authorized to access the locations of and data stored by the administrative hub pertaining to the individuals in the group;

SUBSTITUTE SHEET (RULE 26)

(d) wherein the user may simultaneously display the location history of selected individuals in the group.

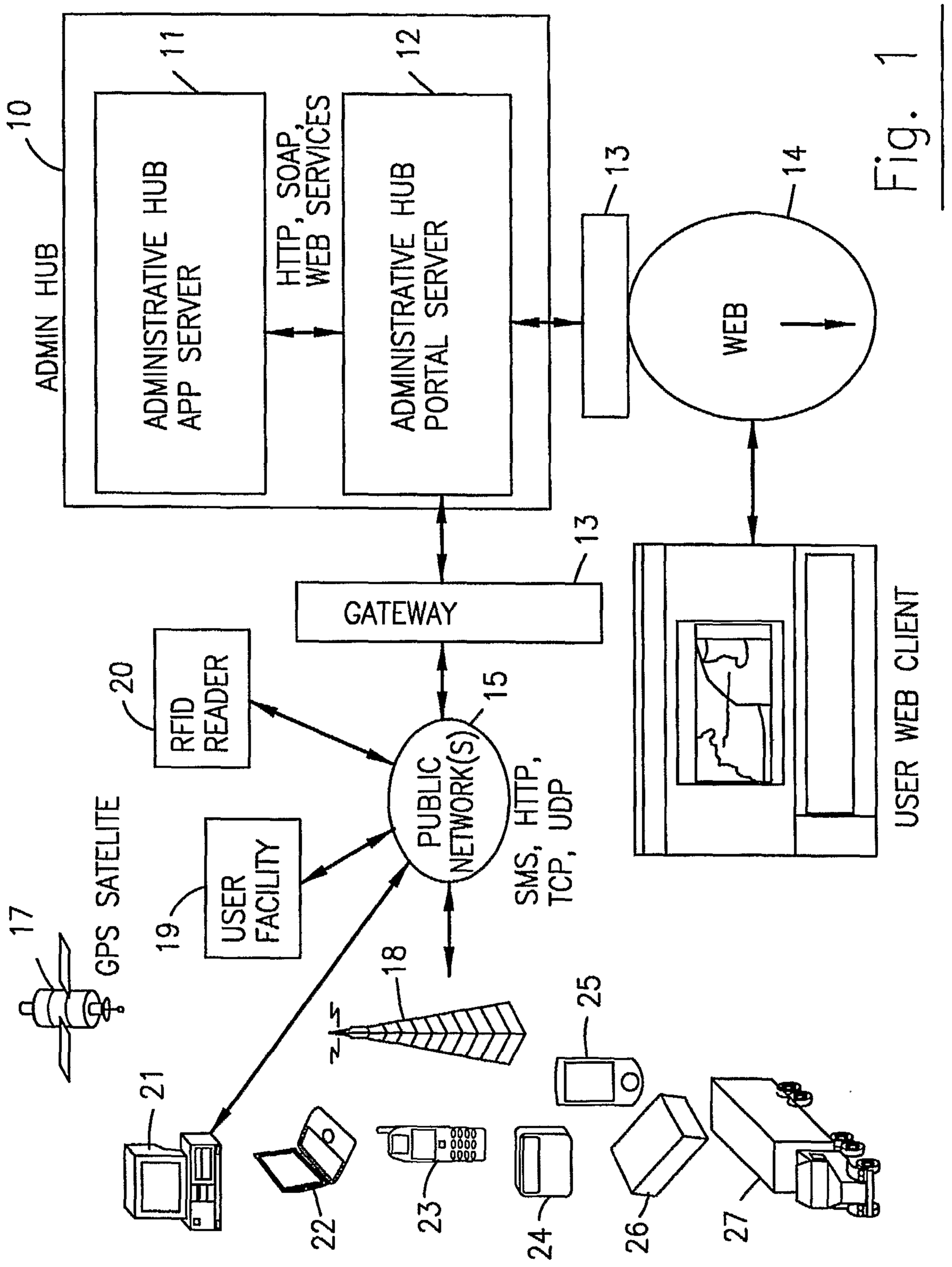

10
ADMIN HUB
11
ADMINISTRATIVE HUB APP SERVER
HTTP, SOAP, WEB SERVICES
12
ADMINISTRATIVE HUB PORTAL SERVER
13
GATEWAY
14
WEB
USER WEB CLIENT
15
PUBLIC NETWORK(S)
SMS, HTTP, TCP, UDP
20
RFID READER
19
USER FACILITY
17
GPS SATELITE
18
21
22
23
24
25
26
27

Fig. 1

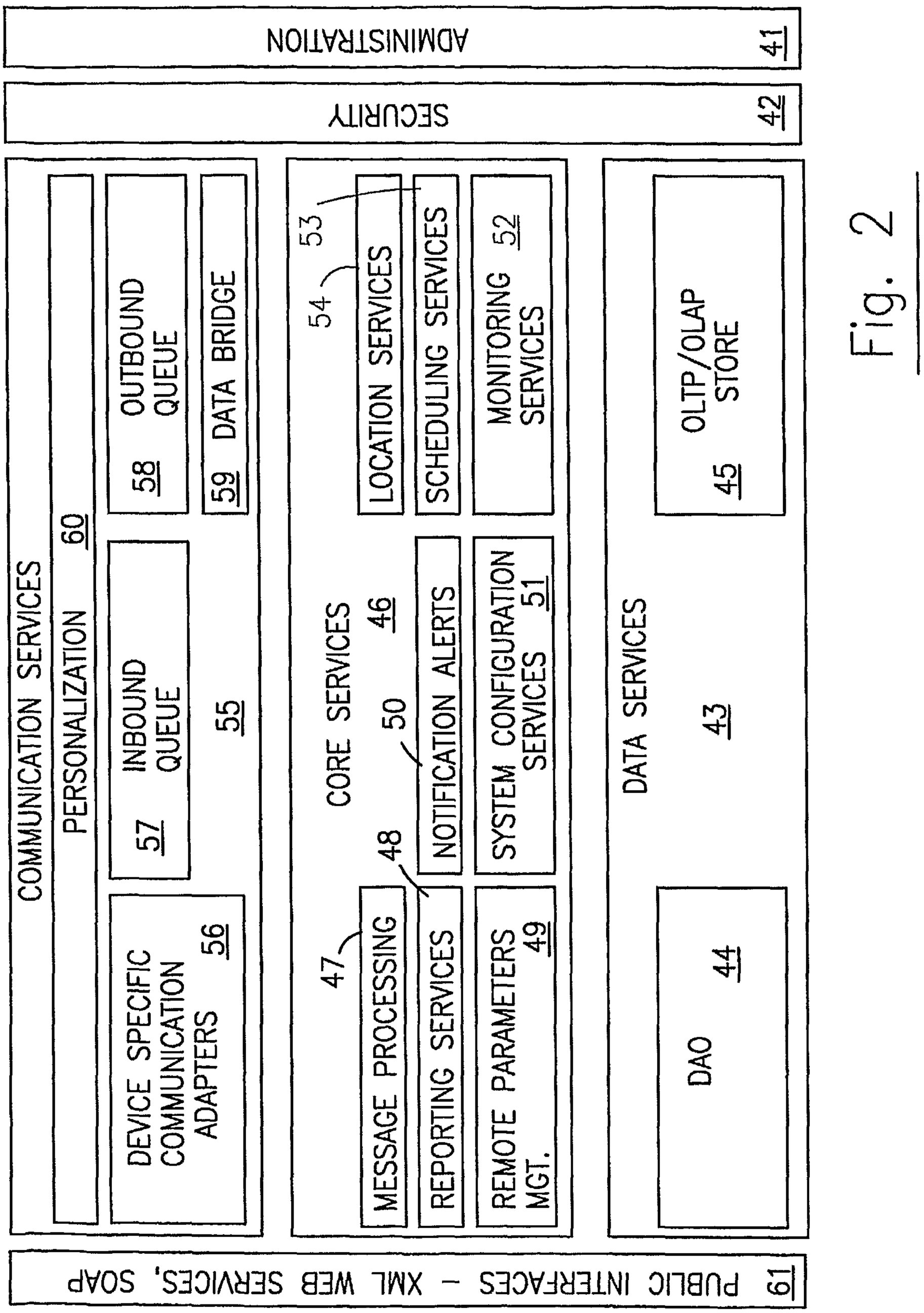

ADMINISTRATION 41
SECURITY 42
11
COMMUNICATION SERVICES
PERSONALIZATION 60
DEVICE SPECIFIC COMMUNICATION ADAPTERS 56
57 INBOUND QUEUE
58 OUTBOUND QUEUE
59 DATA BRIDGE
55
53
54
LOCATION SERVICES
SCHEDULING SERVICES
MONITORING SERVICES 52
CORE SERVICES 46
47
MESSAGE PROCESSING
48
50
NOTIFICATION ALERTS
REPORTING SERVICES
PARAMETERS 49
SYSTEM CONFIGURATION SERVICES 51
REMOTE MGT.
OLTP/OLAP STORE 45
DATA SERVICES
DAO 44
43
PUBLIC INTERFACES - XML WEB SERVICES, SOAP 61

Fig. 2

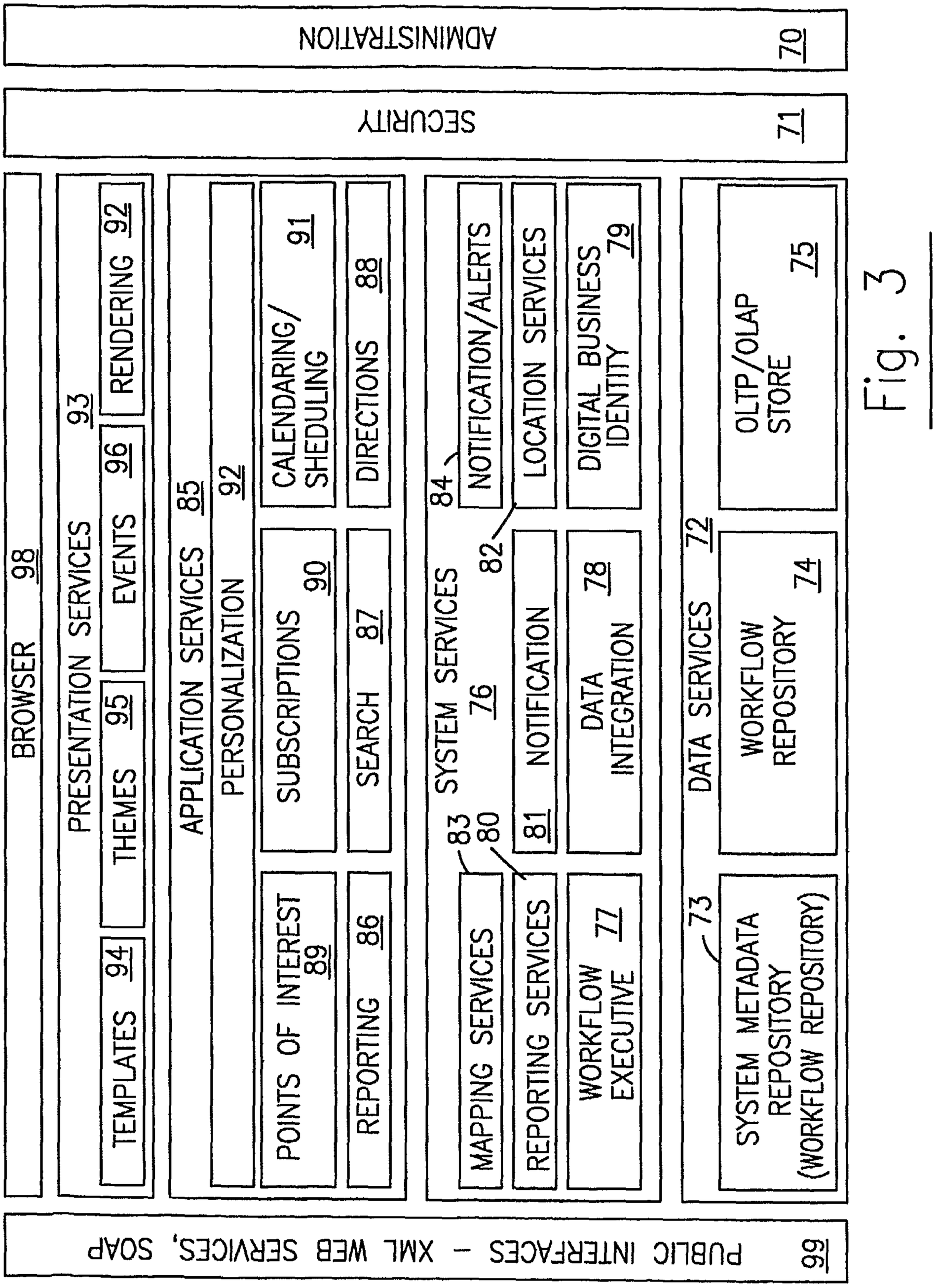

ADMINISTRATION 70
SECURITY 71
12
BROWSER 98
PRESENTATION SERVICES 93
TEMPLATES 94
THEMES 95
EVENTS 96
RENDERING 92
APPLICATION SERVICES 85
PERSONALIZATION 92
POINTS OF INTEREST 89
SUBSCRIPTIONS 90
REPORTING 86
SEARCH 87
CALENDARING/ SHEDULING 91
DIRECTIONS 88
SYSTEM SERVICES 76
MAPPING SERVICES 83
REPORTING SERVICES 81
WORKFLOW EXECUTIVE 77
NOTIFICATION 82
DATA INTEGRATION 78
84
NOTIFICATION/ALERTS
LOCATION SERVICES
DIGITAL BUSINESS IDENTITY 79
DATA SERVICES 72
SYSTEM METADATA REPOSITORY (WORKFLOW REPOSITORY) 73
WORKFLOW REPOSITORY 74
OLTP/OLAP STORE 75
PUBLIC INTERFACES - XML WEB SERVICES, SOAP 66

Fig. 3

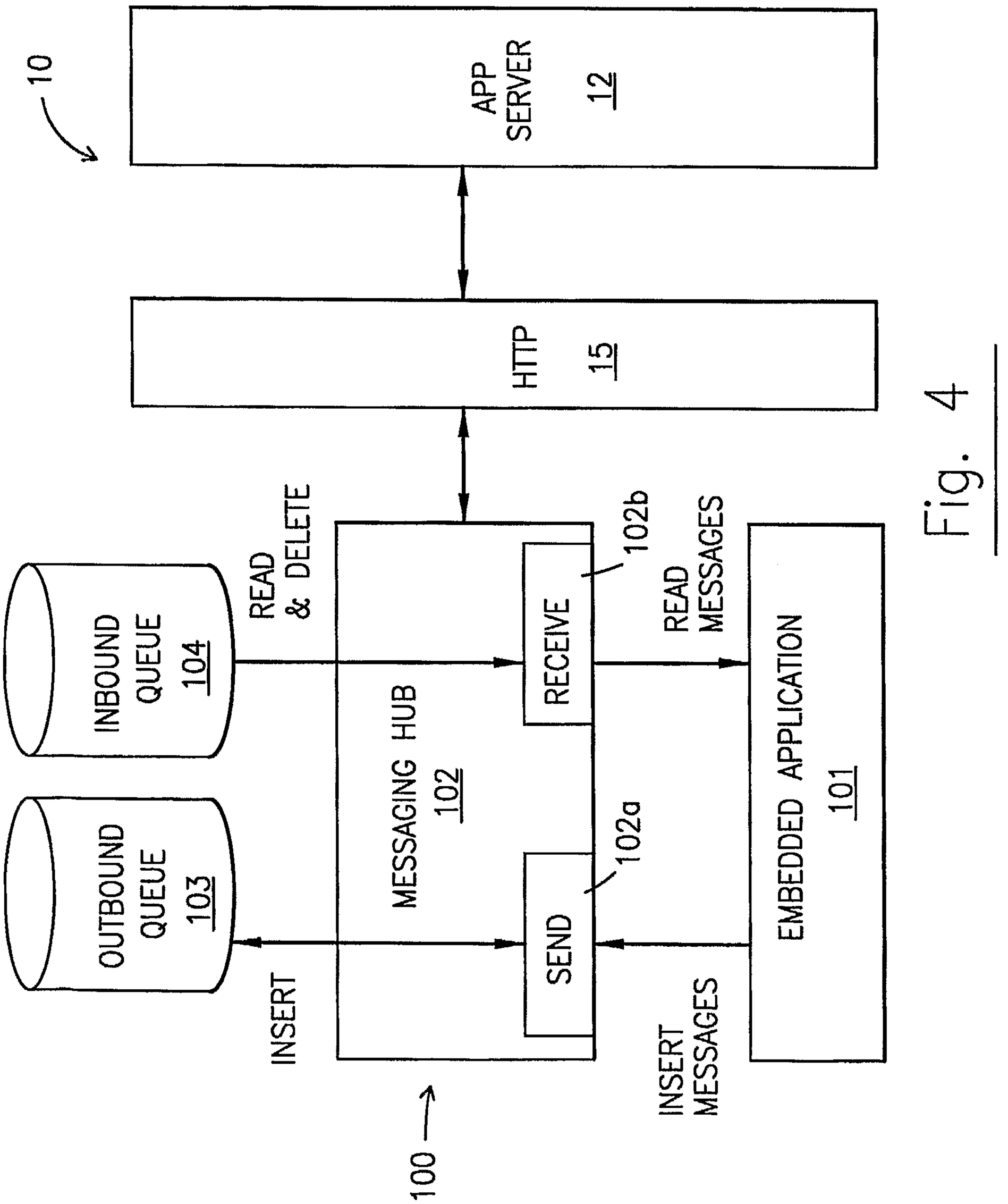

10
APP SERVER 12
HTTP 15
MESSAGING HUB 102
RECEIVE
102b
SEND
102a
READ & DELETE
INSERT
READ MESSAGES
INSERT MESSAGES
INBOUND QUEUE 104
OUTBOUND QUEUE 103
EMBEDDED APPLICATION 101
100

Fig. 4

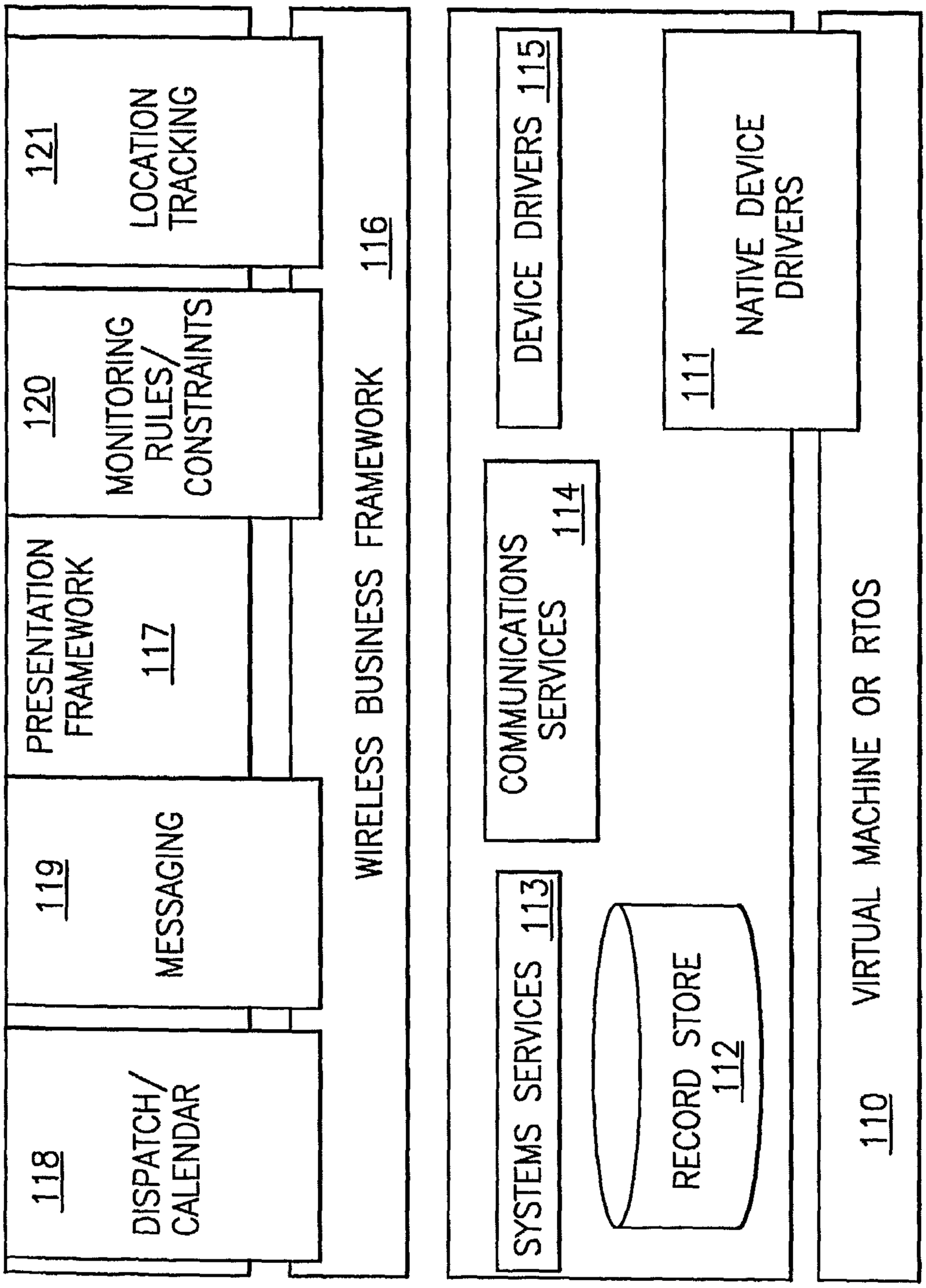

100
120
MONITORING RULES/ CONSTRAINTS
121
LOCATION TRACKING
116
WIRELESS BUSINESS FRAMEWORK
DEVICE DRIVERS 115
111
NATIVE DEVICE DRIVERS
COMMUNICATIONS SERVICES 114
SYSTEMS SERVICES 113
RECORD STORE 112
VIRTUAL MACHINE OR RTOS 110
119
MESSAGING
PRESENTATION FRAMEWORK 117
118
DISPATCH/ CALENDAR

Fig. 5

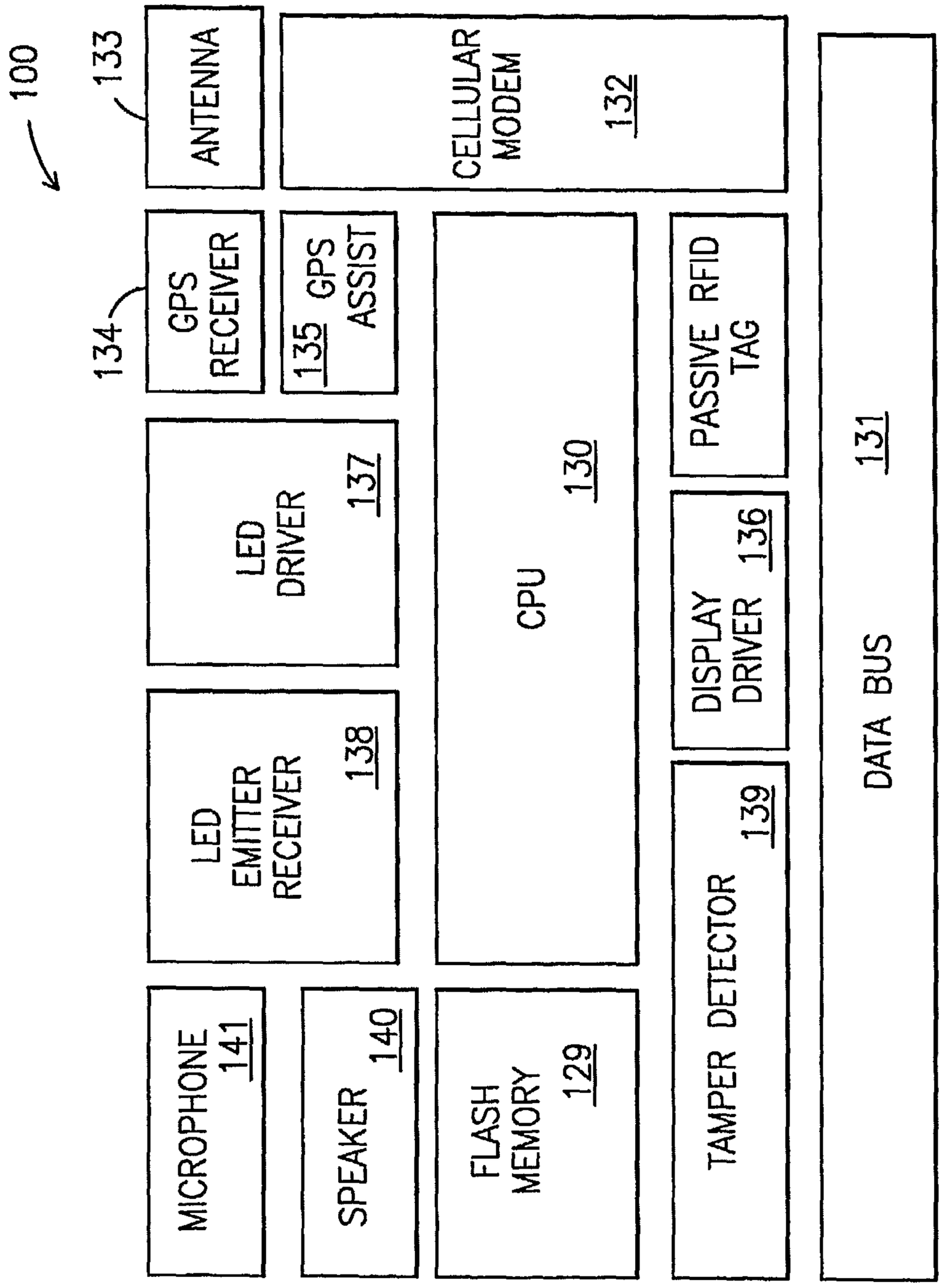

100
133
ANTENNA
CELLULAR MODEM
132
134
GPS RECEIVER
135 GPS ASSIST
LED DRIVER
137
CPU
130
PASSIVE RFID TAG
136
131
LED EMITTER RECEIVER
138
DISPLAY DRIVER
MICROPHONE
141
SPEAKER
140
FLASH MEMORY
129
TAMPER DETECTOR
139
DATA BUS

Fig. 6

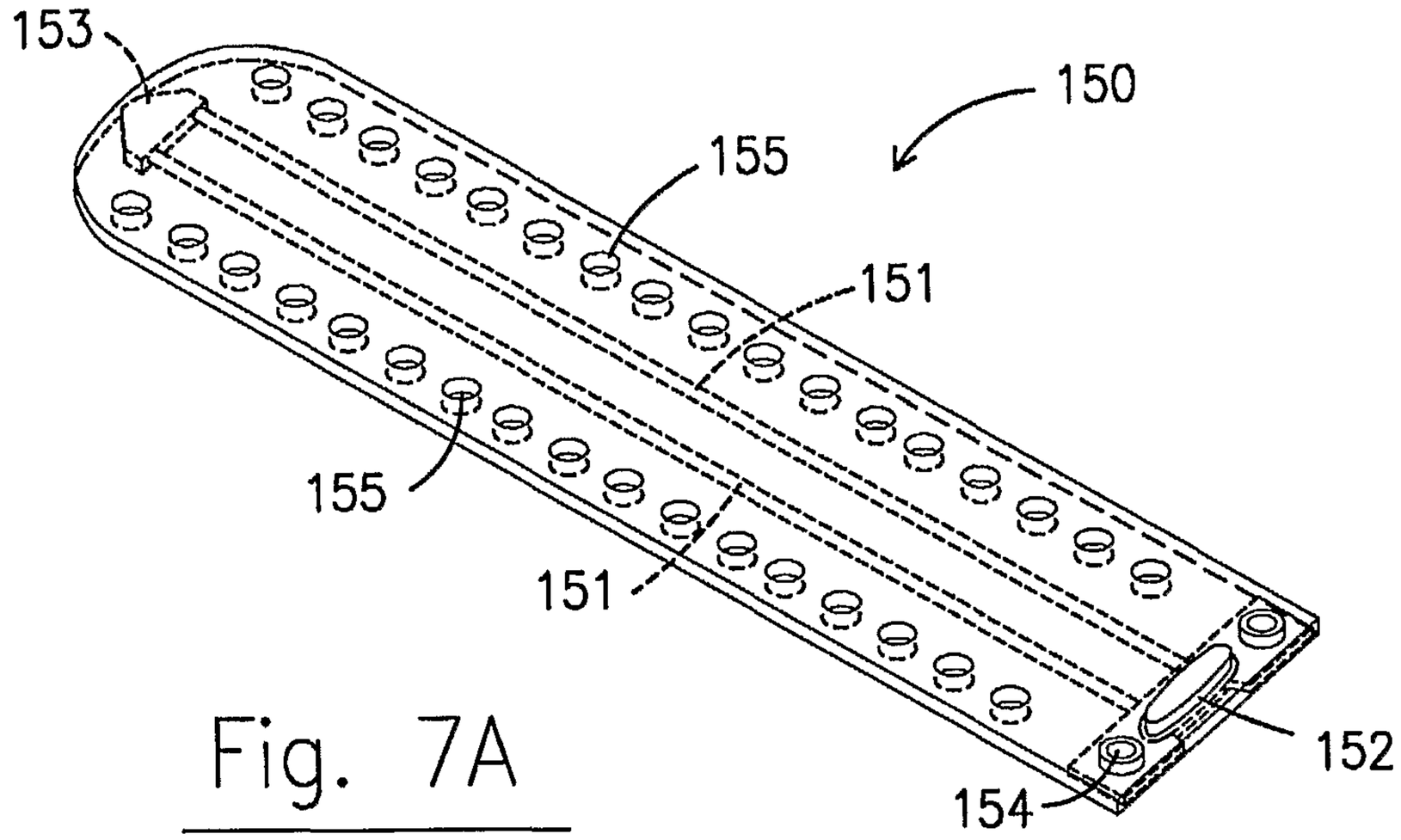

153
150
155
151
155
151
152
154

Fig. 7A

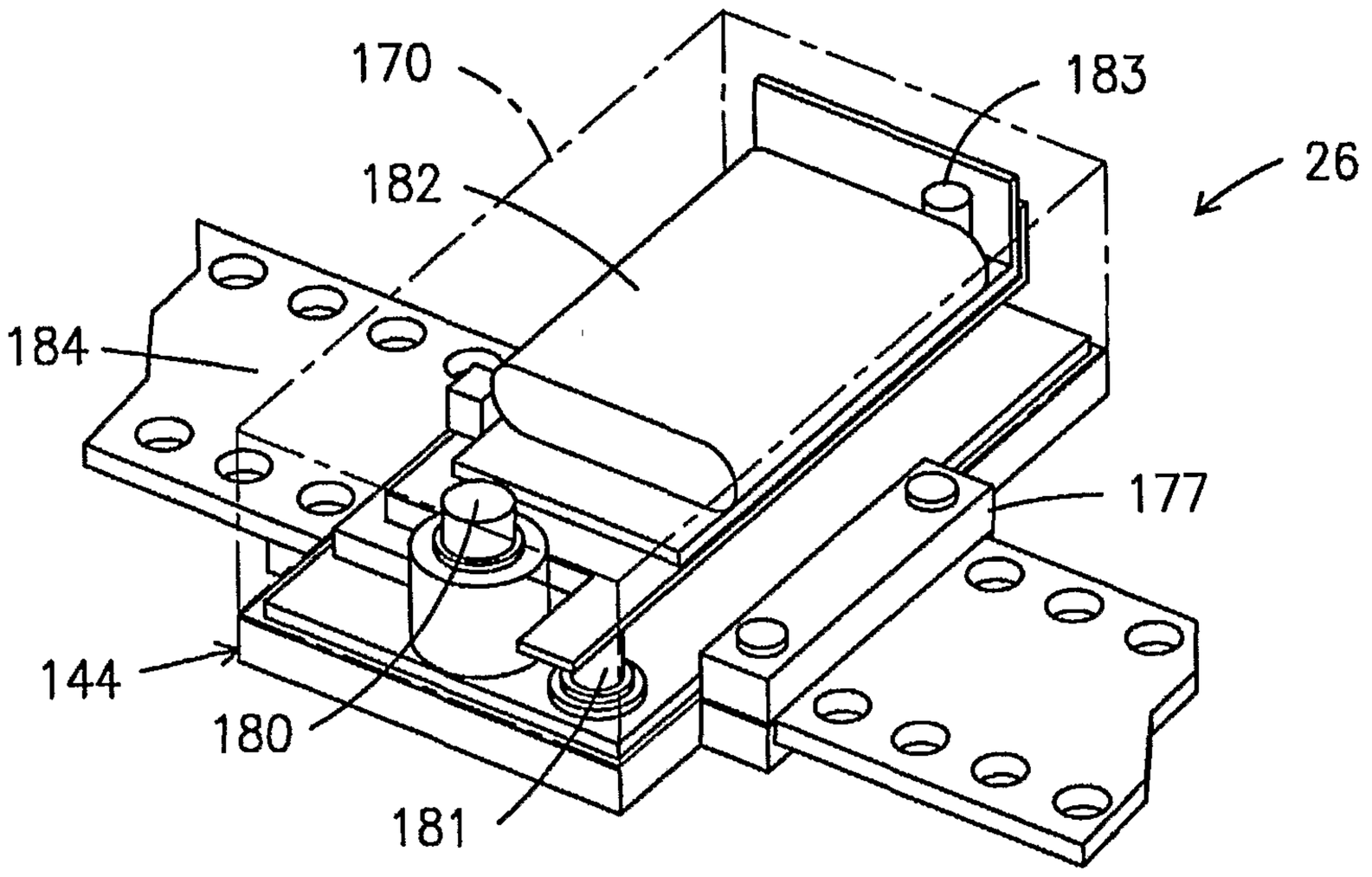

170
183
182
26
184
177
144
180
181

Fig. 7B

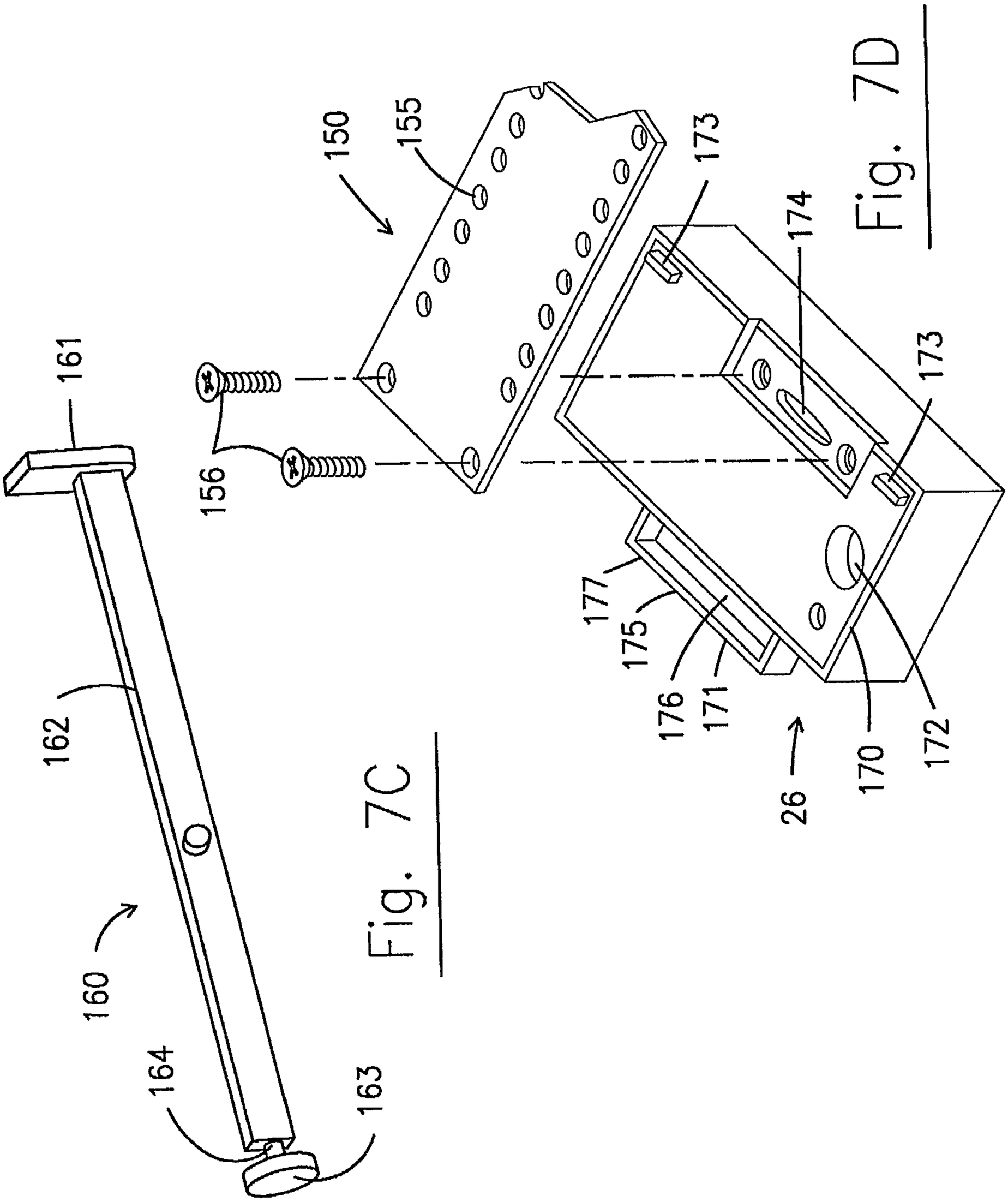

161
162
160
164
163
156
150
155
173
174
173
177
175
176
171
26
170
172

Fig. 7C

Fig. 7D

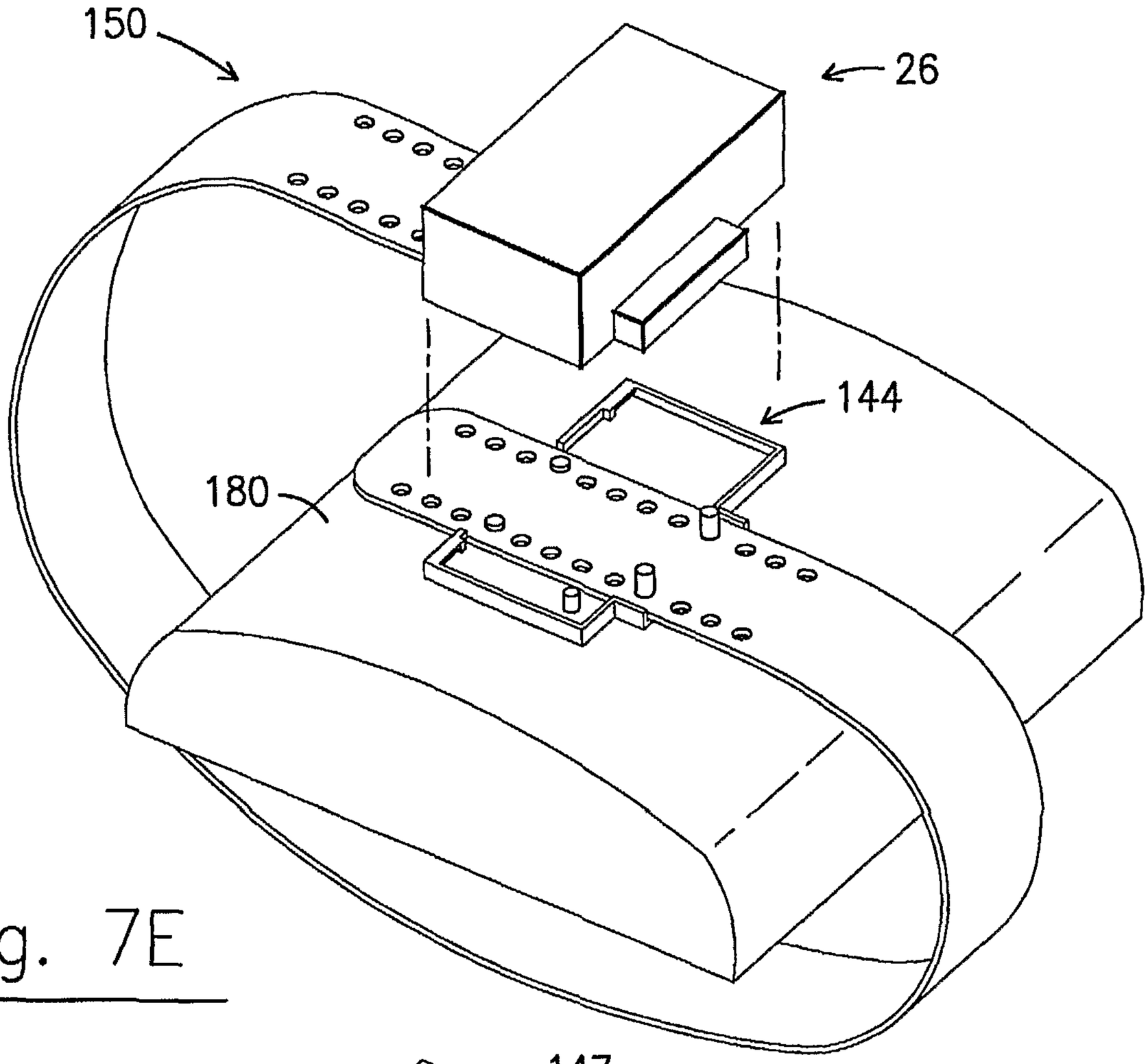


Fig. 7E

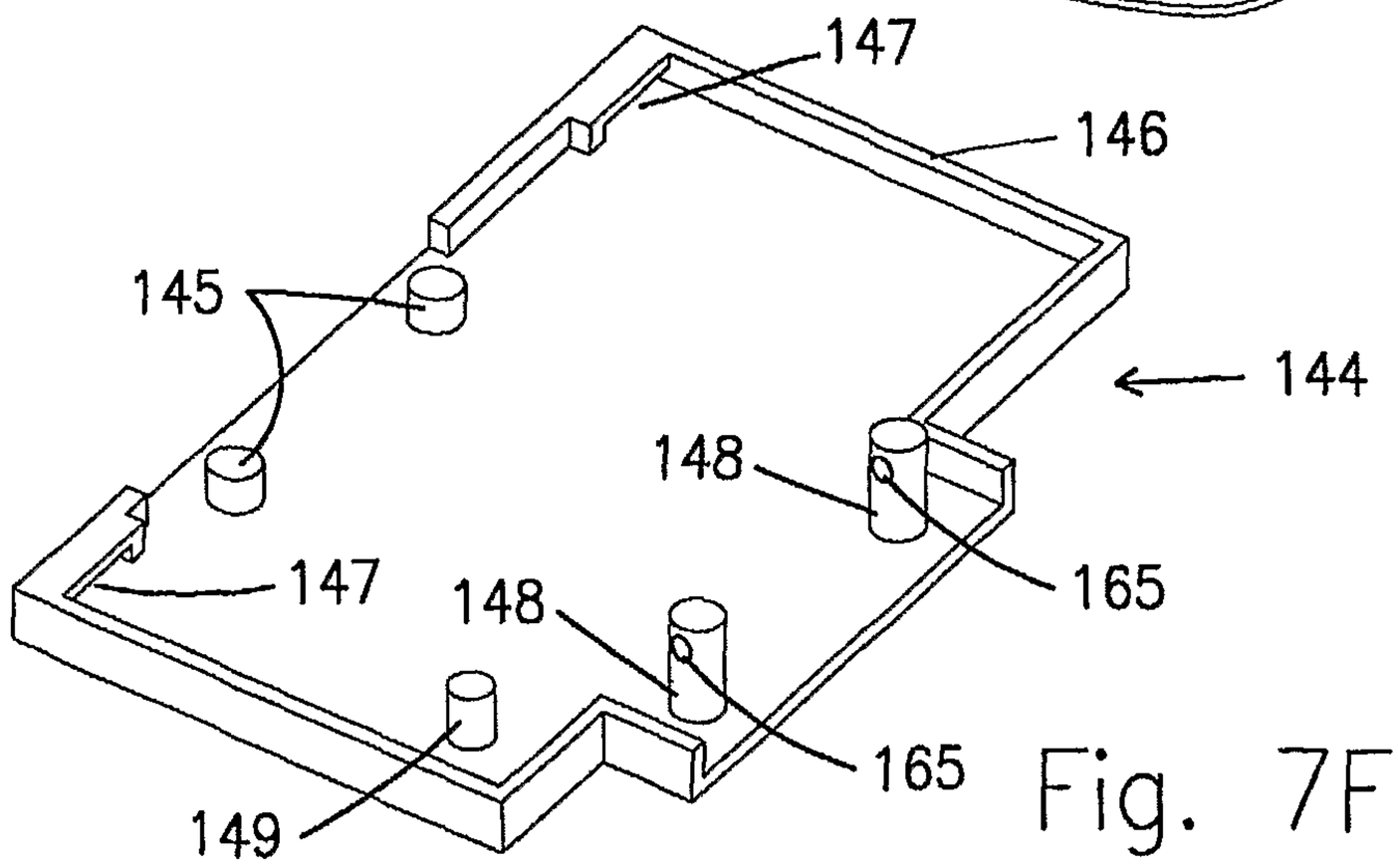


Fig. 7F

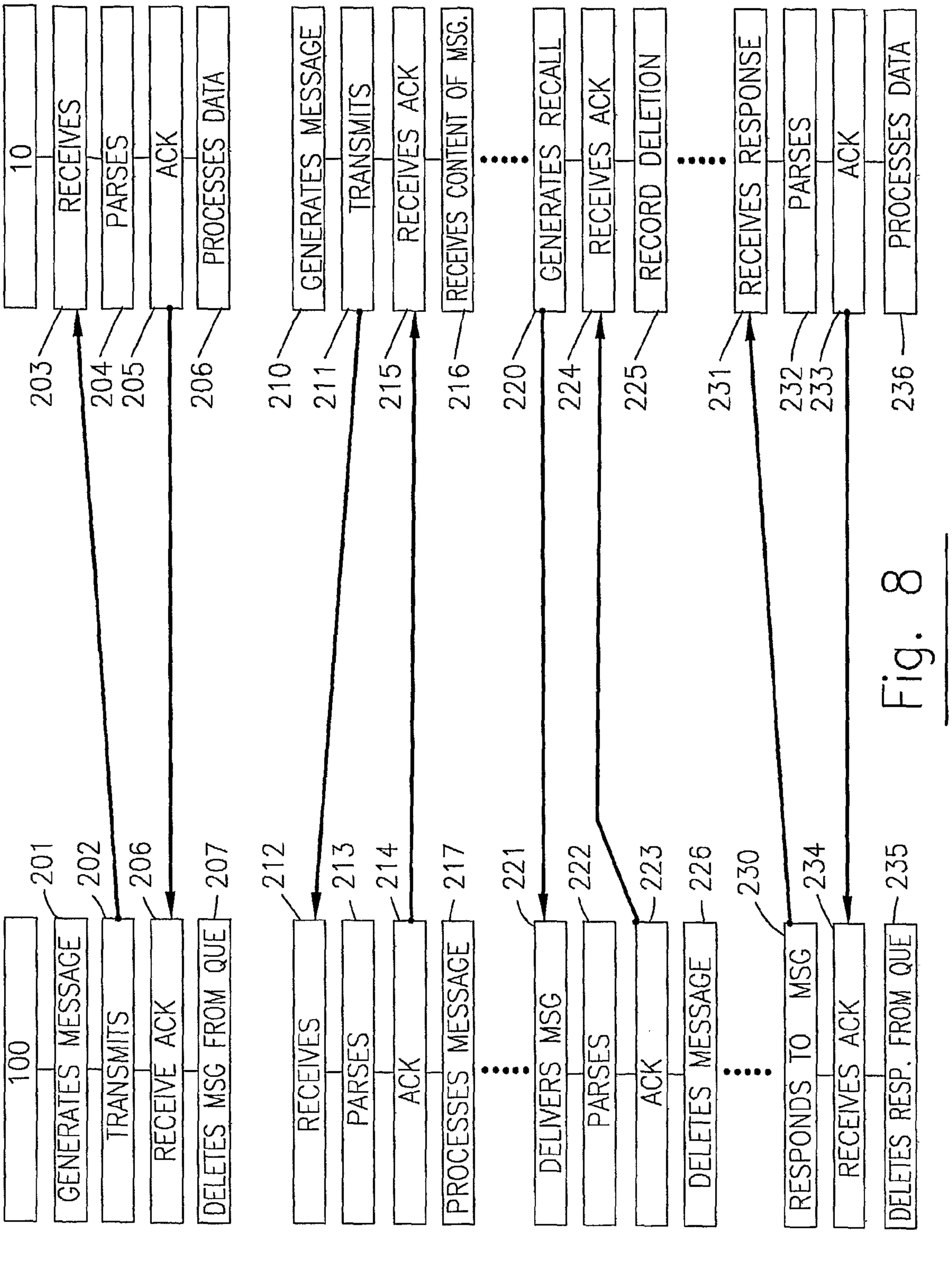

10
RECEIVES
PARSES
ACK
PROCESSES DATA
GENERATES MESSAGE
TRANSMITS
RECEIVES ACK
RECEIVES CONTENT OF MSG.
GENERATES RECALL
RECEIVES ACK
RECORD DELETION
RECEIVES RESPONSE
PARSES
ACK
PROCESSES DATA
203
204
205
206
210
211
215
216
220
224
225
231
232
233
236
100
GENERATES MESSAGE
TRANSMITS
RECEIVE ACK
DELETES MSG FROM Q
RECEIVES
PARSES
ACK
PROCESSES MESSAGE
DELIVERS MSG
PARSES
ACK
DELETES MESSAGE
RESPONDS TO MSG
RECEIVES ACK
DELETES RESP. FROM Q
201
202
206
207
212
213
214
217
221
222
223
226
230
234
235

Fig. 8

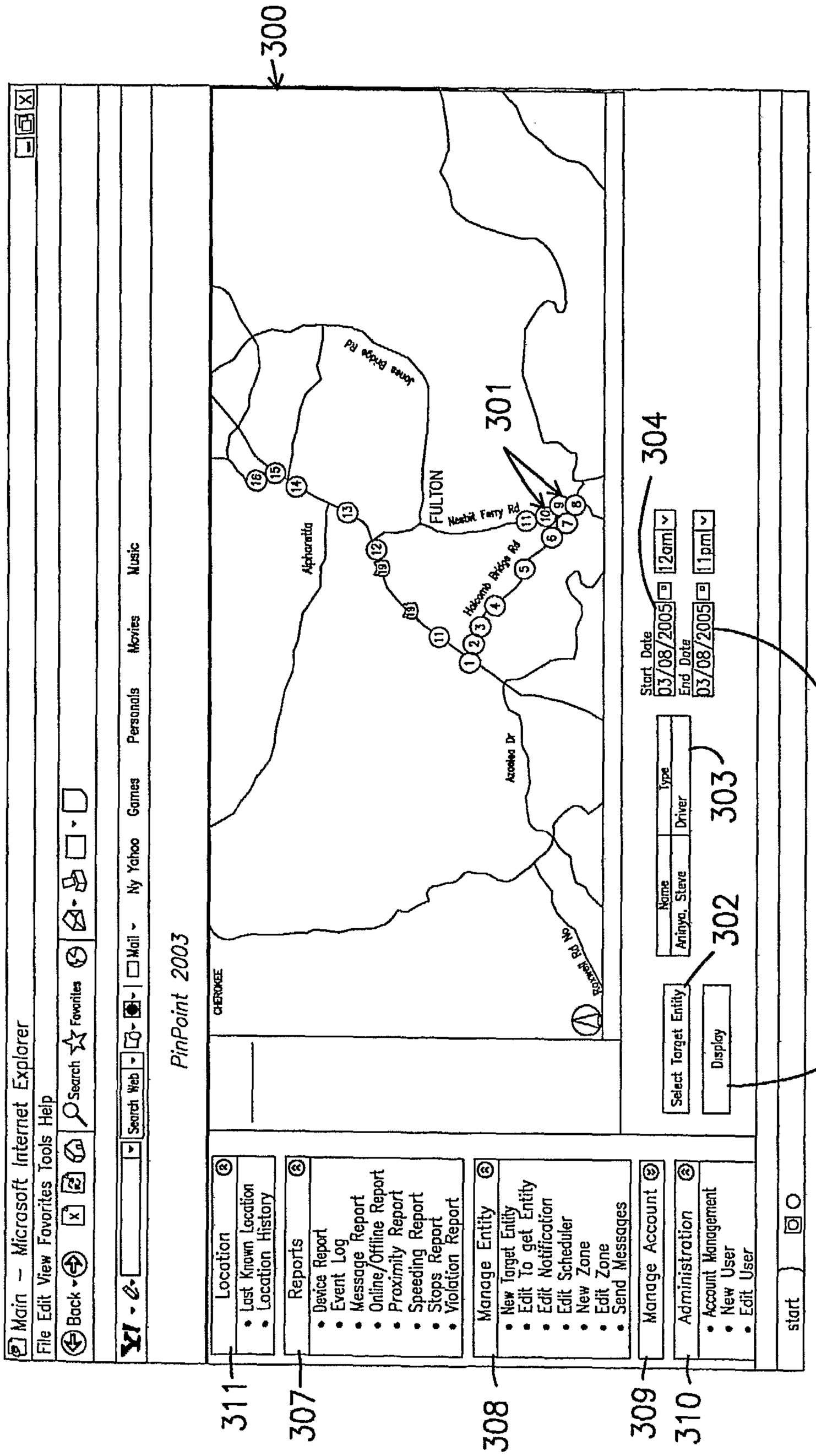
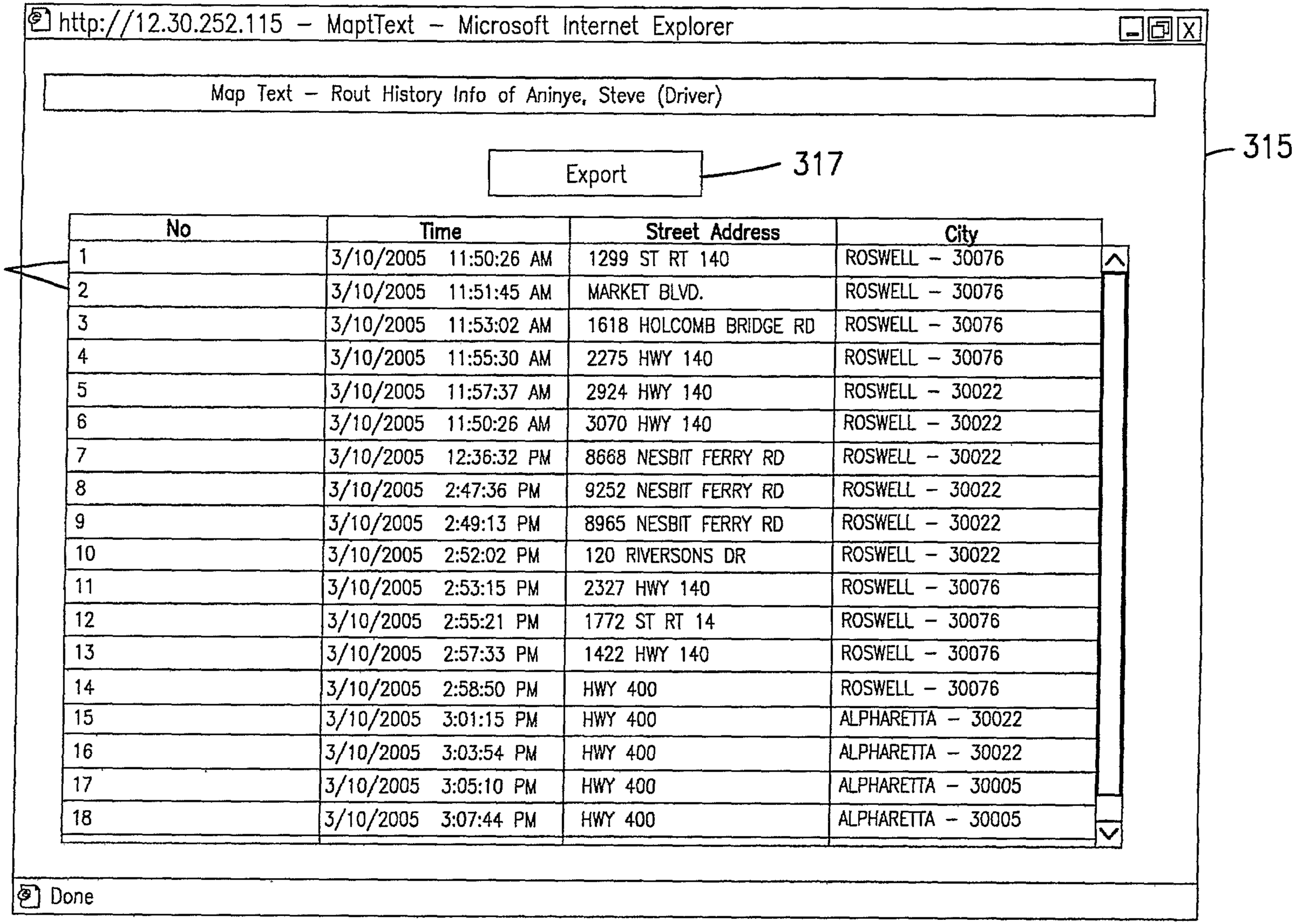

300
301
304
303
302
305
306
311
307
308
309
310
PinPoint 2003
Main - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Mail
My Yahoo
Games
Personals
Movies
Music
Search Web
FULTON
CHEROKEE
Alpharetta
Holcomb Bridge Rd
Azalea Dr
Start Date
03/08/2005
12am
End Date
03/08/2005
11pm
Name
Type
Aninya, Steve
Driver
Select Target Entity
Display
Location
Last Known Location
Location History
Reports
Device Report
Event Log
Message Report
Online/Offline Report
Proximity Report
Speeding Report
Stops Report
Violation Report
Manage Entity
New Target Entity
Edit To get Entity
Edit Notification
Edit Scheduler
New Zone
Edit Zone
Send Messages
Manage Account
Administration
Account Management
New User
Edit User
start

Fig. 9A



No	Time	Street Address	City
1	3/10/2005 11:50:26 AM	1299 ST RT 140	ROSWELL – 30076
2	3/10/2005 11:51:45 AM	MARKET BLVD.	ROSWELL – 30076
3	3/10/2005 11:53:02 AM	1618 HOLCOMB BRIDGE RD	ROSWELL – 30076
4	3/10/2005 11:55:30 AM	2275 HWY 140	ROSWELL – 30076
5	3/10/2005 11:57:37 AM	2924 HWY 140	ROSWELL – 30022
6	3/10/2005 11:50:26 AM	3070 HWY 140	ROSWELL – 30022
7	3/10/2005 12:36:32 PM	8668 NESBIT FERRY RD	ROSWELL – 30022
8	3/10/2005 2:47:36 PM	9252 NESBIT FERRY RD	ROSWELL – 30022
9	3/10/2005 2:49:13 PM	8965 NESBIT FERRY RD	ROSWELL – 30022
10	3/10/2005 2:52:02 PM	120 RIVERSONS DR	ROSWELL – 30022
11	3/10/2005 2:53:15 PM	2327 HWY 140	ROSWELL – 30076
12	3/10/2005 2:55:21 PM	1772 ST RT 14	ROSWELL – 30076
13	3/10/2005 2:57:33 PM	1422 HWY 140	ROSWELL – 30076
14	3/10/2005 2:58:50 PM	HWY 400	ROSWELL – 30076
15	3/10/2005 3:01:15 PM	HWY 400	ALPHARETTA – 30022
16	3/10/2005 3:03:54 PM	HWY 400	ALPHARETTA – 30022
17	3/10/2005 3:05:10 PM	HWY 400	ALPHARETTA – 30005
18	3/10/2005 3:07:44 PM	HWY 400	ALPHARETTA – 30005

Fig. 9B

SUBSTITUTE SHEET (RULE 26)

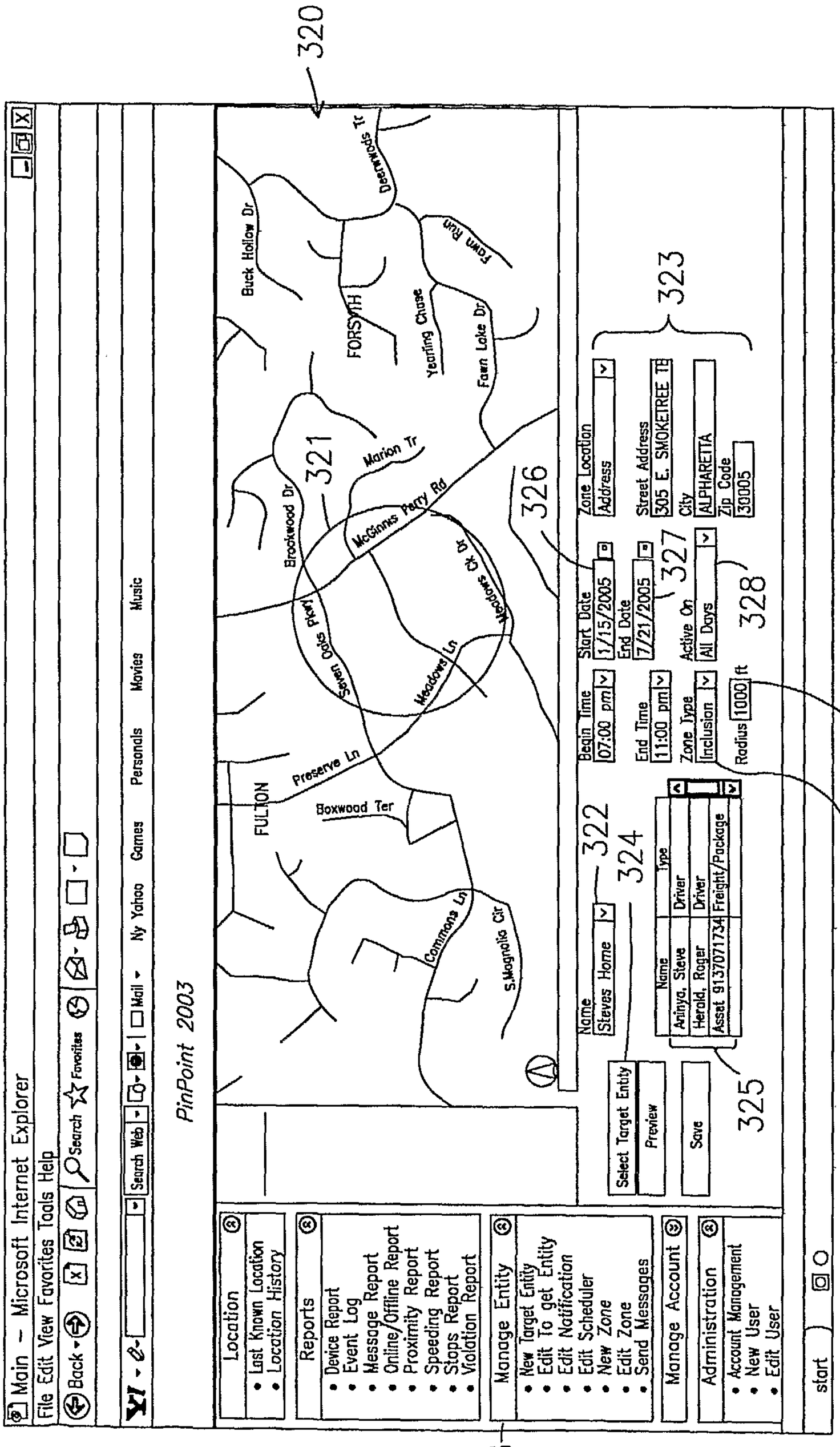

320
Main – Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Search Web
Mail
Ny Yahoo
Games
Personals
Movies
Music
PinPoint 2003
Buck Hollow Dr
FORSYTH
Deerwoods Tr
Yearling Chase
Fawn Run
Fawn Lake Dr
Brookwood Dr
321
Marion Tr
McGinnis Ferry Rd
Seven Oaks Pkwy
Meadows Ck Dr
Meadows Ln
326
FULTON
Preserve Ln
Boxwood Ter
Commons Ln
S.Magnolia Cir
322
324
325
323
327
328
329
330
Zone Location
Address
Street Address
305 E. SMOKETREE TE
City
ALPHARETTA
Zip Code
30005
Start Date
1/15/2005
End Date
7/21/2005
Active On
All Days
Begin Time
07:00 pm
End Time
11:00 pm
Zone Type
Inclusion
Radius
1000
ft
Name
Steves Home
Name
Type
Aninya, Steve
Driver
Herald, Roger
Driver
Asset 9137071734
Freight/Package
Select Target Entity
Preview
Save
Location
Last Known Location
Location History
Reports
Device Report
Event Log
Message Report
Online/Offline Report
Proximity Report
Speeding Report
Stops Report
Violation Report
Manage Entity
New Target Entity
Edit To get Entity
Edit Notification
Edit Scheduler
New Zone
Edit Zone
Send Messages
Manage Account
Administration
Account Management
New User
Edit User
start
308

Fig. 10A

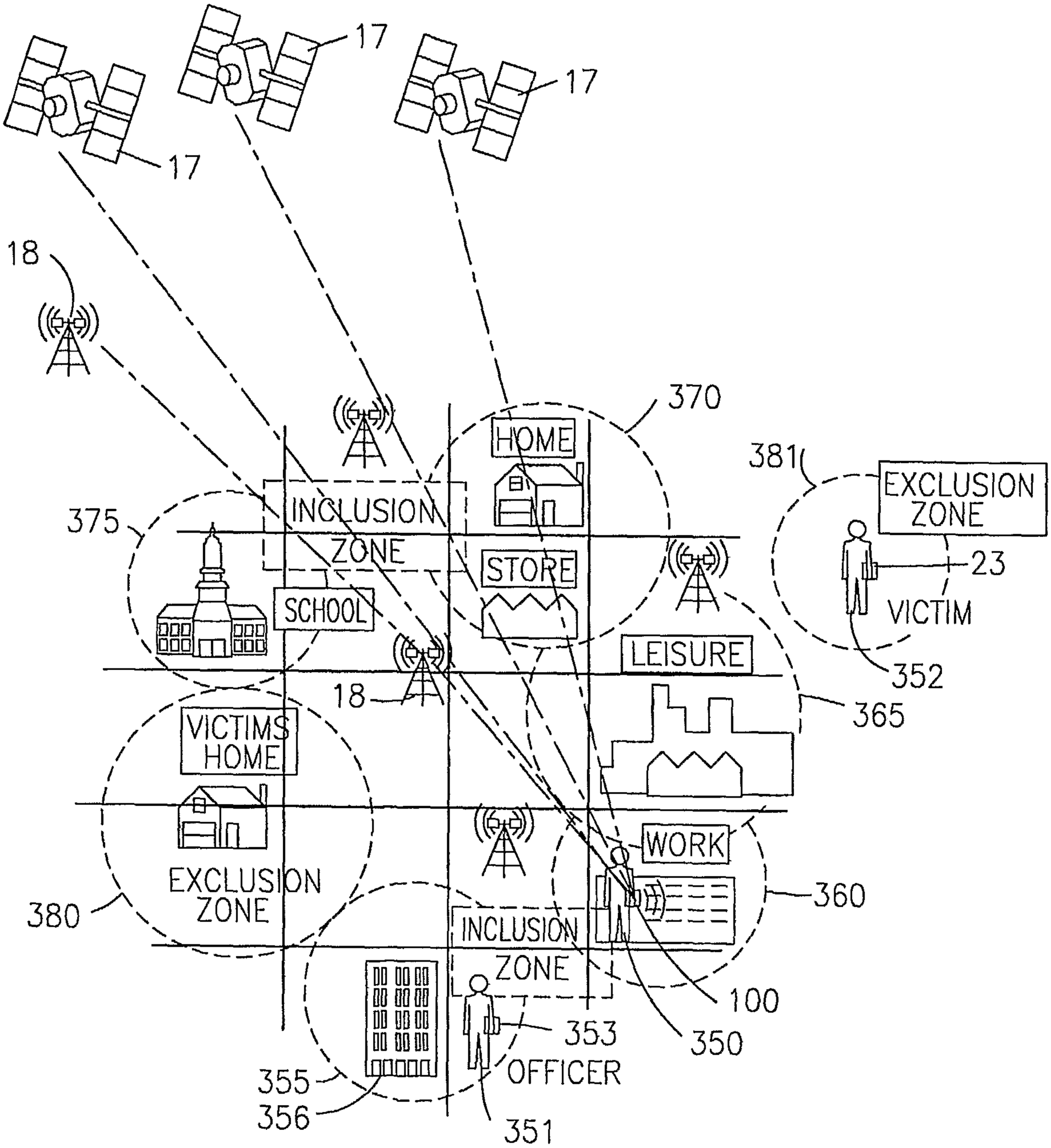

17
17
17
18
370
HOME
381
EXCLUSION ZONE
23
VICTIM
352
375
INCLUSION ZONE
STORE
SCHOOL
18
LEISURE
365
VICTIMS HOME
EXCLUSION ZONE
380
WORK
360
INCLUSION ZONE
100
353
OFFICER
350
355
356
351

Fig. 10B

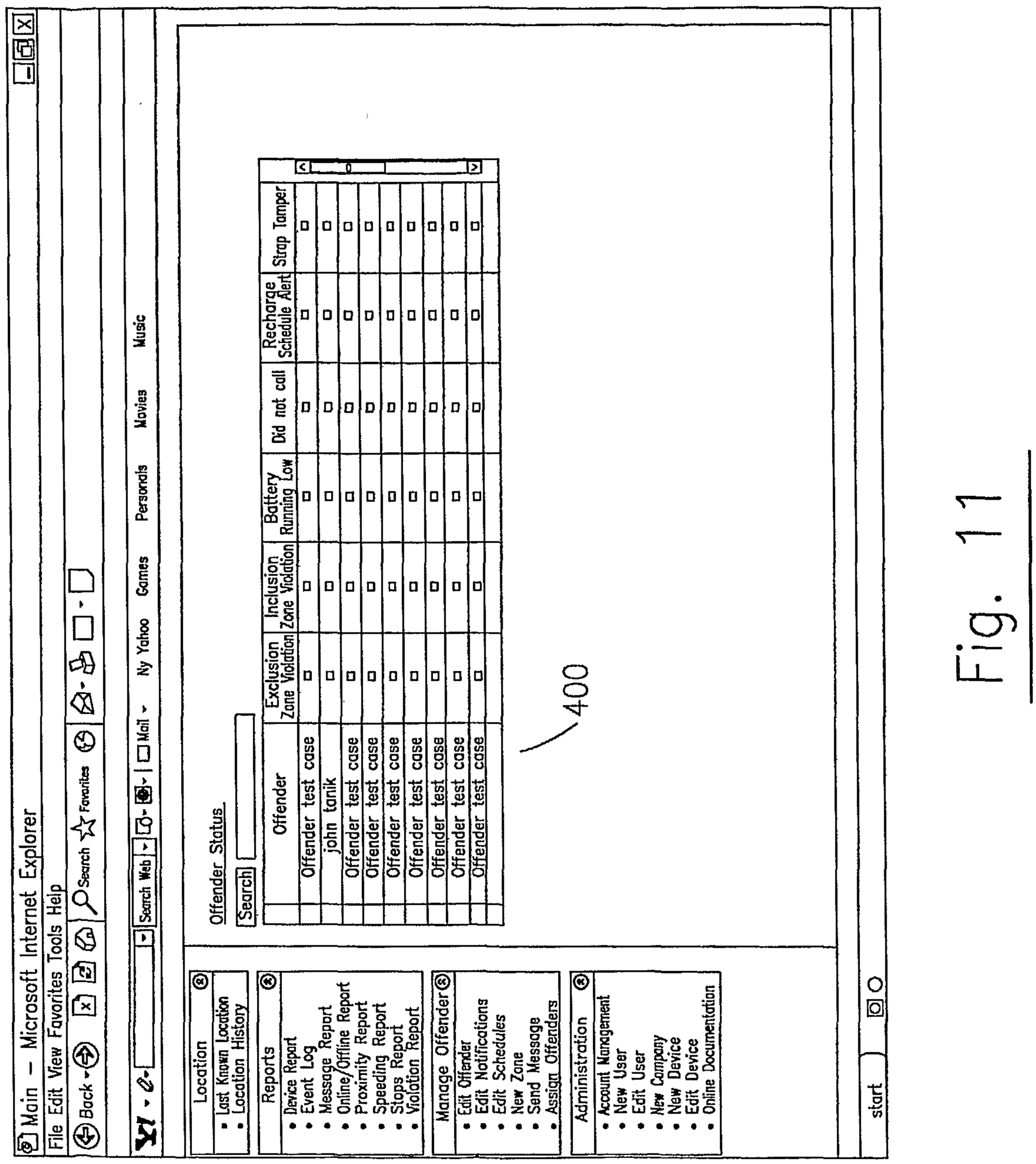

Main – Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Mail
Ny Yahoo
Games
Search Web
Personals
Movies
Music
Location
Last Known Location
Location History
Reports
Device Report
Event Log
Message Report
Online/Offline Report
Proximity Report
Speeding Report
Stops Report
Violation Report
Manage Offender
Edit Offender
Edit Notifications
Edit Schedules
New Zone
Send Message
Assign Offenders
Administration
Account Management
New User
Edit User
New Company
New Device
Edit Device
Online Documentation
Offender Status
Search
Offender
Exclusion Zone Violation
Inclusion Zone Violation
Recharge Schedule Alert
Strap Tamper
Did not call
Battery Running Low
Offender test case
john tanik
400
start

Fig. 11

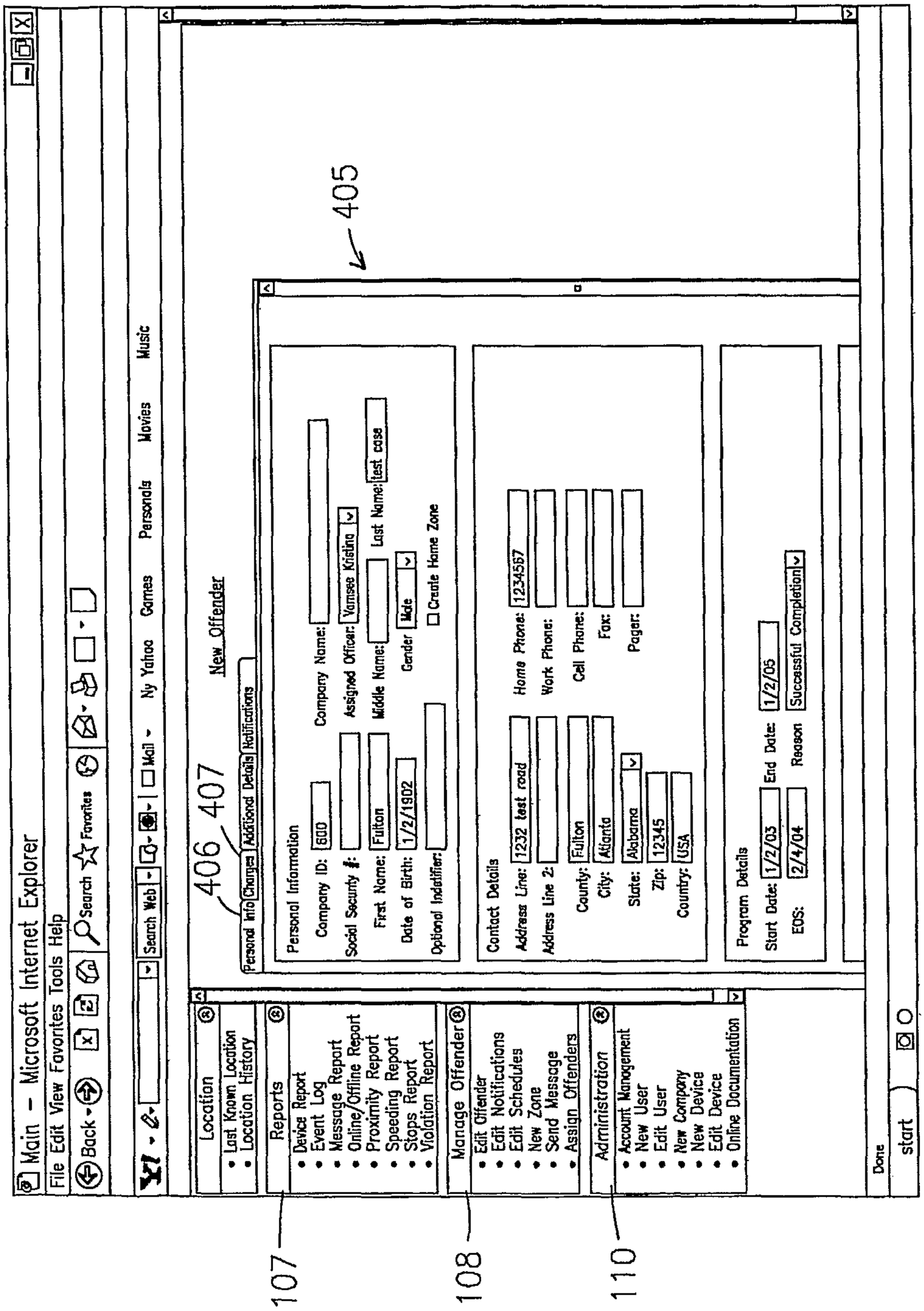

405
406
407
107
108
110
Main - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Search Web
Mail
Ny Yahoo
Games
Personals
Movies
Music
New Offender
Personal Info
Charges
Additional Details
Notifications
Location
Last Known Location
Location History
Reports
Device Report
Event Log
Message Report
Online/Offline Report
Proximity Report
Speeding Report
Stops Report
Violation Report
Manage Offender
Edit Offender
Edit Notifications
Edit Schedules
New Zone
Send Message
Assign Offenders
Administration
Account Management
New User
Edit User
New Company
New Device
Edit Device
Online Documentation
Personal Information
Company ID: 600
Company Name:
Social Security #:
Assigned Officer: Vansee Kristina
First Name: Fulton
Middle Name:
Last Name: test case
Date of Birth: 1/2/1902
Gender: Male
Optional Indatifier:
Create Home Zone
Contact Details
Address Line: 1232 test road
Address Line 2:
County: Fulton
City: Atlanta
State: Alabama
Zip: 12345
Country: USA
Home Phone: 1234567
Work Phone:
Cell Phone:
Fax:
Pager:
Program Details
Start Date: 1/2/05
End Date: 1/2/05
EOS: 2/4/04
Reason: Successful Completion
Done
start

Fig. 12

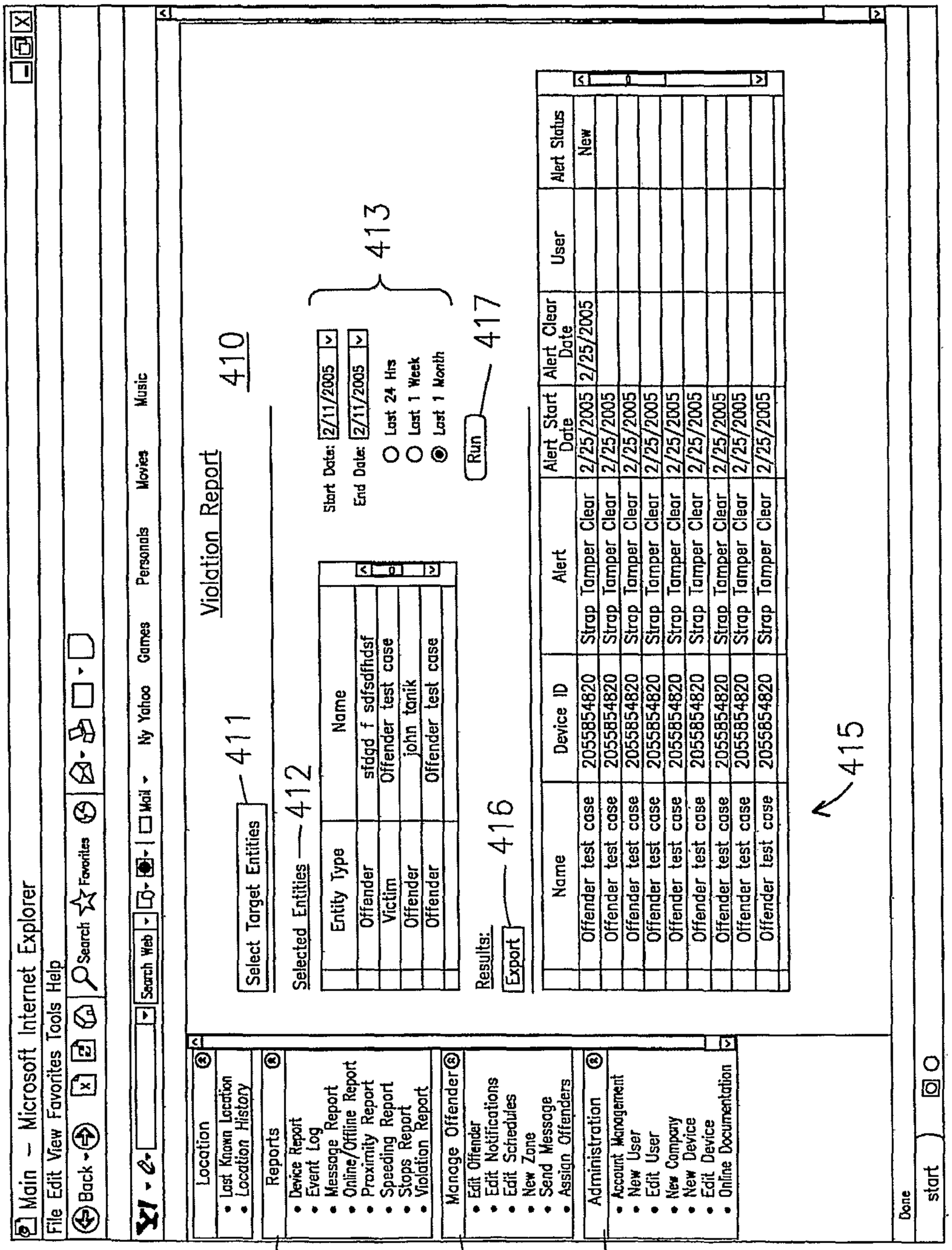

Violation Report
410
Start Date: 2/11/2005
End Date: 2/11/2005
Last 24 Hrs
Last 1 Week
Last 1 Month
413
Run
417
Select Target Entities
411
Selected Entities
412
Entity Type
Name
Offender
sfdgd f sdfsdfhdsf
Victim
Offender test case
Offender
john tanik
Offender
Offender test case
Results:
416
Export
Alert Start Date
Alert Clear Date
User
Alert Status
Clear
2/25/2005
New
Name
Device ID
Alert
Offender test case
2055854820
Strap Tamper Clear
415
Location
Last Known Location
Location History
Reports
Device Report
Event Log
Message Report
Online/Offline Report
Proximity Report
Speeding Report
Stops Report
Violation Report
Manage Offender
Edit Offender
Edit Notifications
Edit Schedules
New Zone
Send Message
Assign Offenders
Administration
Account Management
New User
Edit User
New Company
New Device
Edit Device
Online Documentation
307
308
310

Fig. 13

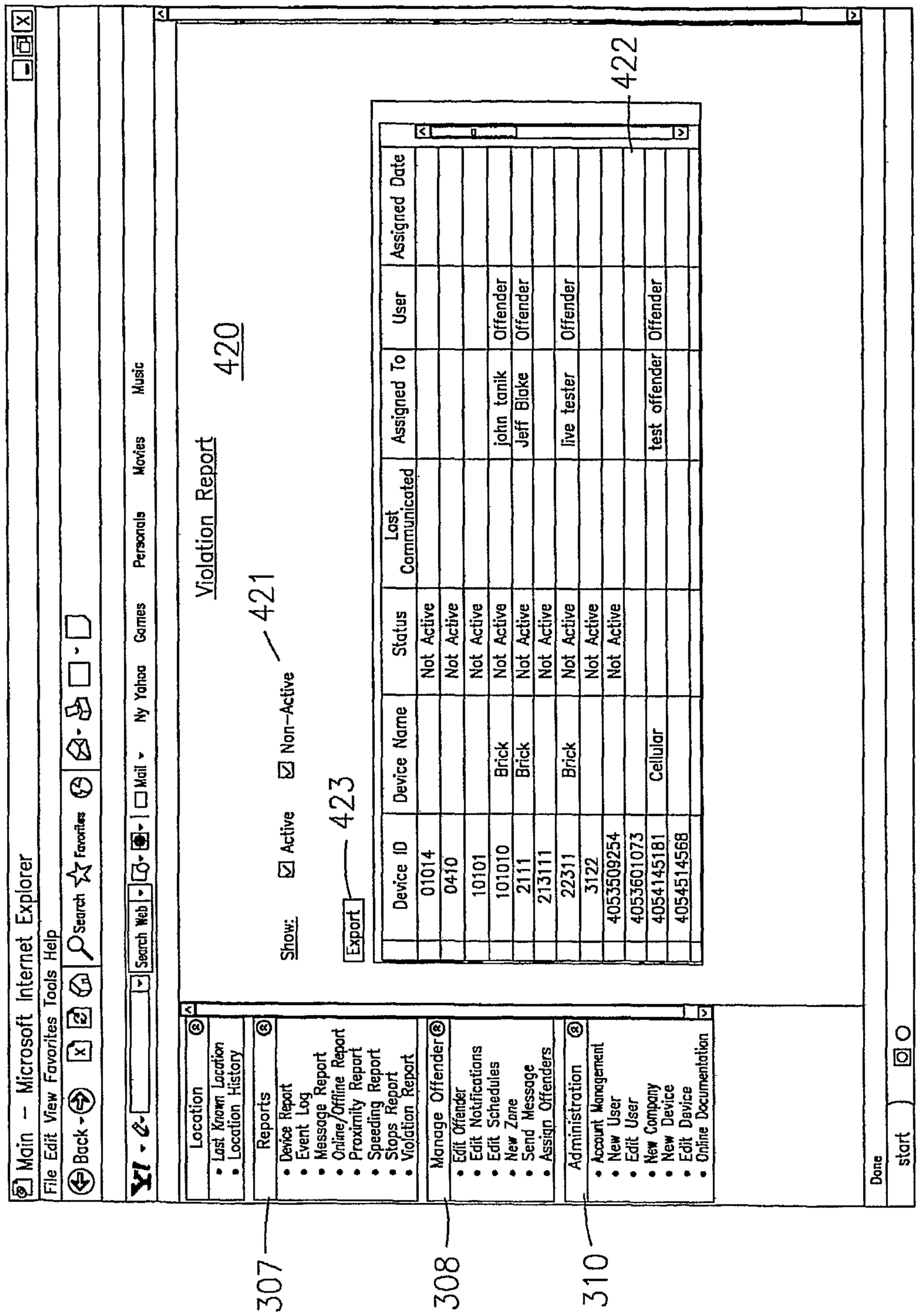

Main – Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Search Web
Mail
Ny Yahoo
Games
Personals
Movies
Music
Violation Report
420
421
422
Show:
Active
Non-Active
Export
423
Device ID
Device Name
Status
Last Communicated
Assigned To
User
Assigned Date
01014
0410
10101
101010
2111
213111
22311
3122
4053509254
4053601073
4054145181
4054514568
Brick
Cellular
john tanik
Jeff Blake
live tester
test offender
Offender
Location
Last Known Location
Location History
Reports
Device Report
Event Log
Message Report
Online/Offline Report
Proximity Report
Speeding Report
Stops Report
Violation Report
Manage Offender
Edit Offender
Edit Notifications
Edit Schedules
New Zone
Send Message
Assign Offenders
Administration
Account Management
New User
Edit User
New Company
New Device
Edit Device
Online Documentation
Done
start
307
308
310

Fig. 14

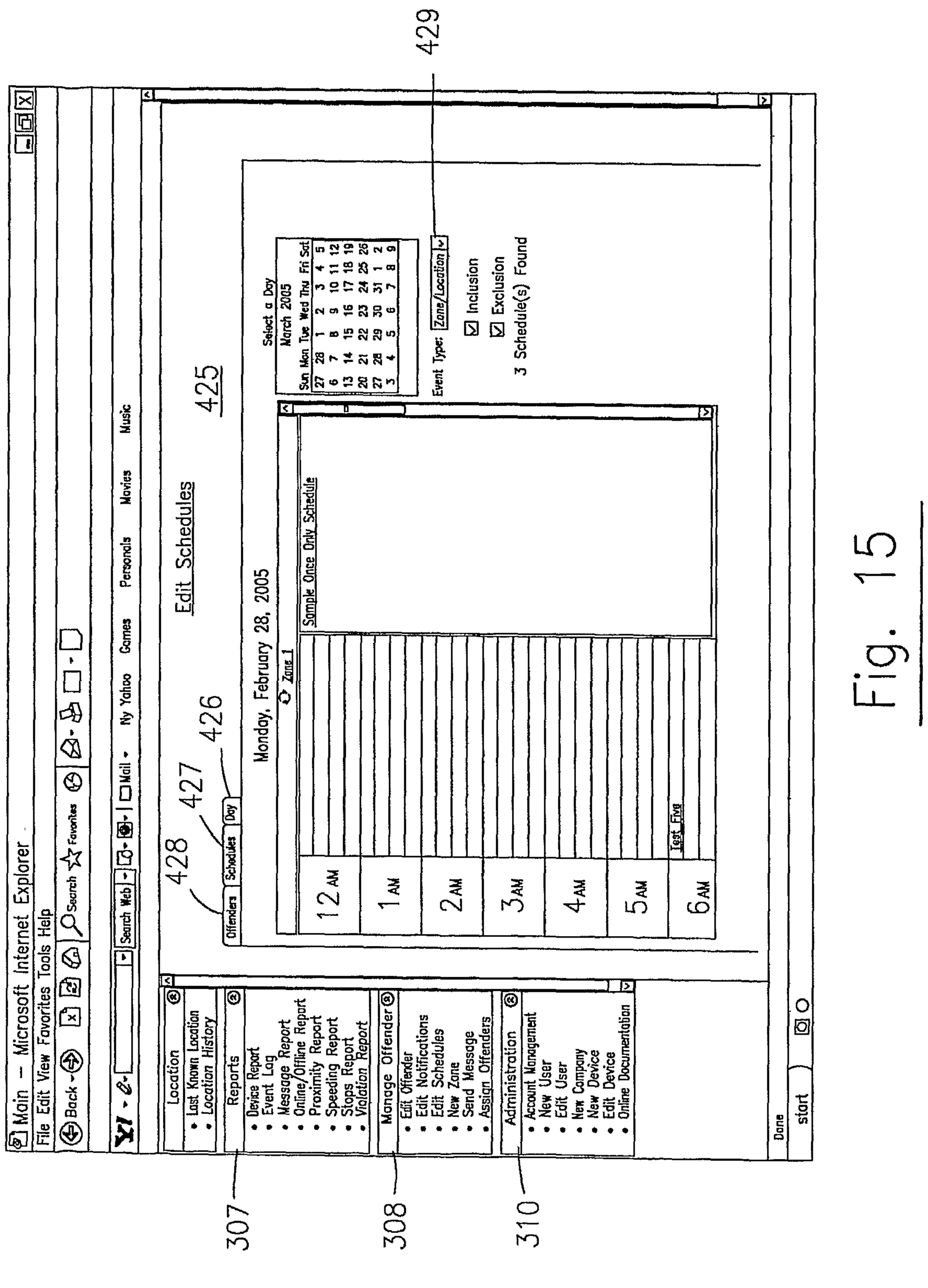

429
425
Edit Schedules
Select a Day
March 2005
Sun Mon Tue Wed Thu Fri Sat
Event Type: Zone/Location
Inclusion
Exclusion
3 Schedule(s) Found
Edit Schedules
428
427
426
Offenders
Schedules
Day
Monday, February 28, 2005
Zone 1
Sample Once Only Schedule
12 AM
1 AM
2 AM
3 AM
4 AM
5 AM
6 AM
Test Five
Main - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Search Web
Mail
My Yahoo
Games
Personals
Location
Last Known Location
Location History
Reports
Device Report
Event Log
Message Report
Online/Offline Report
Proximity Report
Speeding Report
Stops Report
Violation Report
Manage Offender
Edit Offender
Edit Notifications
Edit Schedules
New Zone
Send Message
Assign Offenders
Administration
Account Management
New User
Edit User
New Company
New Device
Edit Device
Online Documentation
Done
start
307
308
310

Fig. 15

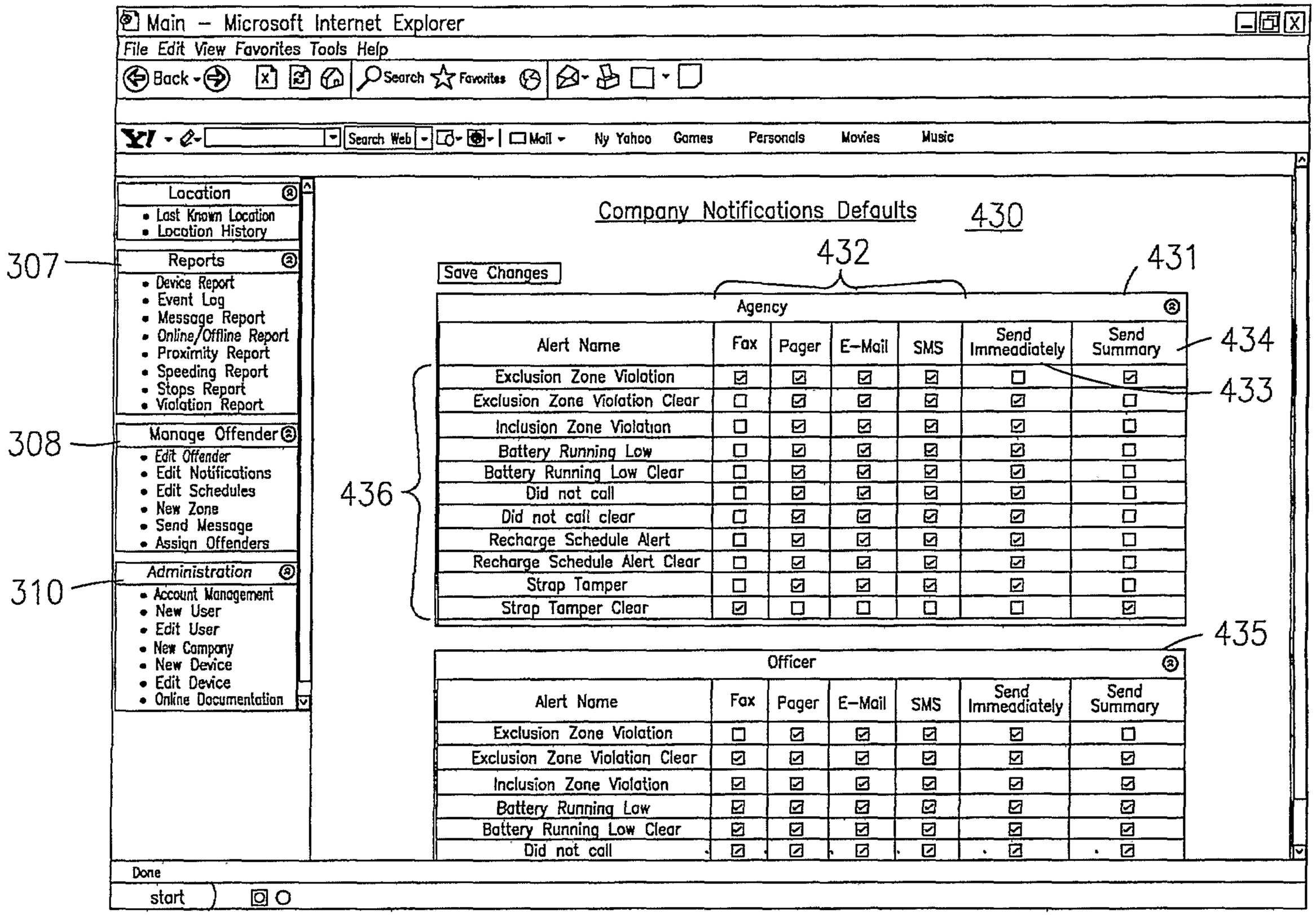

Main – Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Search Web
Mail
My Yahoo
Games
Personals
Movies
Music
Location
Last Known Location
Location History
Reports
Device Report
Event Log
Message Report
Online/Offline Report
Proximity Report
Speeding Report
Stops Report
Violation Report
Manage Offender
Edit Offender
Edit Notifications
Edit Schedules
New Zone
Send Message
Assign Offenders
Administration
Account Management
New User
Edit User
New Company
New Device
Edit Device
Online Documentation
307
308
310
Company Notifications Defaults
430
Save Changes
432
431
Agency
Alert Name
Fax
Pager
E-Mail
SMS
Send Immeadiately
Send Summary
434
433
436
Exclusion Zone Violation
Exclusion Zone Violation Clear
Inclusion Zone Violation
Battery Running Low
Battery Running Low Clear
Did not call
Did not call clear
Recharge Schedule Alert
Recharge Schedule Alert Clear
Strap Tamper
Strap Tamper Clear
435
Officer
Alert Name
Fax
Pager
E-Mail
SMS
Send Immeadiately
Send Summary
Exclusion Zone Violation
Exclusion Zone Violation Clear
Inclusion Zone Violation
Battery Running Low
Battery Running Low Clear
Did not call
Done
start

Fig. 16

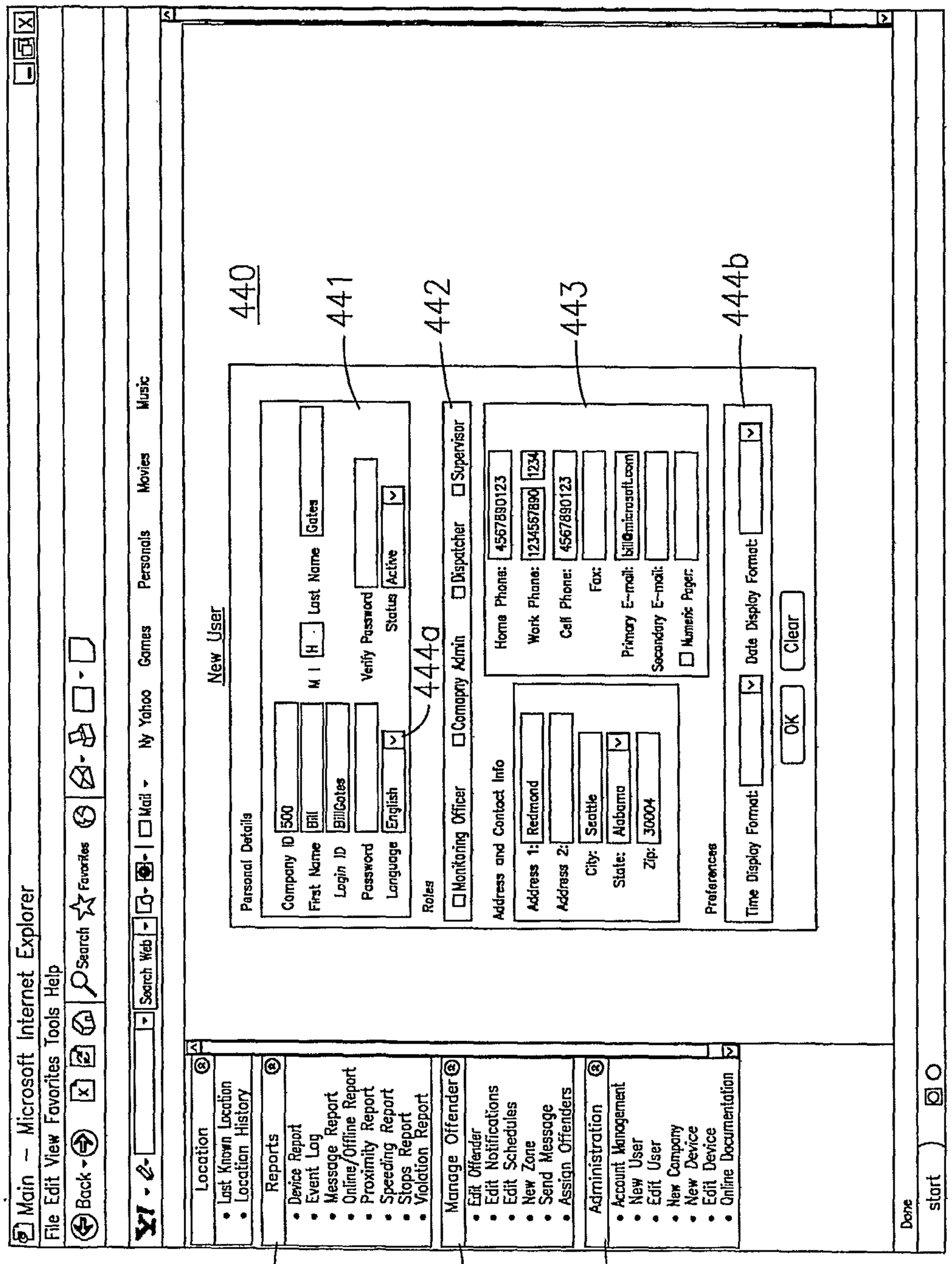

440
441
442
443
444b
444a
307
308
310
Main - Microsoft Internet Explorer
File Edit View Favorites Tools Help
New User
Personal Details
Company ID
First Name
Login ID
Password
Language
Roles
Monitoring Officer
Company Admin
Dispatcher
Supervisor
Address and Contact Info
Address 1:
Address 2:
City:
State:
Zip:
Preferences
Time Display Format:
Date Display Format:
OK
Clear
Location
Last Known Location
Location History
Reports
Device Report
Event Log
Message Report
Online/Offline Report
Proximity Report
Speeding Report
Stops Report
Violation Report
Manage Offender
Edit Offender
Edit Notifications
Edit Schedules
New Zone
Send Message
Assign Offenders
Administration
Account Management
New User
Edit User
New Company
New Device
Edit Device
Online Documentation
Done
start

Fig. 17

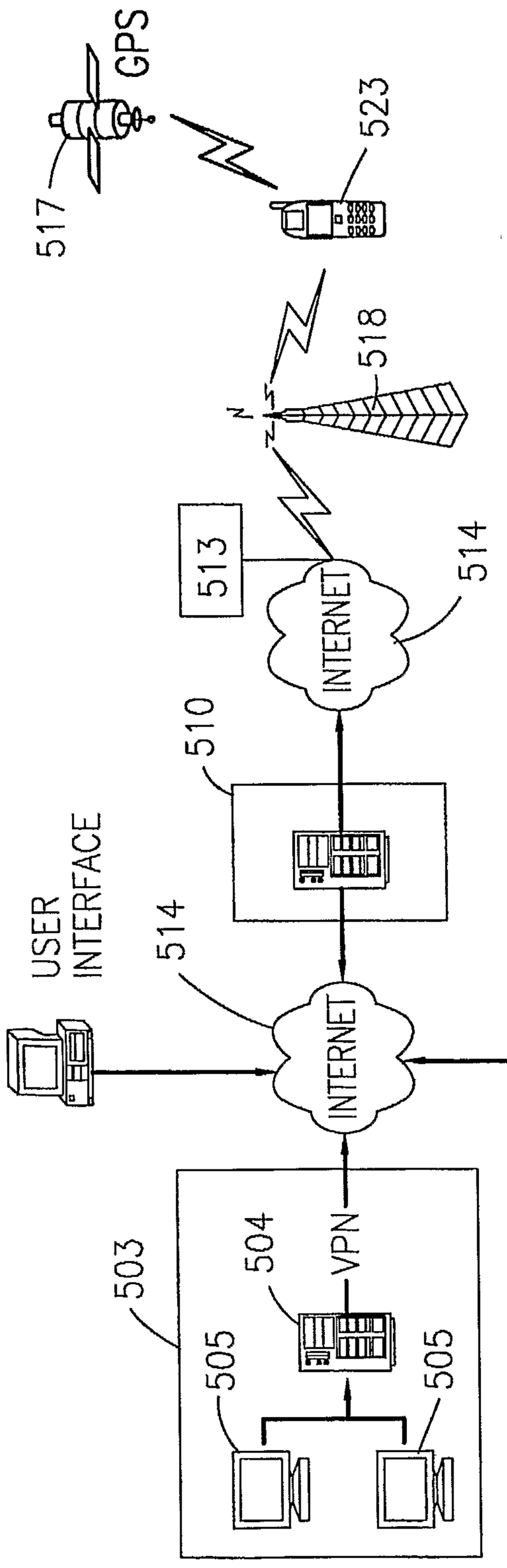

GPS
517
523
518
513
514
INTERNET
510
USER INTERFACE
514
INTERNET
501
502
DATABASE
502
DATABASE
503
504
VPN
505
505

Fig. 18

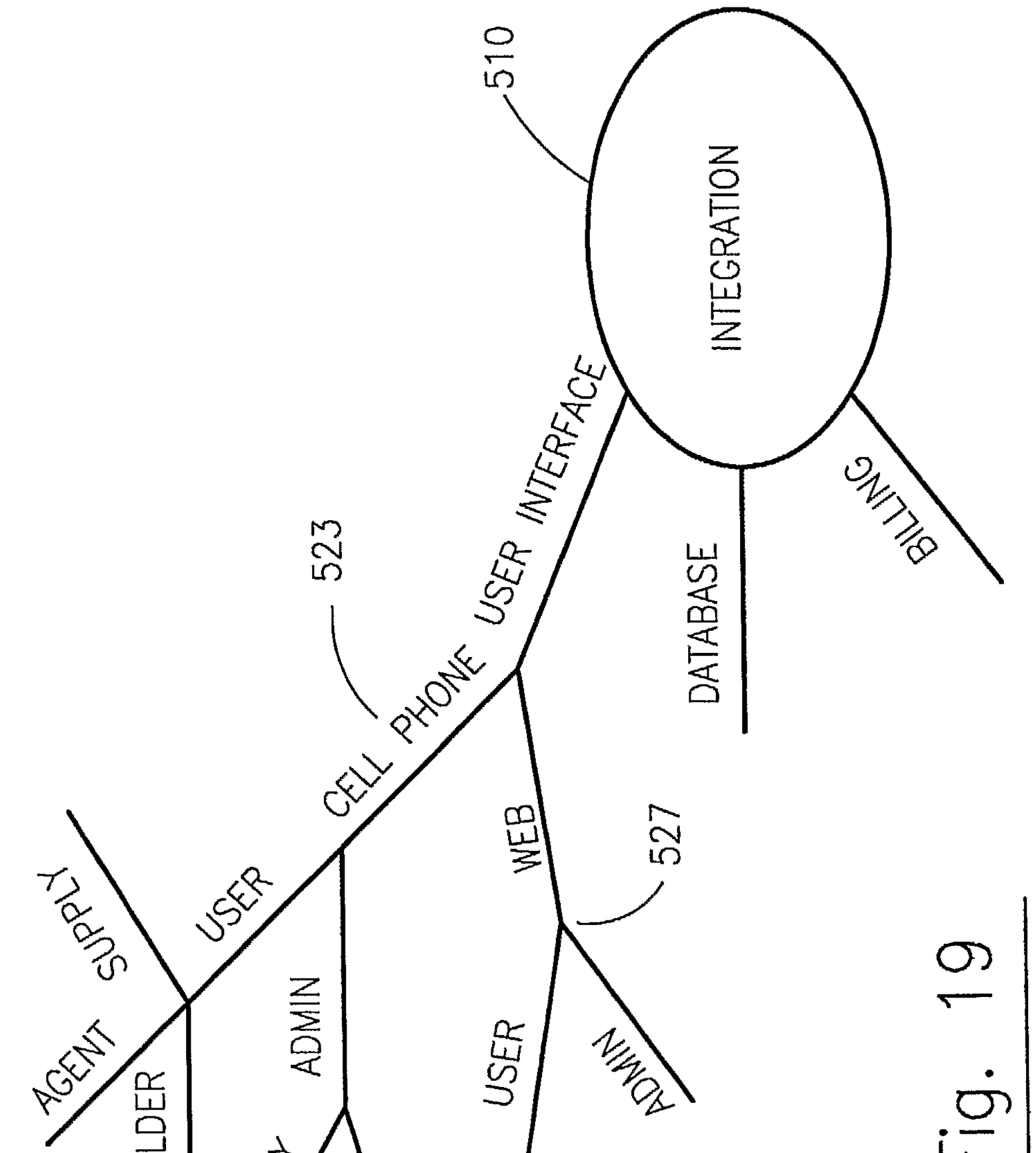

510
INTEGRATION
USER INTERFACE
DATABASE
BILLING
523
AGENT
SUPPLY
USER
CELL PHONE
WEB
527
BUILDER
ADMIN
USER
ADMIN
SURVEY
PROVISION
ADMIN
USER
BAR CODE READER

Fig. 19

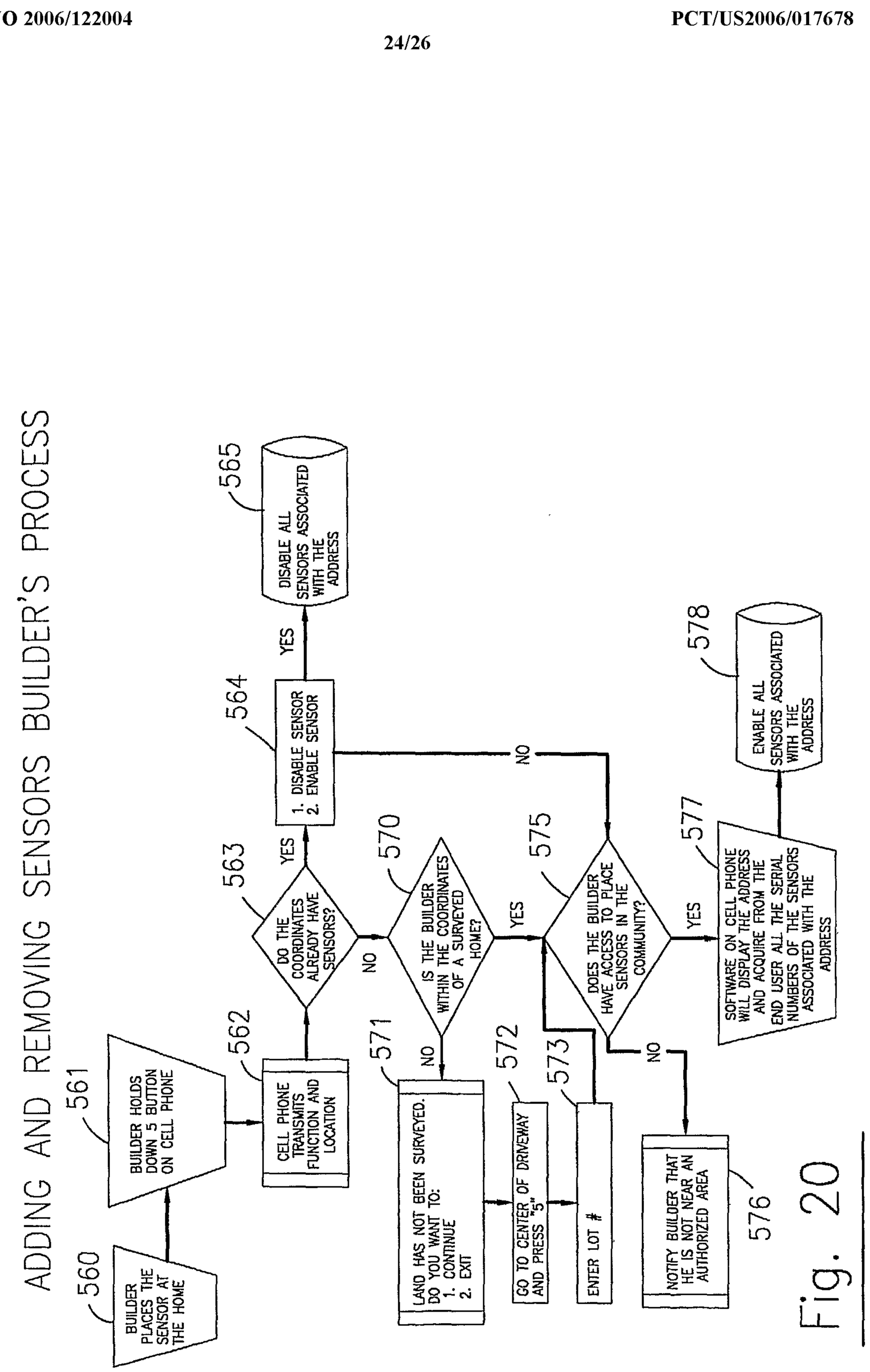

ADDING AND REMOVING SENSORS BUILDER'S PROCESS
560
BUILDER PLACES THE SENSOR AT THE HOME
561
BUILDER HOLDS DOWN 5 BUTTON ON CELL PHONE
562
CELL PHONE TRANSMITS FUNCTION AND LOCATION
563
DO THE COORDINATES ALREADY HAVE SENSORS?
YES
564
1. DISABLE SENSOR
2. ENABLE SENSOR
565
DISABLE ALL SENSORS ASSOCIATED WITH THE ADDRESS
NO
570
IS THE BUILDER WITHIN THE COORDINATES OF A SURVEYED HOME?
NO
571
LAND HAS NOT BEEN SURVEYED.
DO YOU WANT TO:
1. CONTINUE
2. EXIT
YES
575
DOES THE BUILDER HAVE ACCESS TO PLACE SENSORS IN THE COMMUNITY?
YES
577
SOFTWARE ON CELL PHONE WILL DISPLAY THE ADDRESS AND ACQUIRE FROM THE END USER ALL THE SERIAL NUMBERS OF THE SENSORS ASSOCIATED WITH THE ADDRESS
578
ENABLE ALL SENSORS ASSOCIATED WITH THE ADDRESS
NO
572
GO TO CENTER OF DRIVEWAY AND PRESS "5"
573
ENTER LOT #
576
NOTIFY BUILDER THAT HE IS NOT NEAR AN AUTHORIZED AREA

Fig. 20

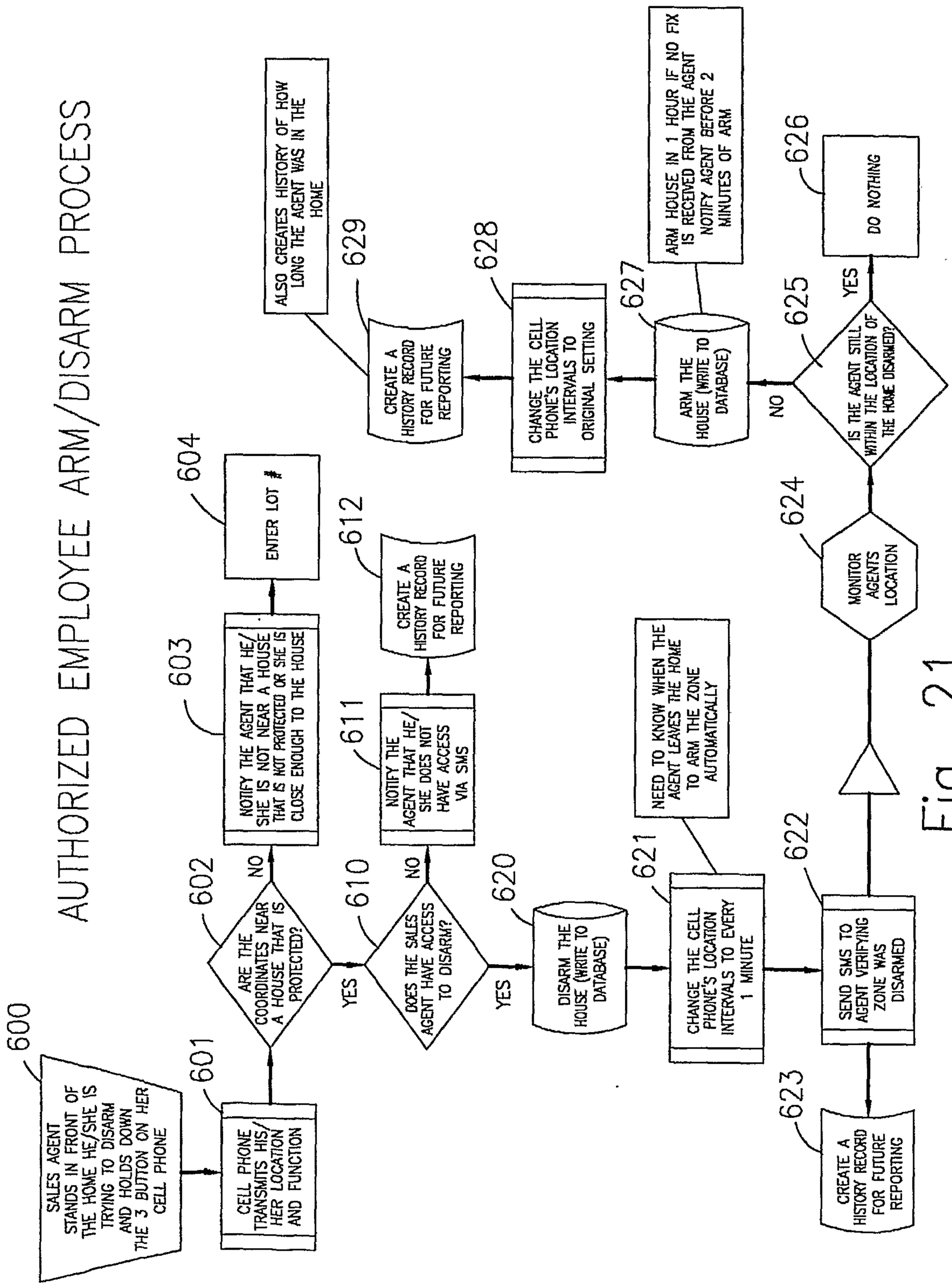

AUTHORIZED EMPLOYEE ARM/DISARM PROCESS
600
601
SALES AGENT STANDS IN FRONT OF THE HOME HE/SHE IS TRYING TO DISARM AND HOLDS DOWN THE 3 BUTTON ON HER CELL PHONE
CELL PHONE TRANSMITS HIS/HER LOCATION AND FUNCTION
602
ARE THE COORDINATES NEAR A HOUSE THAT IS PROTECTED?
NO
603
NOTIFY THE AGENT THAT HE/SHE IS NOT NEAR A HOUSE THAT IS NOT PROTECTED OR SHE IS CLOSE ENOUGH TO THE HOUSE
604
ENTER LOT #
YES
610
DOES THE SALES AGENT HAVE ACCESS TO DISARM?
NO
611
NOTIFY THE AGENT THAT HE/SHE DOES NOT HAVE ACCESS VIA SMS
612
CREATE A HISTORY RECORD FOR FUTURE REPORTING
YES
620
DISARM THE HOUSE (WRITE TO DATABASE)
621
NEED TO KNOW WHEN THE AGENT LEAVES THE HOME TO ARM THE ZONE AUTOMATICALLY
CHANGE THE CELL PHONE'S LOCATION INTERVALS TO EVERY 1 MINUTE
622
SEND SMS TO AGENT VERIFYING ZONE WAS DISARMED
623
CREATE A HISTORY RECORD FOR FUTURE REPORTING
624
MONITOR AGENTS LOCATION
625
IS THE AGENT STILL WITHIN THE LOCATION OF THE HOME DISARMED?
YES
626
DO NOTHING
NO
627
ARM THE HOUSE (WRITE TO DATABASE)
ARM HOUSE IN 1 HOUR IF NO F
IS RECEIVED FROM THE AGENT
NOTIFY AGENT BEFORE 2
MINUTES OF ARM
628
CHANGE THE CELL PHONE'S LOCATION INTERVALS TO ORIGINAL SETTING
629
CREATE A HISTORY RECORD FOR FUTURE REPORTING
ALSO CREATES HISTORY OF HOW LONG THE AGENT WAS IN THE HOME

Fig. 21

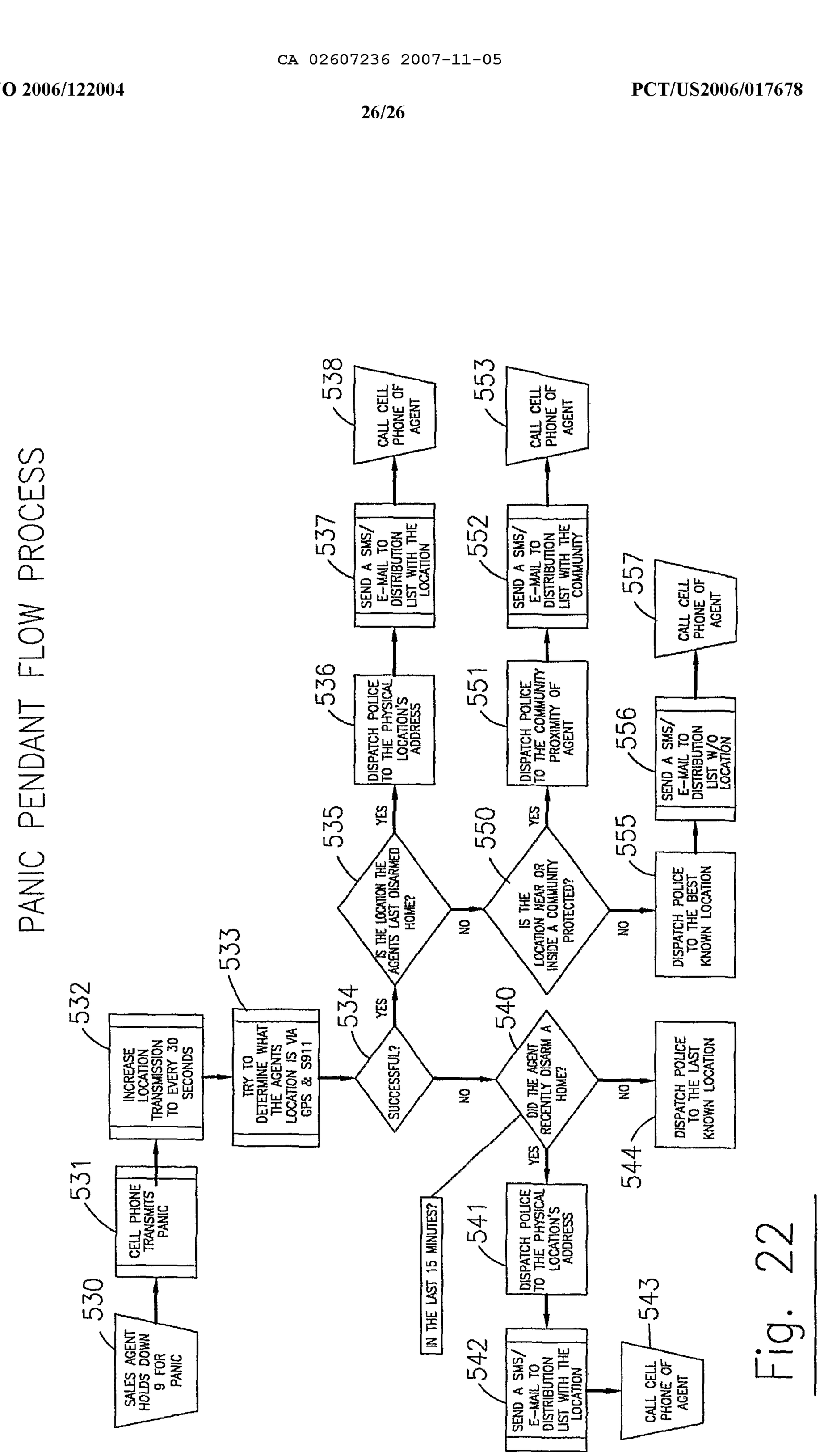
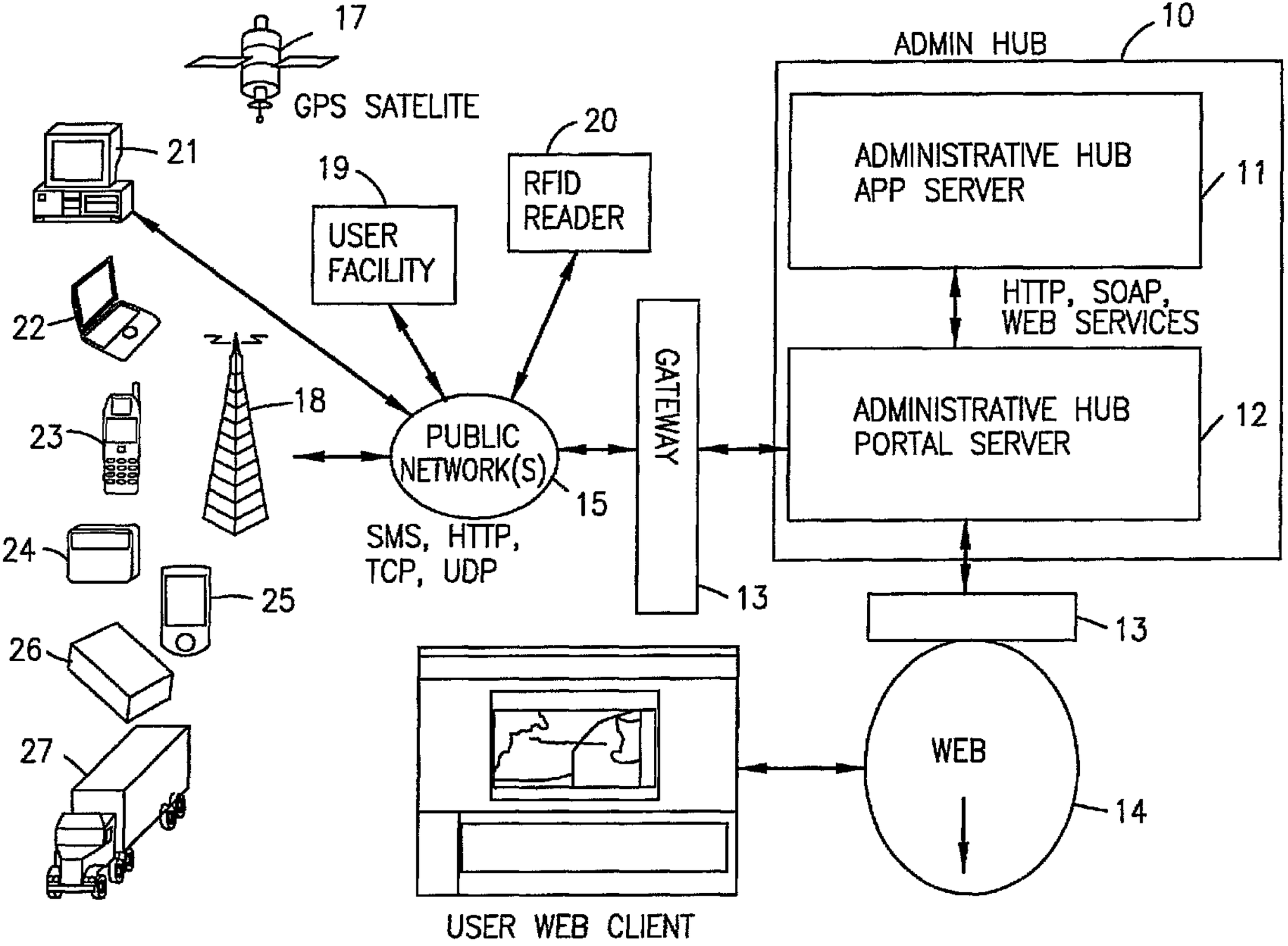

PANIC PENDANT FLOW PROCESS
530
SALES AGENT HOLDS DOWN 9 FOR PANIC
531
CELL PHONE TRANSMITS PANIC
532
INCREASE LOCATION TRANSMISSION TO EVERY 30 SECONDS
533
TRY TO DETERMINE WHAT THE AGENTS LOCATION IS VIA GPS & S911
534
SUCCESSFUL?
YES
535
IS THE LOCATION THE AGENTS LAST DISARMED HOME?
YES
536
DISPATCH POLICE TO THE PHYSICAL LOCATION'S ADDRESS
537
SEND A SMS/ E-MAIL TO DISTRIBUTION LIST WITH THE LOCATION
538
CALL CELL PHONE OF AGENT
NO
550
IS THE LOCATION NEAR OR INSIDE A COMMUNITY PROTECTED?
YES
551
DISPATCH POLICE TO THE COMMUNITY PROXIMITY OF AGENT
552
SEND A SMS/ E-MAIL TO DISTRIBUTION LIST WITH THE COMMUNITY
553
CALL CELL PHONE OF AGENT
NO
555
DISPATCH POLICE TO THE BEST KNOWN LOCATION
556
SEND A SMS/ E-MAIL TO DISTRIBUTION LIST W/O LOCATION
557
CALL CELL PHONE OF AGENT
NO
540
DID THE AGENT RECENTLY DISARM A HOME?
YES
IN THE LAST 15 MINUTES?
541
DISPATCH POLICE TO THE PHYSICAL LOCATION'S ADDRESS
542
SEND A SMS/ E-MAIL TO DISTRIBUTION LIST WITH THE LOCATION
543
CALL CELL PHONE OF AGENT
544
DISPATCH POLICE TO THE LAST KNOWN LOCATION
NO

Fig. 22


17
GPS SATELITE
ADMIN HUB
10
ADMINISTRATIVE HUB
APP SERVER
11
HTTP, SOAP,
WEB SERVICES
ADMINISTRATIVE HUB
PORTAL SERVER
12
21
19
USER
FACILITY
20
RFID
READER
22
18
23
PUBLIC
NETWORK(S)
15
GATEWAY
SMS, HTTP,
TCP, UDP
13
24
25
26
27
13
WEB
14
USER WEB CLIENT