

United
States
of
America

To Promote the Progress

of Science and Useful Arts

The Director

*of the United States Patent and Trademark Office has received
an application for a patent for a new and useful invention. The title
and description of the invention are enclosed. The requirements
of law have been complied with, and it has been determined that
a patent on the invention shall be granted under the law.*

Therefore, this United States

Patent

grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America, and if the invention is a process, of the right to exclude others from using, offering for sale or selling throughout the United States of America, products made by that process, for the term set forth in 35 U.S.C. 154(a)(2) or (c)(1), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b). See the Maintenance Fee Notice on the inside of the cover.

Coke Moya Smead

ACTING DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

Maintenance Fee Notice

If the application for this patent was filed on or after December 12, 1980, maintenance fees are due three years and six months, seven years and six months, and eleven years and six months after the date of this grant, or within a grace period of six months thereafter upon payment of a surcharge as provided by law. The amount, number and timing of the maintenance fees required may be changed by law or regulation. Unless payment of the applicable maintenance fee is received in the United States Patent and Trademark Office on or before the date the fee is due or within a grace period of six months thereafter, the patent will expire as of the end of such grace period.

Patent Term Notice

If the application for this patent was filed on or after June 8, 1995, the term of this patent begins on the date on which this patent issues and ends twenty years from the filing date of the application or, if the application contains a specific reference to an earlier filed application or applications under 35 U.S.C. 120, 121, 365(c), or 386(c), twenty years from the filing date of the earliest such application (“the twenty-year term”), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b), and any extension as provided by 35 U.S.C. 154(b) or 156 or any disclaimer under 35 U.S.C. 253.

If this application was filed prior to June 8, 1995, the term of this patent begins on the date on which this patent issues and ends on the later of seventeen years from the date of the grant of this patent or the twenty-year term set forth above for patents resulting from applications filed on or after June 8, 1995, subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b) and any extension as provided by 35 U.S.C. 156 or any disclaimer under 35 U.S.C. 253.



(12) **United States Patent**
Magaletta

(10) **Patent No.:** **US 12,205,453 B1**
(45) **Date of Patent:** ***Jan. 21, 2025**

(54) **SYSTEM AND METHOD FOR
MULTI-FACTOR LOCATION VERIFICATION**

(71) Applicant: **Robert Magaletta**, Covington, LA (US)

(72) Inventor: **Robert Magaletta**, Covington, LA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 97 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **18/326,139**

(22) Filed: **May 31, 2023**

Related U.S. Application Data

(63) Continuation-in-part of application No. 17/561,435, filed on Dec. 23, 2021, now Pat. No. 11,688,260.

(60) Provisional application No. 63/129,744, filed on Dec. 23, 2020.

(51) **Int. Cl.**
G08B 21/22 (2006.01)
H04B 1/3827 (2015.01)
H04W 4/021 (2018.01)
H04W 4/029 (2018.01)

(52) **U.S. Cl.**
CPC **G08B 21/22** (2013.01); **H04B 1/3827** (2013.01); **H04W 4/021** (2013.01); **H04W 4/029** (2018.02)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,072,396 A 6/2000 Gaukel
7,015,817 B2 3/2006 Copley et al.

7,123,141 B2 10/2006 Contestabile
RE39,909 E 11/2007 Taylor, Jr.
7,292,186 B2 11/2007 Miller et al.
7,619,533 B2 11/2009 Crucilla
8,514,070 B2 8/2013 Roper et al.
8,831,627 B2 9/2014 Aninye et al.
8,862,152 B1 10/2014 Buchholz et al.
8,866,869 B2 10/2014 Fennell
9,218,814 B2 12/2015 Xiong

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 00/5869 2/2000

OTHER PUBLICATIONS

S911 Bracelet Locator ST—For House Arrest, Law Enforcement & Security (<http://www.laipac.com/s911-bracelet.html>).
S911 Enforcer (<http://www.laipac.com/s911enforcer.html>).

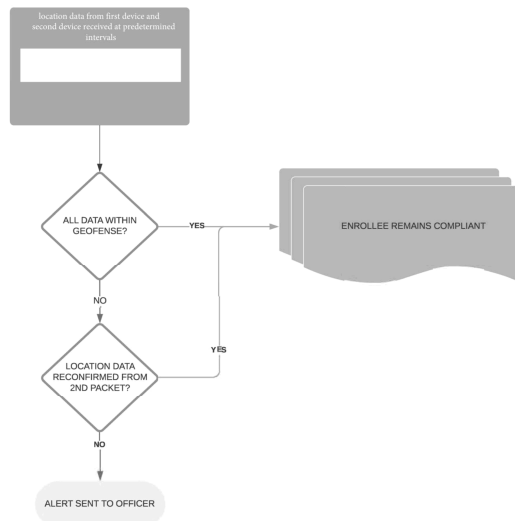
Primary Examiner — Thomas S McCormack

(74) *Attorney, Agent, or Firm* — Garvey, Smith & Nehrbass, Patent Attorneys, L.L.C.; Charles C. Garvey, Jr.; Fabian M. Nehrbass

(57) **ABSTRACT**

A method and system for monitoring an offender or defendant or potential victim utilizing multi-factor location verification. In one embodiment, the multi-factor location verification method and system utilizes GPS location data and WiFi router location data, transmitted on predetermined intervals by an ankle bracelet and wristwatch tamperproof GPS/WiFi tracking device to determine whether the two devices are within a predetermined geolocation. If it is determined in subsequent transmissions of location data that not all location data is within the predetermined geolocation, an alert is sent out indicating that an offender or defendant or potential victim is no longer located within the predetermined geolocation.

20 Claims, 2 Drawing Sheets



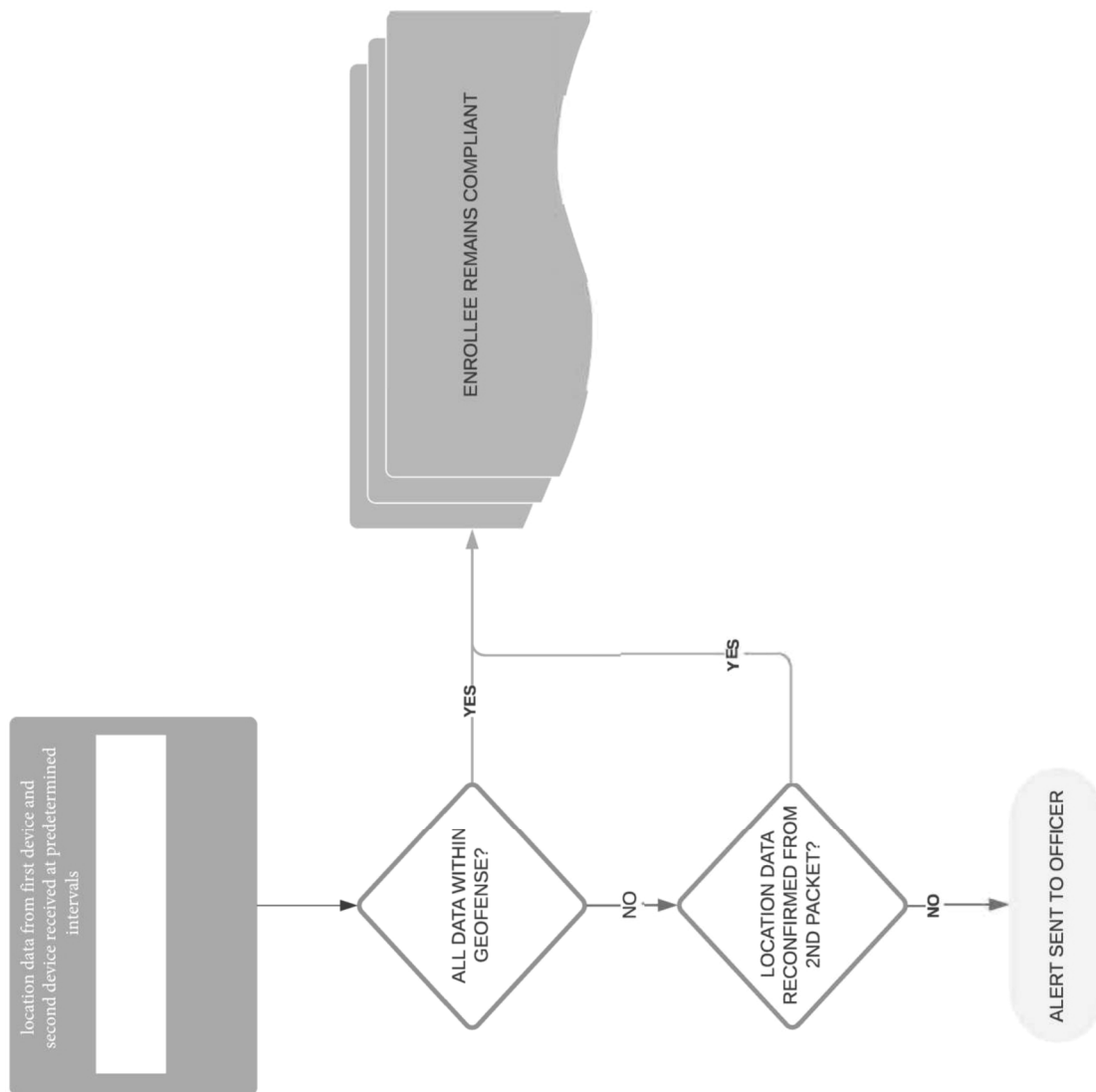
(56)

References Cited

U.S. PATENT DOCUMENTS

9,801,058	B2	10/2017	Tali et al.	
10,255,789	B2	4/2019	Keyton	
10,820,143	B2	10/2020	Segal	
11,062,584	B1	7/2021	Magaletta	
11,308,441	B2	4/2022	Lau et al.	
11,688,260	B1 *	6/2023	Magaletta	G08B 21/0288 340/539.13
2005/0040944	A1	2/2005	Contestabile	
2007/0229350	A1	10/2007	Scalisi et al.	
2008/0012760	A1	1/2008	Derrick et al.	
2010/0267361	A1	10/2010	Sullivan	
2012/0050532	A1	3/2012	Rhyins	
2013/0138397	A1	5/2013	Kiet	
2014/0002575	A1	1/2014	Fennell	
2015/0305655	A1	10/2015	Sharpe et al.	
2016/0158602	A1	6/2016	Lee et al.	
2016/0302706	A1	10/2016	Richards et al.	
2017/0162031	A1	6/2017	Drolshagen et al.	
2018/0049028	A1	2/2018	Tali et al.	
2020/0160720	A1	5/2020	Rivera et al.	
2021/0365865	A1	11/2021	Jones et al.	

* cited by examiner

FIG. 1

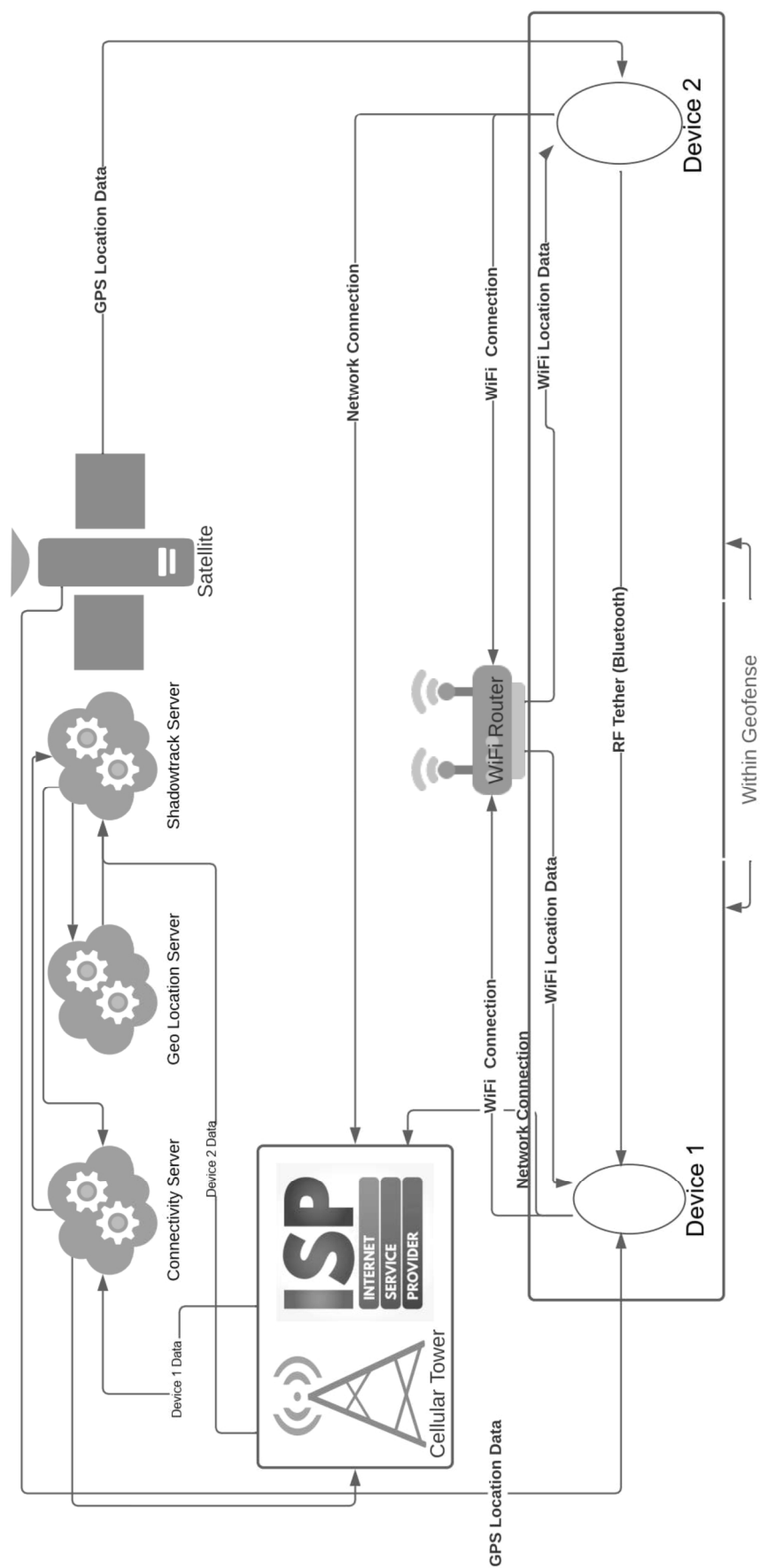


FIG. 2

1

SYSTEM AND METHOD FOR MULTI-FACTOR LOCATION VERIFICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation in part of U.S. patent application Ser. No. 17/561,435, filed 23 Dec. 2021, which claims priority to and the benefit of U.S. Provisional Patent Application Ser. No. 63/129,744, filed 23 Dec. 2020, each of which is hereby incorporated herein by reference as if copied herein.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not applicable

REFERENCE TO A "MICROFICHE APPENDIX"

Not applicable

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an apparatus, method, and system for monitoring an offender, defendant, or potential

2

victim. The present invention utilizes multiple tamperproof tracking devices on a single user; the tracking devices being able to communicate with each other to track an individual user. This combination allows for independent tracking by each device as well as active wireless, e.g., Bluetooth®, communication between each device. In this manner, the confidence in the supervising entity is increased as to whether or not someone is attempting to abscond, departing from the rules of confinement, or being kidnapped.

2. General Background of the Invention

After an arrest, offenders are in some cases released until they are obligated to appear in court before a judge or attend a hearing that is related to their arrest/accused crime. When these defendants or offenders do not show for their appearance or hearing, there is a need to have a notification of such failure to appear. There is also a need to apprehend the offender after such a failure to appear.

The following possibly relevant patents are incorporated herein by reference and listed in chronological order in the below table. The following possibly relevant patent application publications are also incorporated herein by reference and listed in chronological order in the below table.

Document No.	Title	Date
U.S. Pat. No. 6,072,396	Apparatus and Method for Continuous Electronic Monitoring and Tracking of Individuals	Jun. 6, 2000
U.S. Pat. No. 7,015,817	Personal tracking device	Mar. 21, 2006
U.S. Pat. No. 7,123,141	Electronic monitoring systems and methods	Oct. 17, 2006
U.S. Pat. No. 7,292,186	Method and system for synchronizing multiple tracking devices for a geo-location system	Nov. 6, 2007
US RE39,909	Tracking system for locational tracking of monitored persons	Nov. 6, 2007
U.S. Pat. No. 7,619,533	Method and apparatus for monitoring persons	Nov. 17, 2009
U.S. Pat. No. 8,514,070	Tracking device incorporating enhanced security mounting strap	Aug. 20, 2013
U.S. Pat. No. 8,831,627	System and method for tracking, monitoring, collecting, reporting and communicating with the movement of individuals	Sep. 9, 2014
U.S. Pat. No. 8,862,152	Two-piece system and method for electronic management of offenders based on real-time risk profiles	Oct. 14, 2014
U.S. Pat. No. 8,866,869	Parolee communication and control system and method	Oct. 21, 2014
U.S. Pat. No. 9,218,814	Cross monitoring method and system based on voiceprint recognition and location tracking	Dec. 22, 2015
U.S. Pat. No. 9,801,058	Method and system for authenticating an individual's geo-location via a communication network and applications using the same	Oct. 24, 2017
U.S. Pat. No. 10,255,789	Home incarceration confirmation system	Apr. 9, 2019
U.S. Pat. No. 10,706,288	Method of monitoring an offender or defendant	Jul. 7, 2020
U.S. Pat. No. 10,820,143	Rule deviation configuration for offender monitoring devices	Oct. 27, 2020
U.S. Pat. No. 11,062,584	System and method of monitoring an offender, defendant, or potential victim	Jul. 12, 2021
U.S. Pat. No. 11,308,441	Method and system for tracking and monitoring assets	Apr. 19, 2022
US 2005/0040944	Electronic monitoring systems and methods	Feb. 24, 2005
US 2007/0229350	Apparatus and Method for Providing Location Information on Individuals and Objects using Tracking Devices	Oct. 4, 2007
US 2008/0012760	Remote tracking device and a system and method for two-way voice communication between the device and a monitoring center	Jan. 17, 2008
US 2010/0267361	Monitoring device and system	Oct. 21, 2010
US 2012/0050532	Electronic Latch and Locking Device for a Personal Locating and Tracking Device	Mar. 1, 2012
US 2014/0002575	Parolee Communication and Control System and Method	Jan. 2, 2014

Document No.	Title	Date
US 2017/0162031	Methods and systems for providing online monitoring of released criminals by law enforcement	Jun. 8, 2017
US 2018/0049028	Method and System for Authenticating an Individual's Geo-Location Via a Communication Network and Applications Using the Same	Feb. 15, 2018
US 2021/0365865	Electronic Monitoring System with KPI-Based Optimization	Nov. 25, 2021

BRIEF SUMMARY OF THE INVENTION

The present invention is an improvement upon prior apparatuses, methods, and systems for monitoring an offender, defendant, or potential victim. The present invention provides for the simultaneous use of more than one tracking device that can be installed on and/or worn by a single user. A tracking device of the present invention is preferably tamperproof, preferably includes Global Positioning System (GPS) and WiFi (Wireless Fidelity) capabilities, and preferably can be installed on and/or worn by a single person as a single service. For example, in a preferred embodiment, a user can wear both a tamperproof ankle bracelet and a tamperproof wristwatch (or wrist bracelet), each device preferably having both GPS and WiFi (or other desired wireless technology) tracking capabilities. By providing a user with multiple (e.g., preferably at least two tracking devices), there can be independent tracking by each device as well as active wireless, and preferably short-range wireless interconnection (for example, Bluetooth®, communication between each device.

In the present invention, each unit/device preferably determines itself within proximity of the other with an electronic wireless (for example, Bluetooth®) tether from each device to each device. As a result of this active tether, there can be active GPS or WiFi location points, for example, communicated to a third party with higher confidence. Additionally, such a system preferably enables reading through and overcoming rare but possible drift points. In GPS tracking, drift refers to the discrepancy between the recorded position of a GPS device and its actual location. Drift can occur due to various factors such as atmospheric interference, signal blockage, or inaccuracies in the GPS device itself. This discrepancy can lead to errors in tracking the precise location of an object or person being tracked. An additional benefit of the present invention via the use of multiple tracking devices that are preferably tamperproof GPS and WiFi enabled devices is that if a first device fails as the result of a low battery, destruction, or other equipment failure, the other device remains active, allowing location points to continue. With the use of multiple devices, a monitoring system can better avoid errors in location data. For example, where a suspect point is received, the monitoring system of the present invention is able to suppress the suspect point momentarily, rechecking for validity against the location data received by the other device (for example, the ankle monitor or wristwatch in the case of a user wearing an ankle monitor and a wristwatch). If the questionable point is determined to have been in error, for example due to drift, no exception or infraction is recorded.

In the present invention, each device, for example a tamperproof ankle bracelet and a tamperproof watch, can operate in concert with one another or as independent GPS and/or WiFi tracking device. When used together, preferably the active competing tracking points are aggregated into one track unless the active tether (e.g., a Bluetooth® tether) connection indicates the multiple devices are not within the distance limits allowed. In those cases, competing tracking

or constant points are preferably provided by each device until the devices return to an acceptable distance.

If location data is not within geographical limits, two-way voice communication preferably can be established with one or more of the devices, for example with a tamperproof wristwatch possessing such capability, an ankle monitor, a smart phone, or another desired smart device. As used herein, the term “smart” used in conjunction with “phone” or “device” refers to a phone or other electronic device that can interact with other smart phones or smart devices or other electronic devices having similar or compatible wireless technology therein. Wireless technology can include Bluetooth®, Zigbee™, NFC, Wi-Fi, light transmission of data (LiFi) or mobile network technology such as generations 3G, 4G, or 5G).

In one or more preferred embodiments of the present invention, results of an active tether, e.g., Bluetooth®, separation, location points from two separate tracking trails, and Shadowtrack™ monitoring system contact (or lack of response) with an enrollee can be sent to an officer assigned via agency agreed upon protocols.

Determining possible drift of a particular tracking point, response, correction or follow up with a call to a tracking device, e.g., to a wristwatch, is preferably automatic. Determining drift preferably may take approximately one minute, or 1 to 300 seconds or any desired time interval therebetween, for example. Following contact with the tracking device (e.g., wristwatch), or failure to connect, preferably contact with the assigned officer can be automatically made, or made at least within a predetermined amount of time.

An overall advantage of the present invention is to obtain accurate location points by comparing the data received independently by each device and provide redundancy if one device fails or is destroyed. An example of a failure could be a “Band Tamper Alarm”. This alarm preferably can be triggered when it is determined that the band is being tampered with by a user. With one device tamper alarm, a monitoring entity can investigate; if the monitoring entity receives a tamper alarm on both devices, the monitoring entity can notify the supervising officer with extreme confidence of an abscond attempt.

The inventor has the following issued patents and currently pending patent applications. Each of the following patent documents and applications is hereby incorporated by reference as if copied herein in extenso.

Document No.	Title	Date
U.S. Pat. No. 10,706,288	Method of Monitoring an Offender or Defendant	7 Jul. 2020
U.S. Pat. No. 11,062,584	System and Method of Monitoring an Offender, Defendant, or Potential Victim	13 Jul. 2021

5

-continued

Document No.	Title	Date
17/561,435	System and Method of Monitoring an Offender, Defendant, or Potential Victim Using Multi-Factor Location Verification	23 Dec. 2021

The present invention preferably can be utilized with the aforementioned methods and systems in order to improve upon such methods and systems. With the utilization of at least two tamper-proof devices, data can be obtained with more certainty, reducing false warnings and allowing monitoring entities to know, with greater confidence, when an abscond attempt may be made. The use of multiple tamper-proof devices also may disincentivize a user or enrollee or monitored individual from attempting to tamper with a monitoring device or from attempting to otherwise break with the conditions of a user's or enrollee's or monitored individual's release. Specifically, a second wearable device of the present invention preferably can be used in place of, or in addition to, a smartphone device as set forth in U.S. patent application Ser. No. 17/561,435.

The method and apparatus of the present invention solves the problems confronted in the art in a simple and straightforward manner. What is provided includes a method and apparatus that helps solve some of the challenges that agencies are faced with regarding the monitoring of offenders. The method of the present invention provides an improved method wherein a defendant pays to enroll in a program featuring a first, monitoring entity and a second entity, such as a law enforcement entity. As part of the method, a percentage of the revenue received by the monitoring entity is paid according to an agreed formula to law enforcement and/or a prosecutor's office for each parish/county in which the program is implemented.

As part of the method, law enforcement will use the funds to cover the cost to enroll defendants into the monitoring program. Law enforcement will arrest defendants who fail to comply with the terms of their release or fail to appear for court. This method can also include sharing of the agreed fee with a law enforcement agency (e.g. sheriff or police department and/or a prosecutor's office).

Defendants will be monitored when released from jail. These methods include Telephony Network, GPS tracking, Wi-Fi tracking, mobile application, automated notifications, network triangulation, interactive voice interview.

The present invention features a biometric voice verification system that tracks offenders/defendants via an app on a "smart" device, such as a smartphone (e.g., iPhone or Android) or a wearable device such as the ShadoWatch™. The system can be set up to ensure court compliance, sending notifications, such as court date reminders, automatically to the defendants. In another embodiment, the present invention utilizes a smartwatch as the tracking device. In various embodiments, the participant or enrollee can respond to notifications via the app. In various embodiments, the participant or enrollee can make payments.

If a defendant does not show up for court, law enforcement officials can locate a defendant or the offender via the defendant's "smart" device (e.g., smartphone or smartwatch or both) and/or go back and review historical location data in attempts to apprehend the defendant.

The defendants are billed directly for these services. In one embodiment, the fee collected from the accused or

6

defendant is shared according to an agreed formula with a law enforcement agency (e.g., local jail or sheriff's office).

Telephony network can include 2-way voice biometrics, cellular network, location verification, interactive review (self-report) or notifications via push, text, telephony (e.g., with ability to conference a live call).

Continuous GPS tracking can be tracked via ankle or wrist devices.

Mobile applications include GPS location verification, cellular network location verification, facial recognition, interactive interview (self-report), Bluetooth® connected ankle or wrist device, live video as well as notifications via push, text (SMS) and telephony (with the ability to conference a live call).

The present invention features automated notification to ensure court compliance and includes, push, text (SMS), court date reminders with custom notification such as court date change, etc.

The present invention can also feature automated systems for collecting funds directly from the defendant.

In one embodiment of the present invention, an officer can track a defendant's whereabouts and compliance history by either automated or manual intervention.

The method of the present invention can include revenue sharing with a law enforcement agency and/or prosecutor's office, for example, and can include using law enforcement to arrest defendants.

If a defendant does not show up for court, law enforcement officials can locate offenders via their smart device and the method of the present invention and/or go back and review historical location data in attempts to apprehend them.

The method of the present invention features a biometric platform that is a powerful and complete community supervision package. The method of the present invention includes a variety of comprehensive compliance services that can be implemented individually, or as a complete solution, with no geographical restrictions.

A preferred embodiment of method of the present invention provides the following core elements and services:

- 1) voice verification;
- 2) fingerprint;
- 3) facial recognition; and
- 4) mobile application.

The core services of the method of the present invention include, for example, Location Based Services (LBS), Self-Report Interview (SRI), Notifications with optional delivery verification, Random Drug Test (RDT) notifications with message verification delivery, Sobriety, Offender Pay Solutions (OPS), Caseload Management (CLM), Officer Mobile App (OMA), and Travel Pass.

The present invention includes a method of supervising an offender or defendant who has been arrested or incarcerated and then released. Preferably, the method comprises the steps of:

- a) the offender or defendant paying to a first monitoring entity an enrollment fee so that the offender or defendant becomes an enrollee;
- b) wherein in step "a" the enrollee has a mobile device or land line device having a camera and that is able to receive messages and/or telephone calls from the first monitoring entity;
- c) the enrollee receiving from the first monitoring entity a communication;
- d) wherein in step "c" the communication requires that the enrollee film himself or herself using the camera of his or her land line or mobile device;

7

- e) the monitoring entity selecting a method of identifying the enrollee by optionally using voice recognition or facial recognition; and
- f) the monitoring entity notifying a second entity that is a law enforcement entity if the enrollee does not answer the communication of step “c” or is not properly identified by the voice recognition or facial recognition of step “e”;
- g) after step “f” the second entity apprehending the enrollee; and
- h) wherein the fee of step “a” is shared by the first and second entities according to an agreed formula.

Preferably, the enrollee has a curfew schedule and the communication of step “c” is a curfew management call.

In one preferred embodiment, the communication is at a random time selected by the first monitoring entity. In other preferred embodiments, the communication is at an agreed time.

Preferably, in step “c” there are multiple communications before step “f”. Preferably, these communications are at random times.

Preferably, there are multiple enrollees using the same land line or mobile device and wherein an identification pin number or caller identification verifies which enrollee is called.

Preferably, after a failure of voice recognition or facial recognition, an enrollee is able to repeat the voice recognition or facial recognition by an enrollee initiated communication.

Preferably, the enrollee location is determined during step “c”.

Preferably, location is used to confirm that the enrollee is within a telephone service area during steps “c”-“e”.

Another preferred method of the present invention for supervising an offender or defendant who has been arrested or incarcerated and then released, comprises the steps of:

- a) the offender or defendant paying to a first monitoring entity an enrollment fee so that the offender or defendant becomes an enrollee;
- b) wherein in step “a” the enrollee has a mobile device or land line device having a camera and that is able to receive messages and/or telephone calls from the first monitoring entity;
- c) the enrollee initiating a communication with a first monitoring entity using the land line or mobile device, wherein the first entity is optionally able to identify the enrollee by caller identification;
- d) wherein in step “c” the communication requires that the enrollee film himself or herself using the camera of his or her land line or mobile device;
- e) the monitoring entity selecting a method of identifying the enrollee by optionally using voice recognition or facial recognition; and
- f) the monitoring entity notifying a second entity that is a law enforcement entity if the enrollee does not answer the communication of step “c” or is not properly identified by the voice recognition or facial recognition of step “e”;
- g) after step “f” the second entity apprehending the enrollee; and
- h) wherein the fee of step “a” is shared by the first and second entities according to an agreed formula.

Preferably, in step “c” there are multiple communications and the first entity provides to the enrollee a schedule for said communications.

8

Preferably, the communications can be in any language.

Preferably, the enrollee is required to answer questions during one or more of said communications. In some preferred embodiments, the questions are via text message. In these embodiments, it is preferable for the enrollee to be able to answer the questions via text message.

Preferably, after an initial interview, the enrollee is sent an alert that requests a communication from the enrollee to complete the interview with a communication and wherein the alert cannot be dismissed and prevents use of the mobile device until the enrollee initiates the call.

In some preferred embodiments, the communication of step “c” is a text message.

In some preferred embodiments, the communication of step “c” is a notification. The notification is preferably an email, text to speech voice with verification, text to speech without voice verification, SMS, voicemail, or text to speech paired with SMS.

Another preferred method of the present invention for supervising an offender or defendant who has been arrested or incarcerated and then released, comprises the steps of:

- a) the offender or defendant paying to a first monitoring entity an enrollment fee so that the offender or defendant becomes an enrollee;
- b) wherein in step “a” the enrollee has a mobile device or land line device having a camera and that is able to receive messages and/or telephone calls from the first monitoring entity;
- c) the enrollee receiving from the first monitoring entity a communication that is a drug test notification;
- d) wherein in step “c” the communication requires that the enrollee self-identify and/or film himself or herself using the camera of his or her land line or mobile device;
- e) the monitoring entity selecting a method of identifying the enrollee by optionally using voice recognition or facial recognition; and
- f) the monitoring entity notifying a second entity that is a law enforcement entity if the enrollee does not answer the communication of step “c” or is not properly identified by the voice recognition or facial recognition of step “e”;
- g) after step “f” the second entity apprehending the enrollee; and
- h) wherein the fee of step “a” is shared by the first and second entities according to an agreed formula.

Preferably, in step “c” there are multiple communications before step “f”.

Preferably, the enrollee is identified by voice without voice biometric verification, voice with biometric verification, text to speech (TTS), SMS (text message(s)), uploaded wav file in any language, or text to speech and SMS simultaneously.

Preferably, the enrollee is provided with a breathalyzer device and after step “c” is required to use the breathalyzer device to provide a value for the enrollee’s alcohol consumption. Preferably, the value is transmitted to the first monitoring entity via a REST API call from the BACtrack® device which requests and receives responses via HTTP protocol.

A preferred device of the present invention is a smart watch/device for locating, tracking and/or monitoring a person. Preferably, the device includes at least the following:

- a global positioning system (GPS) receiver;
- a wireless telephone communicator;
- a casing which is water resistant;
- a light sensor;
- a heart rate sensor;

a tamper proof band;
 a wireless charger;
 a screen;
 a speaker;
 a microphone;
 software to permit biometric identification of individual wearing device;
 software to permit communication between device and third party or third party device; and
 a camera.
 Preferably, the casing is waterproof.
 Preferably, the casing is waterproof to at least 3 meters.
 Preferably, the casing can work for at least 30 minutes while under up to 15 cm of water.
 Preferably, the screen comprises an interactive interface.
 Preferably, the communication is voice communication.
 Preferably, the communication is not voice communication.
 The methods of the present invention can be carried out with a watch of the present invention, the watch comprising:
 a global positioning system (GPS) receiver;
 a wireless telephone communicator;
 a casing which is water resistant;
 a light sensor;
 a heart rate sensor;
 a tamper proof band;
 a wireless charger;
 a screen;
 a speaker;
 a microphone;
 software to permit biometric identification of individual wearing device;
 software to permit communication between device and third party or third party device; and
 a camera.
 The methods of the present invention can be carried out with a watch of the present invention, the watch comprising:
 a global positioning system (GPS) receiver;
 a wireless telephone communicator;
 a casing which is water resistant;
 a light sensor;
 a heart rate sensor;
 a tamper proof band;
 a wireless charger;
 a screen;
 a speaker;
 a microphone;
 software to permit biometric identification of individual wearing device;
 software to permit communication between device and third party or third party device; and
 a camera.
 The methods of the present invention can be carried out with a system of the present invention, the system comprising:
 a first monitoring entity;
 a second monitoring entity;
 a communications network; and
 a communication device.
 The communication device of the system preferably comprises a watch. Wherein the watch has at least the following:
 a global positioning system (GPS) receiver;
 a wireless telephone communicator;
 a casing which is water resistant;
 a light sensor;
 a heart rate sensor;
 a tamper proof band;

a wireless charger;
 a screen;
 a speaker;
 a microphone;
 software to permit biometric identification of individual wearing device;
 software to permit communication between device and third party or third party device; and
 a camera.
 The methods of the present invention can be carried out with a system of the present invention, the system comprising:
 a computer network;
 a first monitoring entity;
 a second monitoring entity;
 a communications network; and
 a communication device,
 wherein the communication device is a watch comprising:
 a global positioning system (GPS) receiver;
 a wireless telephone communicator;
 a casing which is water resistant;
 a light sensor;
 a heart rate sensor;
 a tamper proof band;
 a wireless charger;
 a screen;
 a speaker;
 a microphone;
 software to permit biometric identification of individual wearing device;
 software to permit communication between device and third party or third party device; and
 a camera.
 The present invention also includes a system to prevent kidnapping, the system comprising:
 a computer network;
 a central monitoring facility;
 a communications network; and
 a communication device,
 wherein the mobile device is a watch comprising:
 a global positioning system (GPS) receiver;
 a wireless telephone communicator;
 a casing which is water resistant;
 a light sensor;
 a heart rate sensor;
 a tamper proof band;
 a wireless charger;
 a screen;
 a speaker;
 a microphone;
 software to permit biometric identification of individual wearing device;
 software to permit communication between device and third party or third party device;
 a camera; and
 a panic alert button.

In this system, preferably the device establishes communication with the central monitoring facility when a triggering event takes places. Preferably, the triggering event comprises an alert generated by the kidnapping victim, a detection of tampering by the device, or detection that the victim or device is outside of a pre-determined safe zone. Preferably, the establishment of communication between the device and the central monitoring facility alerts trained operators of a potential hostage attempt/kidnapping in progress. Preferably, once communication is established, a cen-

11

tral station operator asks the victim if they are okay via the two-way voice function of the device and if the victim responds they are okay, the operator will respond by asking them what their secret passphrase is; wherein the victim has the option of responding with the phrase associated with a false alarm that all is okay or a phrase associated with an actual kidnapping or hostage event; wherein if the phrase stated by the victim matches the passphrase on file, the operator will respond by thanking the victim and stating that they have verified the passphrase, and to have a good day; wherein authorities are dispatched once victim responds with passphrase on file.

A device of the present invention is preferably a smart watch/device for locating, tracking and/or monitoring a person. Preferably, the device comprise:

- a global positioning system (GPS) receiver;
- a wireless telephone communicator;
- a casing which is water resistant;
- a tamper proof band;
- a charger;
- a screen;
- a speaker;
- a microphone;
- software to permit biometric identification of individual wearing device;
- software to permit communication between device and third party or third party device; and
- a camera.

Preferably, the casing can work for at least work for at least 30 minutes while under up to 1 m of water. Preferably, the device meets the standards of an IP67 waterproof rating.

In one or more preferred embodiments of the present invention, a method is provided for monitoring an individual, comprising the steps of: providing an individual with a first wearable device and a second wearable device (for example, the first wearable device can be a tamperproof wristwatch and the second device can be an ankle bracelet) (the present invention is not limited to two wearable devices—in certain embodiments, an individual can be given more than two, such as three or four wearable devices); connecting the first wearable device and second wearable device wirelessly (for example, using a radiofrequency tether); using software to set a maximum allowable distance between the first wearable device and the second wearable device; connecting the first wearable device and the second wearable device to a cellular network; connecting the first wearable device and the second wearable device to an internet service provider, e.g., using a WiFi router; obtaining GPS location data by the first wearable device and by the second wearable device; obtaining WiFi router location data from the WiFi router by the first wearable device and the second wearable device; transmitting the GPS location data and WiFi location data from the first wearable device and the second wearable device to one or more servers; and comparing the GPS location data and WiFi location data from the first wearable device and the second wearable device to determine whether the first wearable device and the second wearable device are within the maximum allowable distance. When the user is outside of the range of an internet service, e.g., a WiFi router, the user method can be altered so that the tracking and monitoring is dependent only on the data which does not include the internet service, e.g., WiFi router, location data.

Preferably, the method is performed with GPS location data being obtained at predetermined intervals. Preferably, internet service location data, e.g., WiFi location data is obtained at predetermined intervals. Preferably, all the loca-

12

tion data is obtained at predetermined intervals. For example, the location data may be obtained at least every minute. The location data can be obtained at least every 10 seconds. The location data can be obtained at least every 5 seconds. The location data can be obtained every second. In certain preferred embodiments, all location data can be obtained at the same time and/or pursuant to the same interval. In other preferred embodiments, the location data from an internet service, such as WiFi, and GPS can be obtained at different times and/or at different intervals.

If, during monitoring of a user/individual it is determined that the user/individual is not within a set geolocation area, an alert can be sent to a supervising officer.

The method can also be performed with one or more of the following additional steps: receiving additional location data from the wearable devices if it is determined that the first wearable device and second wearable device are not within the maximum allowable distance of each other; and sending an alert if the additional location data does not demonstrate that the first wearable device and second wearable device are within the maximum allowable distance of each other.

Additionally, the method can comprise a step of sending connection data by the first wearable device and the second wearable device to one or more servers as to whether the first wearable device and the second wearable device are connected to each other. Data can be transmitted at any desired interval, for example every minute, every 30 seconds, every 10 seconds, etc.

The present invention also provides a number of systems for monitoring whether an individual is within a set location. In one or more of these embodiments, the system preferably comprises the steps of: providing an individual with at least two wearable devices; connecting the wearable devices to each other wirelessly, for example, using a radiofrequency tether; using software to set a geolocation area, wherein the geolocation area is a maximum allowable distance between the wearable devices; connecting the wearable devices to a cellular network; connecting the wearable devices to an internet service provider, e.g., using a WiFi router; obtaining GPS location data by the wearable devices at a predetermined interval (for example, at least every minute or every five minutes or every 30 seconds); obtaining internet or WiFi router location data from the internet service or WiFi router by the wearable devices at a predetermined interval (for example, at least every five minutes, or every minute, or every thirty seconds); transmitting the GPS location data and internet or WiFi location data from the wearable devices to one or more servers by the cellular network or internet service provider if the wearable devices are without a cellular network connection; comparing the GPS location data and WiFi location data from the wearable devices to determine whether all location data is within the set geolocation area; receiving additional location data from the wearable devices if it is determined that not all location data is within the set geolocation area; and sending an alert if the additional location data is not all within the set geolocation area.

In the various embodiments of the present invention, preferably at least one of the wearable devices may comprise a casing which is water-resistant; a tamper-proof band; a display screen; a speaker; a microphone; software to permit biometric identification of an individual wearing the device; software to permit communication between the device and a third party or a third party device; and/or a camera. Preferably one of the wearable devices may comprise a tamper

13

proof band and software to permit biometric identification of an individual wearing the device.

The dual use of tamper proof tracking devices can also be used to help prevent a kidnapping. The present invention provides one or more systems for helping to prevent a kidnapping, preferably comprising: a computer network; a central monitoring facility; a communications network; a first communication device; and a second communication device; wherein the first communication device is preferably a wearable device comprising: a global positioning system (GPS) receiver; a wireless telephone communicator; and a panic alert button; and wherein the second communication device is preferably an ankle monitor; and wherein the first and second communication devices establish communication with a central monitoring facility; wherein the first and second communication devices are connected or able to be connected to an internet service, e.g., via a WiFi router; wherein the first and second communication devices obtain and transmit GPS location data and internet or WiFi location data (e.g., if connected to a WiFi router, if not, they only transmit GPS location data) at predetermined intervals; wherein the GPS location data and WiFi location data from the wearable device and ankle monitor is reviewed (or only GPS location data if no WiFi location data is available) to determine whether all location data is within a set geolocation area, wherein the geolocation area is a maximum allowable distance between the wearable device and ankle monitor; wherein if not all location data from the wearable device and ankle monitor is within the set geolocation area in at least two subsequent transmissions of location data, a triggering event takes place and an alert is sent to a central monitoring facility to alert trained operators of a potential hostage attempt/kidnapping in progress. As in the other methods, preferably the predetermined time interval can be any time, but preferably is short enough so that there is sufficient confidence in the location of the wearer of the devices. For example, the predetermined time interval can be about five minutes, about 1 minute, about 30 seconds, about 10 seconds, etc.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

For a further understanding of the nature, objects, and advantages of the present invention, reference should be had to the following detailed description, read in conjunction with the following drawings, wherein like reference numerals denote like elements and wherein:

FIG. 1 is a flow chart showing a method of utilizing a preferred embodiment of a multi-location verification system of the present invention; and

FIG. 2 is diagram showing receipt and transmission of data using a preferred embodiment of a multi-factor location verification function of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The curfew management application of the present invention allows the user to verify whether a defendant, offender, or enrollee is at a designated location at a specific time. In one embodiment of the present invention, the curfew management application uses voice verification and facial recognition during inbound/outbound curfew calls to positively identify an enrollee. The curfew management application allows the user (such as a law enforcement official, for example) to schedule random calls or push notifications at a

14

desired frequency. These calls or push notifications may be placed outbound to the enrollee or the enrollee may be required to call into the system from the designated location. The application uses a feature that retrieves caller ID information and may alert the user if the enrollee is calling in from an unauthorized phone number. In one embodiment, the user may be notified if the enrollee fails to successfully complete inbound/outbound curfew calls due to no answer, hang ups, busy signals, and voicemails.

Utilizing curfew management and the curfew management application of the present invention enables a law enforcement agency to efficiently monitor the whereabouts of enrollees. Curfew management provides the ability to create a set or random curfew schedule. The curfew management application of the present invention enables an agency to:

- 1) schedule random curfew calls during a specific time frame on a certain day;
- 2) schedule random outbound curfew calls during a daily, weekly, monthly, or random period;
- 3) modify a curfew schedule;
- 4) send random push notifications to the enrollee's smart phone to initiate a curfew call;
- 5) use caller ID feature that detects if the enrollee is attempting to place an inbound call from an unauthorized phone number or use call forwarding;
- 6) positively identify the enrollee by using voice verification or facial recognition technology;
- 7) enable the enrollee to perform a voice verification request via the telephony network and the option to perform a verification request using a Wi-Fi data network;
- 8) easily access reports of all tracking history;
- 9) provide instant, daily, or weekly automated user email alerts of non-compliant calls;
- 10) reduce false non-compliance results by specifying multiple attempts to reach an enrollee before they are found to be non-compliant;
- 11) audit all user modifications to compliance or enrollee caseload history;
- 12) set the amount of time between call attempts;
- 13) provide manually initiated on demand outbound verification calls or alerts;
- 14) restrict manually initiated calls;
- 15) listen to voice verification files for each call;
- 16) provide quick view button for current calls as well as future scheduled calls;
- 17) cancel individual or multiple calls without adjusting the schedule;
- 18) provide proprietary multi verification channel registration and verification to reduce or eliminate voice failures;
- 19) require callbacks after verifications (Call forwarding spoofing);
- 20) set the number of call attempts prior to becoming non-compliant;
- 21) modify the compliance status of a call;
- 22) add user notes to a compliance call;
- 23) provide audited recordings of any user changes on the enrollee profile;
- 24) provide audit recordings of future call cancellations;
- 25) identify an inbound call by either caller ID or pin number (this is ideal in a case where more than one enrollee is using the same telephone number);
- 26) scheduling templates to minimize entering repetitive schedules;
- 27) avoid location spoofing;

15

- 28) easily filter curfew calls by a call number that is auto generated for each call;
- 29) filter curfew calls by compliance status;
- 30) filter curfew calls by date; and
- 31) filter calls by call type.

The present invention enables law enforcement to schedule inbound/outbound calls daily, weekly or monthly (recurs once every (x) number of days or weeks or months), or in a customizable schedule, and can include the following features (alone or in combination):

- 1) Randomly scheduled calls that allow the user to choose which days and the frequency of calls during a given weekly or monthly period;
- 2) customized frequency of required inbound/outbound calls;
- 3) enable or disable feature for inbound/outbound schedules;
- 4) ability to disable a schedule until a specific date;
- 5) open end date on curfew schedule so that the schedule recurs until the enrollee is disabled; and
- 6) ability to modify a curfew schedule.

The present invention can include a "Curfew Call" feature that can include any of the following aspects, alone or in combination:

- 1) designate the number of inbound/outbound calls to be placed to or from an enrollee during a specific period of time;
- 2) designate the number of alerts to be sent to an enrollee's smart device (for example, smart phone) requiring the enrollee to initiate an inbound call during a specific time frame;
- 3) random call frequency;
- 4) restrict inbound calls from unauthorized numbers or allow any phone number;
- 5) ability to identify an inbound call by either caller ID or a PIN number (this feature is used when more than one enrollee is using the same telephone);
- 6) schedule multiple attempts on outbound calls;
- 7) ability to set the amount of time between outbound call attempts;
- 8) ability to cancel individual or multiple calls without adjusting the call schedule;
- 9) ability to see scheduled outbound calls 30 days in advance;
- 10) manually initiated on demand outbound call;
- 11) quick view button capability to conveniently view outbound calls scheduled for the current day or for the next 30 days;
- 12) user ability to filter curfew calls for a specific enrollee by call number, date, compliance status, or call type;
- 13) call forwarding detection; and
- 14) alerts to the user if the enrollee fails to check in or check in outside of the required schedule time.

The present invention can include the following Additional Call Features:

- 1) proprietary multiple verification channel registration and verification to reduce or eliminate voice failures;
- 2) ability to listen to voice verification files for each call;
- 3) call review capabilities along with the ability to modify compliance and add notes to calls;
- 4) audit recordings of any user changes;
- 5) scheduling templates to avoid entering repetitive schedules;
- 6) restrictions placed on the smartphone app to prevent it from being deleted or tampered with

16

- 7) automated alert to the user if enrollee's smartphone device battery is low, has been turned off, or if the device is dead
- 8) agency feature that allows the enrollee to complete a verification call after a voice failure;
- 9) allows the enrollee to use more than one landline telephone number to be monitored on;
- 10) ability to cancel future scheduled inbound/outbound calls;
- 11) ability to export for compliance history reports;
- 12) ability to generate call history reports by specified date; and
- 13) ability to generate compliance activity reports per enrollee, per user, and per entity.

The following are benefits of the Outbound Curfew Management feature of the present invention:

- 1) increases productivity for the agency by automating verification of an enrollee's whereabouts without interaction from the user;
- 2) increases productivity by preventing false non-compliances due to schedule changing abilities, call review, and call compliance modification features;
- 3) increases productivity by preventing false non compliances by using call adjustment or cancellation features for scheduled or allowed time away from home;
- 4) provides user accountability by auditing all user changes and modifications to enrollee profiles;
- 5) provides a recording of each call for user review or proof of an imposter; and
- 6) aids users in combating location spoofing.

Location Services (LBS)

The present invention can include Location Based Services (LBS) which allows the user to verify a participant's whereabouts using multifactor location verification technology. An example of such verification technology is a wearable device, such as a wristwatch, (e.g., the ShadoWatch™) which can incorporate Wi-Fi, GPS, and Network location technology to increase location accuracy while enhancing battery life. A smart wearable device such as the ShadoWatch™ can feature an attractive tamperproof wristwatch with color display. Such a watch can also be water-proof and include motion sensors, vibration alerts, messaging, heart rate and blood pressure detection. The watch can offer the ability to communicate with the participant by using two-way voice or electronic messaging. The watch also can have a QR activation feature that allows for a convenient and effortless activation process for users in the field. The ShadoWatch is preferably managed through the ShadowtrackONE™ total corrections platform designed for managing all services from one unified easy to use platform. LBS can also be paired with voice verification and facial recognition technology to positively identify the participant. Shadowtrack offers the flexibility of a minimally invasive tracking solution utilizing LBS on a landline telephone, mobile telephone or via the Shadowtrack mobile. This allows the participant to be discreetly monitored without having to wear any equipment.

The location services feature of the present invention allows the agency, such as a law enforcement agency, to:

- 1) efficiently monitor the whereabouts of an enrollee during a specific time frame;
- 2) efficiently monitor if the enrollee is attempting to enter a restricted area;
- 3) monitor an enrollee at a specific address or within the range of an entire state;
- 4) detect location spoofing; and

17

- 5) use on demand or automated random location frequency.

In one embodiment of the present invention, the location of the enrollee can be verified in the following ways, alone or in combination:

- 1) cellular triangulation of the smart device (for example, for the ShadoWatch);
- 2) GPS positioning coordinates;
- 3) scheduled silent location verification;
- 4) silent on demand user-initiated location verification;
- 5) pairing location services with voice verification and/or facial recognition to ensure the enrollee is with the telephone device during location verification; and
- 6) on demand manual GPS location request.

In one embodiment of the present invention, when the verification call is completed, location coordinates are sent to the Shadowtrack® platform via an application protocol interface (API).

The user can review location results via the following ways:

- 1) displayed on a map via the enrollee's profile;
- 2) displayed on the enrollee compliance tab via a "View Map" button that is listed for each inbound or outbound call;
- 3) displayed with a color-coded PIN for easy viewing: green for compliant (inside fence) and red for non-compliant (outside fence), for example;
- 4) GPS coordinate results logged on a map on the enrollee's compliance call details;
- 5) GPS results displayed with a color-coded PIN on a map within the call details for easy viewing as green for compliant (inside fence) and red for non-compliant (outside fence); and
- 6) location verification results logged on the enrollee compliance tab via the mobile app.

Additional location verification features include:

- 1) compatibility with all major cellular carriers;
- 2) on demand voice verification combined with location verification;
- 3) option to initiate facial recognition verification in the event of a suspicious voice verification alert;
- 4) allows the user to create multiple Inclusion Zones to verify if the enrollee is at home, school, work, treatment program, etc.;
- 5) allows the user to create multiple Exclusion Zones to verify if the enrollee is near a restricted area;
- 6) customizable radius options to broaden or tighten a designated location area;
- 7) allows the user the option to set up a state radius in comparison to the enrollee's designated location address;
- 8) a feature set at the admin level that allows the agency to set all enrollee location radius's to a state wide parameter depending upon a certain interview protocol assigned to them;
- 9) an alert to the user if the enrollee does not initiate their location within a specified time frame;
- 10) API error for failure to reach the app due to the device being turned off or the app is not running
- 11) the ability for the Shadowtrack® platform to send messages that display an alert on the enrollee's smart device screen that must be manually dismissed;
- 12) feature that automatically prompts the enrollee on the next call to opt in to location services on their mobile device if an opt out occurs at any time;
- 13) mobile registration feature that alerts the user if a mobile phone number is "Not Locatable"; and

18

- 14) allows the user the ability to override location coordinates manually.

The following are some benefits of the location services feature of the present invention:

- 1) improves efficiency by allowing users to automate monitoring enrollee's whereabouts on a consistent basis;
- 2) non-compliant alerts to help the user manage enrollee non-compliance due to being outside of a designated location;
- 3) assists in combating enrollees attempting to turn off Location services on their device to prevent location verification by alerting the user when this happens;
- 4) prevents location spoofing; and
- 5) allows the user the ability to tighten the radius area to miles but also broaden the radius area for the entire state of the enrollee's designated location address.

In one or more preferred embodiments of the present invention, a multi-factor location verification function comprises: the ability to receive independent location data from a wrist-worn device and from a mobile device that is preferably tethered to a wrist-worn device via a wireless connection, e.g., a radio frequency connection such as a Bluetooth® connection or from multiple wearable devices. Preferably, the wearable devices are tamperproof. The aforementioned devices preferably can transmit internet or WiFi and GPS location information to a server on predefined time intervals. The intervals of transmission may vary, for example, between 1 second and 1 hour. For example, the devices may each transmit WiFi location information at least every 5 minutes. The interval of transmission can be adjusted. Similarly, the devices may each transmit GPS location information on the same or different intervals as that of transmission of the WiFi location information. Preferably, location data is transmitted from each device at the same time. However, if not done at the same time, the server can parse the data and synchronize once data is received from multiple devices. Preferably, all location information (both GPS and internet or WiFi) is transmitted from each device at the same time. However, if not done at the same time, the server can parse the data and synchronize once all the data is received. The preferable intervals of transmission for GPS location information preferably are the same as that of transmission of internet or WiFi location information.

FIG. 1 is a flow chart depicting a preferred embodiment of a system of the present invention. In the multi-location verification system shown in FIG. 1, the location of an enrollee/participant is verified to determine whether a first wearable device (for example, a tamperproof wrist device) and a second wearable device (for example, an ankle monitor) of the enrollee/participant are within a predetermined geofence. The predetermined geofence preferably is a floating geofence. While the present invention can determine an enrollee/participant's location using location data and can set a static geofence (e.g., an enrollee's home if user/enrollee is on house arrest), the geofence described in FIG. 1 is preferably a floating geofence, meaning it can move with the two devices. Predetermined geographical parameters are preferably established within which the first wearable device and second wearable device must fall. If location data indicates that the two devices are not within the geofence, then the monitoring agency knows that the enrollee is no longer located with both wearable devices. While breaking of an electronic communications tether, e.g., of the Bluetooth® connection between devices, would suggest an enrollee is no longer with both devices, a floating geofence preferably can serve as another mechanism to ensure the

enrollee remains compliant. Moreover, it is possible that a floating geofence can be set to a smaller distance than what is enabled by an electronic communications tether, e.g., a Bluetooth® connection, such that an electronic communications tether or Bluetooth® connection between the first wearable device and second wearable device can be maintained even though the enrollee does not remain compliant within shorter or smaller range floating geofence parameters. In one or more preferred alternative embodiments, a smart phone or other smart device can be utilized in addition to the two wearable devices. In this manner, the system is enabled to be even more confident at knowing the location of an enrollee/participant.

If it is determined that an enrollee/participant is not within a predetermined geofence, an alert preferably is sent to an officer or designated law enforcement agency or to system control. The predefined intervals of transmission of location information for each device and each type of location information (e.g., WiFi or GPS) is preferably synced so that each type of location information (e.g., WiFi and GPS) can be sent from each of the two (or more) devices at the same time. Once the data is received by the server, custom-developed software logic preferably is included in the system that is adapted to compare the independent location data of each device to determine, with a high degree of accuracy, the location of the enrollee wearing the devices as well as the distance between the devices. Specifically, location data is preferably received from both devices at which point logic is preferably adapted to compare the location points and determine if both points are within a pre-determined floating geolocation area. Law enforcement, system control preferably has the ability to set the size of the geolocation area (or under certain circumstances a user may be given the ability to). It can be of any desired size and preferably is of a size to ensure that the enrollee is wearing both wearable devices (and in those embodiments utilizing a smart phone, located within a designated proximity of the smart phone). For example, the floating geofence could be 5 to 10 feet by 5 to 10 feet. If one location point from any of the devices falls outside of the pre-determined geolocation area (geofence), the server preferably is adapted to await for confirmation on the second location packet of data. If a point falls outside of this geolocation area on the second location data packet, a notification alert preferably is then generated. If both location points are confirmed to fall within the geofence, the enrollee remains compliant. Location data preferably is continuously sent, per the predetermined intervals. Moreover, by comparing the location data of two or more devices, the present invention is able to more accurately determine whether or not an enrollee is located within a static geofenced area and/or within a floating geofence area as compared to systems utilizing only one device and the present invention allows for more accurate determination of an enrollee's location.

If one of the location points is not within the given geographical parameters of the other device, additional logic can be considered to confirm the irregular location coordinates. As previously noted, for example, when a location point falls outside of a floating geolocation fence area (indicating thus that the devices are too far apart), a subsequent data packet can be considered to confirm that the person is in fact outside of the floating geolocation fence area. If additional verification is unsuccessful (e.g., irregular location coordinates are confirmed), the appropriate personnel can be notified that at least one of the devices is no longer within the configured geofence of the two devices. As noted,

the geofence size can be set by law enforcement or system control and is typically sized to about 10 feet by 10 feet, or about 100 square feet.

With the use of the multi-factor location verification, each device should be together, within designated proximity of one another, to remain compliant. In the present invention, the multi-factor location verification function preferably determines whether there is a separation between the multiple devices (wearable devices and possible smart phone or smart device in embodiments utilizing a smart phone or other smart device) by using internet or WiFi and GPS location data in addition to an electronic tether such as a Radio Frequency (RF) tether to determine a separation. In some embodiments, it is possible to only use internet or WiFi and GPS location data if desired and not utilize an electronic or RF tether to determine separation, though utilization of an electronic or RF tether in addition to location data is preferable. In addition to a separation determination, the present invention preferably has the ability to determine the distance between the devices, and each location is preferably compared against each other to verify a location point's accuracy.

A diagram showing a preferred embodiment of a multi-factor verification function is set forth in FIG. 2. In FIG. 2, two devices, Device 1 and Device 2 are depicted. In one or more preferred embodiments, device 1 can be a wristwatch and device 2 can be an ankle bracelet, each of which are preferably tamper proof. However, as explained previously, the two wearable devices can also be used in conjunction with a smart phone or other desired smart device in certain embodiments. As seen in FIG. 2, both wearable devices can be tethered together via a wireless or radio frequency (e.g., Bluetooth®) connection. Each device can be connected to an internet provider, e.g., using a WiFi router will be included in this example. As such, each device can obtain WiFi location data of the WiFi router. Each device can also obtain GPS location data from a satellite. Each device can transmit both the GPS location data as well as WiFi location data to one or more servers utilizing a network connection.

As shown in FIG. 2, the devices preferably can transmit such information utilizing a cellular network connection or an internet network connection, or both. Upon receipt of the location information, the servers preferably are adapted to utilize the location data to determine, as explained above, whether the two devices are within a floating geofence area and can also determine whether a person is within a predetermined geofence area. A connectivity server of the present invention preferably can be used in the system to collect location data from devices using, for example, MQTT (The Standard for IoT Messaging). As discussed at <https://mqtt.org/>, (which is hereby incorporated herein by reference) "MQTT is an OASIS standard messaging protocol for the Internet of Things (IoT). It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth." OASIS stands for Outcome and Assessment Information Set. The Connectivity Server then can take the device 1 data and transmits it to a Shadowtrack™ server where it can thereafter be transmitted to the geolocation server. Location data from the second device preferably is sent to the Shadowtrack™ server. The Shadowtrack™ server then preferably transmits information to the Geolocation Server. The geolocation Application Protocol Interface (API) preferably returns a location and accuracy radius based on information about cell towers and WiFi nodes that the mobile client can detect. The Shadowtrack™ server is where a proprietary application of

21

the present invention can be installed and is used to receive data from the connectivity and geolocation servers. As seen in FIG. 2, it is possible for the multi-factor location verification system to function without a cellular network connection, as the server preferably can be accessed via a WiFi

FIG. 1 explains the relationship between a first device, e.g., a watch, and a second device, e.g., an ankle monitor, and how they can communicate with the servers, e.g., cloud based servers, to independently determine if both devices are within a given geo location. The location data preferably is not dependent on the devices being tethered to each other to determine that a second device is nearby. The independent location data from each device preferably can be processed in a cloud server network to determine their proximity to each other. A tether, e.g., a RF tether, between the devices preferably acts as a backup form of location verification by ensuring the devices are together. Once the location and tether data is received by an application server, which can be in a cloud server network, the application server can then send geo location data to the location server to obtain a reverse geo location that can be used to compare to a roving inclusion zone by the devices to determine whether the devices are together.

In one or more preferred embodiments, the simultaneous use of both an ankle bracelet and wristwatch tamperproof GPS/WiFi tracking device installed on a person can thus be used as a single service (one on a wrist and one on an ankle). This combination allows for independent tracking by each device as well as active Bluetooth® communication between each device. This combination preferably enables the below functions.

Each unit determines itself within proximity of the other with an electronic Bluetooth® tether between and from each device to each device. The result is active GPS or WiFi location points with higher confidence, reading through and overcoming rare but possible drift points. Should one device fail as the result of low battery, destruction, or other equipment failure, the other device remains active, allowing location points to continue. Where a suspect point is received, Shadowtrack™ monitoring system suppresses it momentarily, rechecking for validity against the location data received by the other device (ankle or wristwatch). If the questionable point is determined to have been in error, no exception or infraction is recorded.

Each device, the ankle bracelet and the watch, operate in concert with one another or as independent GPS and or WiFi tracking devices. When used together, the active competing tracking points are aggregated into one track unless the Bluetooth® connection indicates they are not within the distance limits allowed. In those cases, competing tracking or constant points are provided until they return to an acceptable distance.

If location data is not within geographical limits, two-way voice communication can be established with the wristwatch.

The results of the Bluetooth® separation, two separate tracking trails, and Shadowtrack™ monitoring system contact (or lack of response) with the enrollee is then sent to the officer assigned via agency agreed upon protocols.

Determining possible drift of a particular tracking point, response, correction or follow up with a call to the wristwatch is preferably is automatic, taking approximately one minute. Following contact with the wrist-

22

watch, or failure to connect, contact with the assigned officer preferably can be automatic.

An overall advantage provided by one or more preferred embodiments of the system and method of the present invention is to obtain accurate location points by comparing the data received independently by each device and provide redundancy if one device fails or is destroyed. An example of a failure could be a “Band Tamper Alarm”. With one device tamper alarm, system control can investigate; if a tamper alarm on both devices is received, and system control can notify a supervising officer with extreme confidence of an abscond attempt.

Self-Report Interview (SRI)

In one embodiment, the present invention includes a “self-reporting” service feature that consists of an interactive voice interview of customized questions that allows the user to obtain current information for the participant without the need for a face to face visit. The participant can conveniently complete their interview utilizing any telephone device or via the Shadowtrack mobile App. The SRI service supports any language and includes automatic transcription of participant responses. An exception report is generated from the participant responses and which the users can conveniently access. Exception responses are also noted on the participant profile via an audio file and can automatically be transcribed from speech to text. The SRI also includes scheduled reminders that can be placed to the participant via phone call, text, or email. Interview reminders improve participant compliance and ensure interview sessions are completed in a timely manner. The self-reporting service can be paired with LBS to not only verify the participant’s whereabouts during the self-reporting session but to also randomly verify their location at any time during the month.

Utilizing the Interactive Voice Interview (Self-Report) service of the present invention allows the agency to:

- 1) improve efficiency by eliminating user contact directly with the enrollee to retrieve updated information ranging from enrollee contact information, employment status, interaction with law enforcement or arrests, or any other type of information the user would like to retrieve from the enrollee;
- 2) improve enrollee accountability by reminding the enrollee they have an upcoming self-report session; and
- 3) obtain current records and contact information for the enrollee in a more efficient manner.

In various embodiments of the present invention, the Interactive Voice Interview feature can include:

- 1) the ability to schedule the interview to begin on a specific date;
- 2) the ability to schedule the interview duration to be an hour, day, week, month; and
- 3) option to schedule the interview to recur daily, weekly, monthly, and yearly.

In various embodiments of the present invention, interview reminders of the Self-Report service can be scheduled in the following ways:

- 1) a certain number of days prior to the interview period;
- 2) hours or minutes prior to interview expiration date;
- 3) recur every day until the end of the interview period;
- 4) recur a fixed number of times; and
- 5) logic that stops interview reminders once an interview has been complete.

In various embodiments of the present invention, features of the Self-Report service can include:

- a) supports any language as well as hearing impaired;
- b) interactive voice response that allows the enrollee to respond to questions asked during self-reporting;

23

- c) recordings (such as wav file) of all enrollee interview responses the user can hear;
- d) ability to create custom self-reporting protocols with an unlimited number of questions;
- e) option to accept self-reporting interviews after the interview period has expired;
- f) allows you to pair random location verification called “Quick Checks” with self-reporting;
- g) agency feature that allows the enrollee to complete an interview after a voice verification failure;
- h) allows the user to create interview schedule templates per Entity to avoid repetitive entering of schedules;
- i) administrative ability to lock Interview schedule templates to prevent users from modifying templates;
- j) allows the user the ability to share Interview schedule templates with additional sub entities;
- k) ability to require an Interview to be completed by forcing the enrollee to complete the interview on the next inbound or outbound call once the interview period has expired;
- l) when a verification call API request is received, an alert will be displayed on the screen, along with a sound and vibrate, requesting that the enrollee call in to the Shadowtrack® platform to complete their interview by clicking on the alert window. The alert cannot be dismissed and prevents use of the mobile device until the enrollee initiates the call or manually dismissed the alert;
- m) when the verification call is completed the interview questions will be played as well as the location coordinates are sent to the Shadowtrack® platform via API. This can be set to automatically be sent out within minutes of the call. Shadowtrack® has logic to set off an alert if the location coordinates are not received by the user within five minutes; and
- n) allows the option for the enrollee to initiate facial recognition after an alert is received on the smartphone. Once identity verification is completed the enrollee will receive an SMS text of the interview questions. The enrollee can respond to the interview questions via text message or voice.

The following are some benefits of the Interactive Voice Verification feature of the present invention:

- 1) Increases productivity for the agency by eliminating the user’s personal interaction to obtain information from the enrollee;
- 2) Allows the agency to designate how frequently self-reporting is required in order to aid in upkeep of current information for the enrollee;
- 3) Implements enrollee responsibility in reporting updated information to the user by placing self-reporting reminders;
- 4) Increases user efficiency by sending automated reports for enrollee’s that fail to self-report;
- 5) Allows the user to pair random location verification with self-reporting to ensure the enrollee has not left a designated area during a self-reporting period; and
- 6) No transcription is required with smartphone.

Notifications

An embodiment of the notification service of the present invention provides a robust automated solution to communicate with the participant. This service allows the user the flexibility of sending notifications in several different formats including Text Message, Text to Speech (TTS), Email, and Voicemail. The user can schedule one time or recurring messages to one participant or multiple participants at the same time. The Shadowtrack application logs the date and

24

time the participant received the notification, the details and format of the message, and the date and time the participant listened to the message. Future scheduled notifications can be cancelled at the user’s discretion. This service allows the user to view all notification history for a participant as well as view future scheduled notifications for a period of time, for example, up to ninety days (90) in advance.

In a preferred embodiment, utilizing the Notification service allows the agency to:

- 1) Improve efficiency by eliminating user contact directly with the enrollee;
- 2) Improve efficiency by allowing the user to send a notification to multiple enrollees at one time;
- 3) Scheduled and random customized notifications via speech, text to speech, text messaging or uploaded recorded voice, for example, which is useful for court and probation appointment reminders; and
- 4) Conveniently schedule exclusion dates for notifications so that notifications are not placed on specified dates.

Notifications Platform Functionality

- 1) Schedule notification in the following ways, for example:
 - a) Email;
 - b) Text to speech with voice verification;
 - c) Text to speech without voice verification;
 - d) SMS;
 - e) Voicemail; and
 - f) Text to speech paired with SMS.
- 2) Example notification features:
 - a) Ability to send out a mass notification to more than one enrollee;
 - b) Ability to send more than one type of notification to an enrollee at a time;
 - c) Ability to schedule a notification to occur at a specific time and date;
 - d) Ability to schedule a notification to recur on a set schedule such as a daily, weekly, or monthly period;
 - e) Ability to schedule exclusion dates for a notification so that notification are not placed on specified dates
 - f) Ability to schedule a notification to recur randomly during a daily, weekly, monthly, or random period;
 - g) Ability to verify if a notification message was heard by an enrollee;
 - h) Ability to select “Voice Verification” so that the enrollee must verify their identity before the notification message plays;
 - i) Phone call placed to the enrollee that allows the enrollee to listen to the notification message;
 - j) Allows the enrollee to call into the application in the event of a missed call and hear the notification message;
 - k) Ability to turn voice verification off for notifications;
 - l) Ability to make additional attempts to deliver the notification if a voice failure occurs;
 - m) Ability to verify the date and time an SMS or other notification was sent to the enrollee;
 - n) Ability to pair voice verification with text to speech and voicemail notifications during additional attempts to deliver the notification message;
 - o) Ability to restrict notifications by enrollee;
 - p) Allows the enrollee to send a voicemail to their assigned user;
 - q) Support for multiple languages, including Spanish and English, text to speech technology converting typed phrases to voice;

25

- r) Push notification sent to the enrollee via their mobile device that allows them to view the notification message on their mobile device; and
- s) Ability to conveniently schedule notifications per enrollee and per entity from the User's main dash-
board.

Example Benefits of Notifications:

- 1) Increases productivity for the agency by eliminating the user's personal interaction to communicate mes-
sages;
- 2) Increases productivity by allowing the user to deliver messages to multiple enrollee's one or more times; and
- 3) Increases efficiency by allowing the user to verify the enrollee has received the notification message.

Random Drug Testing (RDT)

A preferred embodiment of the drug testing service of the present invention offers a turnkey-solution to refine the entire drug testing process from start to finish. Shadowtrack's Random Drug Test is a solution for all aspects of drug testing including automated notification to the participant when they are selected to report for a test, an offender pay option (OPO) to collect payment for testing, and integration with testing facilities that allows for final test results to be documented in the application. Shadowtrack's approach to drug testing allows the participant to receive a notification to report for testing instead of requiring them to call into an automated system on a daily basis. This amounts to pointless additional calls and wasted officer resources. Users can create random or scheduled drug testing templates to designate the frequency of testing and include a custom notification message. Notifications can be placed to the participant via email, text to speech, or text. Shadowtrack's detailed color code reports allow the user to conveniently manage who is reporting for testing. The color code report can be viewed in a list, calendar, or graph format and can be exported in Excel or PDF format. Users can also view future scheduled notifications up to three months in advance. This allows the agency to properly plan staffing needs as well as office closures. Drug testing templates can conveniently be placed on hold or disabled. The RDT service also allows the user to designate specific dates they would like to exclude from scheduling drug testing notifications. This service improves the overall efficiency and productivity of users by automating the entire drug testing process.

Utilizing the Random Drug Test service allows the agency to accomplish the non-exhaustive list of tasks:

- 1) Allows the user to place enrollees into named groups for random or fixed scheduled drug testing notifications;
- 2) Have unlimited number of groups;
- 3) Allows the user the flexibility of suspending drug testing notifications at the agency's discretion;
- 4) Allows the agency the ability to modify notification templates;
- 5) Allows the user the option to move an enrollee to another group;
- 6) Custom report available to the user so they are aware of what enrollees have been notified to report for drug testing and/or have upcoming drug testing notifications scheduled;
- 7) Improve efficiency by automating drug testing notifications to enrollees only when a drug test is required;
- 8) Includes voice verification to ensure the correct person is receiving the drug testing notification message;
- 9) Includes the ability to send an SMS message once it is determined an enrollee has not answered the call;

26

- 10) Allows the enrollee to call into the Shadowtrack® system to hear the notification message if they miss the phone call;
- 11) Sends the agency analytical data via reports regarding drug testing results; and
- 12) Sends an alert to the enrollee via the smartphone app to view the drug testing notification message. The alert message must be initiated or dismissed.

Example Random Drug Testing Platform Functionality

- 1) Send Drug Testing notifications to an enrollee in one or more of the following formats:
 - a) Voice without voice biometric verification;
 - b) Voice with voice biometric verification;
 - c) Text-to-Speech (TTS);
 - d) SMS (text messages);
 - e) Uploaded wav file in any language; and
 - f) Text-to-Speech and SMS combined simultaneously.
- 2) Send "Drug Testing" notifications at the following frequencies:
 - a) Daily fixed schedule;
 - b) Weekly fixed schedule;
 - c) Monthly fixed schedule;
 - d) Daily random schedule;
 - e) Weekly random schedule;
 - f) Monthly random schedule;
 - g) Selectable applicable days that allows the user to exclude specific days of the week;
 - h) Allows the user to specify preferred times of the day to deliver drug testing notification message; and
 - i) Feature that allows the user to exclude drug testing days for their agency via a calendar so that drug testing notifications are not placed on these dates.
- 3) Multiple attempts to deliver a drug testing notification:
 - a) Shadowtrack® will automatically place additional retries to deliver a drug testing notification in the event of a missed call due to a no answer, hang up, voicemail, or answering machine;
 - b) Allows the enrollee to call into the Shadowtrack® application to hear a missed drug testing notification; and
 - c) The user can pair an SMS message to be sent to an enrollee's mobile if the enrollee does not answer the call attempts to deliver the drug testing notification message.
- 4) Create Custom drug testing templates:
 - a) Allows the user to create a custom template for each group that specifies drug testing frequency and custom drug testing message details;
 - b) Allows the user the ability to modify drug testing templates;
 - c) Allows the user the flexibility of suspending/unsuspending drug testing templates at the agencies discretion; and
 - d) Allows the user the ability to schedule specific holidays to restrict drug testing notifications from being sent out per entity.
- 5) The ability to place an enrollee into a group to designate drug testing frequency:
 - a) Allows the user to assign an enrollee to a group to automatically schedule the frequency of drug testing notifications;
 - b) Allows unlimited number of groups per agency; and
 - c) Allows the user the option to move an enrollee to another group to increase or decrease the frequency of drug testing notifications.

27

6) Reporting:

- a) Custom reports available to the user so they are aware of what enrollees have been notified to report for drug testing and/or have upcoming drug testing notifications scheduled;
- b) Report displays the time and date the enrollee received the drug testing notification;
- c) Report displays the call disposition of the drug testing notification call;
- d) Report displays the group name each enrollee is assigned to;
- e) Report displays the enrollee's assigned user; and
- f) Random Drug Test summary reports include the total number of enrollees utilizing the drug testing service, a breakdown of how many enrollees are in each group, and a breakdown of call results per enrollee.

7) Service Types:

- a) Service can be used as a standalone or paired with any other Shadowtrack® service, for example.

Example Benefits of Random Drug Testing Service

- 1) Increases productivity for the agency by eliminating the user's interaction to notify an enrollee to report for drug testing;
- 2) Allows the agency to determine the days and times that are most convenient for enrollees to report for drug testing;
- 3) Allows the agency to place drug testing on hold for holidays or specific dates;
- 4) Allows the agency to set the discretion of how many enrollees report for drug testing; and
- 5) Provides the agency with analytical data as a way to document drug testing results in an effort to increase or decrease drug testing frequency for the enrollee or perform caseload studies.

Sobriety

A preferred embodiment of the present invention may include a sobriety module that works in conjunction the Shadowtrack mobile app. The app and device work with Android and IOS devices. In certain embodiments, BAC-track is an electronic device that is integrated with the Shadowtrack mobile app to utilize facial recognition, alcohol consumption detection, and location verification. The device requires no installation and can be purchased directly by the participant. Shadowtrack will send random alerts notifying the participant an "Alcohol Test is Required". Once the alert is sent, the participant will have a configurable amount of time to complete the Sobriety test before becoming non-compliant. Once the test is completed, the Blood Alcohol Content (BAC) score, location of the test, and a picture of the participant while performing the test will be logged in the participant's profile in the Shadowtrack application. If the initial BAC score is above 0.0 a secondary test will be initiated to verify the validity of the initial result. The Shadowtrack mobile app works in conjunction with the BACtrack device to detect spoofing with other devices and includes liveness testing to ensure the validity of each test. This service provides a discreet and cost-effective approach to sobriety testing.

If the test is completed, the device application may send the following results, for example, to the Shadowtrack® platform:

- 1) Blood alcohol score (BAC);
- 2) Location of the test; and
- 3) Picture of the enrollee.

28

Utilizing the Breathalyzer Option allows the agency to have the following features, for example:

- 1) Combine facial recognition with alcohol consumption detection via an electronic device that requires no installation and is purchased and shipped directly to the enrollee;
- 2) Facial recognition liveness test to prevent enrollees from using a photograph or recorded video;
- 3) Anti-spoofing that includes the ability to detect other devices within Bluetooth® range throughout the duration of the sobriety test;
- 4) Ability to detect the blue light on the breathalyzer device is on during a sobriety test to prevent spoofing; and
- 5) Outbound voice verification request only (Independent of alcohol test).

Example Breathalyzer Platform Functionality:

- 1) Combines facial recognition with alcohol consumption detection via an electronic device, such as BACtrack®, that requires no installation and is purchased and shipped directly to the enrollee. In a preferred embodiment, when the Shadowtrack® app receives a verification call API request, a push notification will be displayed on the screen, along with a sound and vibrate, requesting that the enrollee call into the Shadowtrack® platform to complete a sobriety test. The alert will stay on the display until the enrollee initiates the call or manually dismisses the alert; preferably, the BAC value is transmitted to the first monitoring entity by a REST API call from the BACtrack® device which requests and receives responses via HTTP protocol (a REST API defines a set of functions which developers can perform requests and receive responses via HTTP protocol such as GET and POST").
- 2) Enrollee may be prompted to place their face inside a designated square area on their mobile device to ensure accuracy of facial recognition during enrollment and subsequent sobriety testing;
- 3) When the verification call is completed, location coordinates may be sent to the Shadowtrack® platform. This can be set to automatically send out within a set time, such as minutes of the call. In one embodiment, Shadowtrack® has logic to set off an alert if we do not receive the location coordinates within five minutes;
 - a) Inbound voice verification request (Independent of alcohol test);
 - b) There may be a button on the app that generates a phone call to the Shadowtrack® platform to perform a voice verification; and
 - c) Once this button is pressed, the app may also send location coordinates.
- 4) Alert message displayed to the enrollee when low battery of the breathalyzer device is detected.
- 5) Facial recognition liveness test to prevent enrollees from using a photograph or recorded video.
- 6) Anti-spoofing that includes the ability to detect other devices within Bluetooth® range.
- 7) The Shadowtrack® platform may trigger a non-compliant event and notify the assigned user for any of the following reasons, for example:
 - a) The breathalyzer score is greater than a predetermined level;
 - b) Failure to receive a reading from the device within time specified;
 - c) Picture does not match enrollment picture in the Shadowtrack® application. NOTE: An event can be

29

- manually converted to non-compliant and the user will be required to add notes as to why the status was changed;
- d) An alert may be sent to the user if a test result is not received within a predetermined time frame; and
 - e) Error for failure to reach the app due to the device being turned off or the app is not running.
- 8) Send random "Sobriety Test" notifications in one or more of the following non-exhaustive list of formats:
- a) Voice without verification;
 - b) Voice with voice biometric verification;
 - c) SMS;
 - d) Text-to-speech (TTS);
 - e) Uploaded WAV file in any language; and
 - f) Alerts via the Shadowtrack® Mobile App.
- 9) Attempts:
- a) Single or Multiple test attempts prior to non-compliant; and
 - b) Adjustable time frame between attempts.
- 10) Perform location validation:
- a) Perform silent location verification checks utilizing GPS during Sobriety tests; and
 - b) User ability to send an alert to the enrollee for live video interaction in the event of a failed Sobriety test.
- 11) User non-compliant notification types:
- a) Bridge voice call with enrollee and user;
 - b) SMS;
 - c) TTS; and
 - d) WAV.
- 12) Reporting:
- a) Detailed compliance report to include:
 - Date and time of test
 - Location of test
 - BAC Score
 - a Picture
 - b) Facial recognition score-facial recognition technology may be used to compare the image taken during the test with the reference image obtained during enrollment. We will then use the confidence score received against a facial mismatch threshold established in the Shadowtrack® application. In addition to all other data provided on the Shadowtrack® platform
 - c) Reporting methods:
 - Instant upon non-compliant event
 - Summary on a specified time table
- 13) Service Types:
- a) Sobriety tests can be a stand-alone service or incorporated with any of the other Shadowtrack® platform services.
- 14) Unscheduled Tests:
- a) If a test is received outside of a scheduled screening window, the test is considered a non-compliant event and shall be indicated as "Outside Window" under the compliance heading "Test Window"; and
 - b) Tests results received within the time allotted shall be labeled "Inside Window".
- Benefits include:
- 1) Economical—service will be provided with little to no markup on existing Shadowtrack® services;
 - 2) Ownership—enrollee owns device and can continue testing after completing court ordered program to aid in maintaining sobriety;
 - 3) Easy to use—takes less than one minute to perform screening;

30

- 4) Unobtrusive—no embarrassing leg devices that can affect employment, family life or interfere with medical conditions;
- 5) Convenient—small device—can be carried in your pocket; and
- 6) Unified platform—Integrated with all other Shadowtrack® solutions.

Caseload Management (CLM)

In a preferred embodiment, the Caseload Management service of the present invention allow the user to manage an enrollee's case while on the Shadowtrack® program.

Shadowtrack's caseload management (CLM) service provides an all-inclusive solution for users to manage their caseload more efficiently. CLM can be paired with any of Shadowtrack's other services or integrated with the agencies' existing case load management system. Users can take advantage of the CLM service by utilizing automated reminders triggered by requirement deadlines and create custom reminders and tasks that help the user and participant to stay on top of required duties. Users can also utilize the caseload calendar that allows for scheduling of appointments as well as an overall view of the participants upcoming scheduled events. The CLM service allows an agency to utilize custom mail merge documents, upload documents, attach them to the participant profile, enter free handed notes, and keep track of analytical data and demographics for participants. Shadowtrack's custom caseload reports can provide an agency with overall analytical data as a way to document demographics, crime statistics, and success/failure rates to perform caseload management studies.

Caseload Management service allows the agency to:

- 1) Integrate with all of Shadowtrack®'s modules to increase user efficiency;
- 2) Improve enrollee accountability by reminding the enrollee they have an upcoming deadline;
- 3) Obtain current records and contact information for the enrollee in a more efficient manner; and
- 4) Send scheduled and random customized notifications via text to speech, text messaging, email, or uploaded voicemail. Great for court and probation appointment reminders

Example of Caseload Management Platform Functionality

- 1) Customizable API integration capability with 3rd party software;
 - a) Import data into the Shadowtrack® application that can include but is not limited to the following:
 - Name
 - Address
 - Phone number
 - Color Code
 - Entity referral code
- 2) Conditions
 - a) Conditions are customizable per entity and can be setup up based on the individual needs of the entity;
 - b) Auto populated deadline reminders for conditions can be generated for the enrollee to improve efficiency in completing court ordered requirements; and
 - c) Ability to override any automatic notifications.
- 3) Caseload Management Events
 - a) "Requirements by Offense" button that generates a list of requirements that are based on the enrollee's offense;
 - b) Scheduled reminders sent to the enrollee based off of requirement deadlines designated by the user;
 - c) Shows the auto populated dates set by each requirement the enrollee is scheduled to complete;

31

- d) Allows the user to enter dates for program deadlines, enrollment dates, payment dates, and completion dates;
 - e) Allows the user to print a checklist that lists all condition requirements, deadlines, and Caseload Management information entered by the assigned user;
 - f) Ability to automatically notify enrollee a fixed number of days prior to completing the program of the date the program will end;
 - g) Ability to send scheduled TTS, SMS, and email notifications to the enrollee;
 - h) Option to send a text message to the user when an interview (Self-Report) is incomplete;
 - i) Logic that prevents editing of Caseload Management Notifications that have already been sent;
 - j) The ability to view time and date confirmation on the dashboard indicating that the enrollee received their reminder alert;
 - k) The enrollee profile will be automatically assigned a color to alert the user of the status of completing requirements. The requirement stages are color coded as follows:
 - GREEN—Requirement is in good standing
 - YELLOW—Requirement approaching deadline
 - ORANGE—Requirement in “Grace Period”
 - RED—Requirement passed
 - BLUE—Requirement is complete
 - l) A report will be available to the entity so they can review the color code status of each enrollee.
- 4) Calendar
- a) An event calendar per enrollee that displays all future deadline and condition requirements for the next 30 days;
 - b) Ability to schedule appointments via the calendar;
 - c) Ability to send out an appointment reminder via email one day prior to the appointment date;
 - d) The enrollee calendar will also display conditions and requirements as follows:
 - Condition due dates
 - Condition reminders
 - Appointments
 - No show
 - Drug test notification
 - Ability to see each requirement in the stage color
 - Ability to add manually caseload event
- 5) Notes
- a) Case notes can be entered by users along with an audit trail so the user name that entered the note is listed
- 6) Automated Mail Merge Letters
- a) Automated certificate of completion letter generated by the application once condition requirements have been successfully completed;
 - b) Ability to generate a “Terms and Condition” form with all program requirements merged on the document;
 - c) Transactions;
 - d) Ability to add debits and credits;
 - e) Ability to view transactions by type;
 - f) Show up to date balance on account;
 - g) Ability to send payment reminders based on payment due date; and
 - h) Auto generated transaction ID numbers.

32

- 7) Reports
- a) Recidivism reports that allow the entity to run annual reports on enrollees that have completed program requirements if the enrollee has been rearrested;
 - b) Customizable reports per entity that can display the following:
 - Misdemeanor referrals
 - Felony referrals
 - DWI referrals
 - DWI with required meetings
 - Automatic referrals
 - Number of enrollments
 - Number of appointments
 - Reports with statistical data showing the following:
 - Profile demographics
 - Charges
 - Program conditions and stage requirements
 - Completed total enrollees
 - Success rate
 - enrollee compliance
- 8) Documents
- a) Ability to upload and store documents, certificate, and test results
- 9) Contacts
- a) The ability to associate authorized contacts with the enrollee;
 - b) The ability to associate multiple contact types to an enrollee such as Caseworker, Judge, Lawyer, family member, etc.; and
 - c) The ability to identify contacts as “Share Authorized” indicating the user has permission to share information regarding the enrollee with this contact.
- 10) Authorized Lab
- a) The ability to associate an enrollee with an authorized lab location for drug testing; and
 - b) The ability to generate an automated mail merge letter to be sent to the authorized lab notifying them of enrollee information, lab requirements for testing, and that the enrollee is going to be reporting for drug testing on a specific date.
- Benefits of Caseload Management
- 1) Provides user accountability by auditing all user changes and modifications to enrollee profiles;
 - 2) Improves efficiency by allowing users to automate program condition deadlines and reminders to the enrollee;
 - 3) Increases efficiency in user Caseload Management by sending automated reports to users for enrollee’s that fail to meet program deadlines;
 - 4) Increases productivity by allowing the user to deliver messages to multiple enrollee’s one or more times;
 - 5) Allows the agency to determine the days and times that are most convenient for enrollees to report for testing, counseling, or face to face meetings;
 - 6) Provides the agency with analytical data as a way to document demographics, crime stats, success/failure rate or perform Caseload Management studies;
 - 7) Economical-service will be provided with little to no markup on existing Shadowtrack® services; and
 - 8) Calendar feature to easily manage an enrollee’s upcoming appointments, court dates, etc.

Example Mobile Application

A preferred embodiment of the “Shadowtrack®” mobile app provides the ability to monitor an enrollee using voice or facial recognition for curfew, self-reporting, location verification, and sobriety via their mobile device. The

33

mobile app features on demand push notifications for sobriety, self-reporting, curfew, and location verification, for example.

The Mobile Application May Allow the Agency to:

- 1) Conveniently complete a voice enrollment via the mobile app;
- 2) Conveniently Initiate on demand or scheduled push notifications to the enrollee;
- 3) Improve enrollee compliance by having them call into the application to complete a push notification rather than having random phone calls being placed to the enrollee;
- 4) Improve the accuracy of location verification via the mobile app;
- 5) Combat enrollee spoofing of their mobile device with built in technology to detect this; and
- 6) Monitor movement of the enrollee mobile device during lengthy periods of inactivity in the event the user suspects the enrollee is not with their mobile phone.

Example Mobile Application Platform Functionality

1) Mobile App

- Available for Android and iOS users
- Available in English and Spanish
- Scheduled and on demand push notifications to the enrollee via the mobile app for location verification, interview, voice verification, and sobriety
- Automated notification sent to the user if the enrollee fails to initiate a push notification by a specific time frame
- Alert to the user if the enrollee logs out of the mobile app at any time
- Alert to the user if the enrollee denies permission to receive notifications. If the enrollee turns off notifications at any time while utilizing the mobile app a non-compliant "Permission Denied" call will be listed on the compliance tab.
- Allows completion of sobriety push notifications during curfew outbound calls
- Improves enrollee compliance by placing multiple attempts to reach the enrollee by SMS and phone when a push notification is not responded to
- Motion detection technology so the user can monitor suspicious time periods of enrollee inactivity with the mobile phone
- Ability to obtain mobile device information like device model and version when an enrollee logs into the mobile app
- Noncompliance message displayed to enrollee that states the assigned user will be notified when they log out of the mobile app
- Silent Location verification performed when an enrollee logs out of the mobile app
- When the app receives a verification call API request, an alert will be displayed on the screen, along with a sound and vibrate, requesting that the enrollee call into the Shadowtrack® platform by clicking on the alert window. The alert cannot be dismissed and prevents use of the mobile device until the enrollee initiates the call or manually dismisses the alert
- Ability for enrollee to perform a voice verification request via the telephony network and the option to perform a verification request using a Wi-Fi data network.

34

2) Facial Recognition

Requires the enrollee to take a picture of themselves upon enrollment to ensure facial recognition accuracy;

Pairs facial recognition with Sobriety to ensure the identity of the enrollee when completing a sobriety test

Automated facial recognition triggered when a failed voice verification occurs

Ability to send a request for live video interaction between the user and the enrollee in the event of a failed facial recognition

An SMS message is sent to the enrollee once a push notification expires and the enrollee has not responded

An auto generated phone call is placed to the enrollee once a push notification expires and the SMS message has already been sent out and the enrollee still has not responded

The facial recognition threshold allows the user to easily raise or lower the enrollee facial recognition score.

Facial recognition threshold can be set at a preferred score per entity or per enrollee

Enrollee is prompted to place their face inside a designated square area on their mobile device to ensure accuracy of facial recognition during enrollment and subsequent facial recognition push notifications

3) Benefits of the Mobile Application

- 1) Improves user efficiency by preventing so many non-compliant alerts since the enrollee is calling in to report instead of receiving random calls'
- 2) Improves enrollee accountability by attempting to reach the enrollee in the event of a failure to respond to a push notification;
- 3) Improves location accuracy by obtaining location coordinates for the enrollee directly from the mobile app utilizing GPS;
- 4) Provides additional security by featuring built in technology to prevent location spoofing; and
- 5) Automated non-compliance alerts sent to the user when an enrollee logs out or deletes the mobile app.

Officer Mobile App (OMA)

The Officer Mobile App (OMA) allows the user to easily access and manage their caseload via their mobile device. The OMA allows the user to view a custom caseload summary of participants per service. User can also access compliance notifications, view tracking history, initiate on demand or scheduled verification sessions, and initiate on demand or scheduled location-based services. In addition to this, the user can send custom notifications and initiate two-way communication to the ShadoWatch™. The OMA provides a practical solution to manage one's caseload both in the office and in the field. With the user App coupled with the ShadoWatch™, the user is always in contact with the participant.

The Officer Mobile application allows the agency to:

- 1) Increase efficiency by allowing the officer the convenience of managing their caseload via their mobile device;
- 2) Increase enrollee compliance by allowing the user the ability to prompt a live interactive video session or phone call to the enrollee in the event of a non-compliance event;
- 3) Allows the user to specify custom viewing of enrollee compliance history; and

35

- 4) Increase efficiency by sending on demand or scheduled custom push notifications to the enrollee via their mobile phone.

Example Officer Mobile Application Platform Functionality

- 1) Available for multiple platforms, such as Android and iOS users;
- 2) Can be used with a mobile device, such as a phone or tablet;
- 3) On demand buttons to initiate requests or view compliance;
- 4) Allows the user to create scheduled and on demand push notifications to their enrollees for location verification, interview, voice verification, and sobriety;
- 5) Custom compliance viewing history capability that allows the user to choose viewing options for a set number of days, weeks, months, or a custom date period;
- 6) Allows the user to initiate on demand phone calls or live video interactive sessions;
- 7) Allows the user the convenience of listening to calls that result in a failed voice verification by playing the wav file from the call on their mobile device;
- 8) Allows the user to initiate on demand location verification of the enrollee;
- 9) Customizable compliance alert frequency that allows the user to designate how often they would like to receive compliance alerts such as instantly, daily, or weekly; and
- 10) Customizable administrative option for viewing permissions that restrict the user from viewing other user caseloads or entities if required.

Benefits of the Officer Mobile Application

- 1) Improves user efficiency and mobility by allowing the user to effectively monitor their caseload via their mobile device;
- 2) Improves enrollee compliance by allowing the officer to initiate on demand phone calls and live video interaction in the event of a non-compliance; and
- 3) Improves user efficiency by allowing the user to complete enrollments, make adjustments to schedules, and review compliance all from their mobile device.

Example Travel Pass

The travel pass feature allows for efficient and concise management of participants returning home from approved travel. This service works in conjunction with Shadowtrack's caller ID, voice verification, and location verification services. The service allows the user to enter "Return Dates" for the participant. The participant is then required to check into Shadowtrack's automated system by this date. If the participant fails to check in by this date, fails verification, or is found to be outside of the designated location, they will be considered non-compliant. An automated email will then be sent to the user. The travel pass feature increases participant's accountability and ensures the user is effectively managing the participant's whereabouts while on supervision.

The travel pass service allows the agency to:

- 1) Efficiently manage caseload travel requests via the application eliminating direct contact with the enrollee to verify they have returned from travel;
- 2) The automated non-compliance alert allows the user to enforce enrollee accountability to return from travel by required return dates;
- 3) Minimize the risk of a user forgetting about a travel pass request;
- 4) Verify the enrollee is back at their required location using location services; and

36

- 5) Gives the user the ability to schedule travel passes via the User Mobile Application.

Example Travel Pass Platform Functionality

- 1) Custom Shadowtrack® script that allows the enrollee the option to check in from travel. The script may play as follows:
"To notify your user that you have returned from travel, press 5"
Once 5 is pressed, we verify that the location is within the authorized radius
- 2) Ability to enable the "Return From Travel Check In" custom script only when a "Travel Pass Start Date" is entered in the application otherwise the custom script will not play;
- 3) A travel pass section listed at the top of the compliance tab to enter the travel "Start Date" and "Return Date";
- 4) Travel pass results logged on the compliance tab;
- 5) A non-compliant call logged once the "Return Date" has arrived and the enrollee has not checked in;
- 6) The ability to generate a report to view what enrollees have not completed a check in by the required "Return Date"; and
- 7) Ability to run the following reports during a specified time period:
Total travel passes requested
Total travel pass returns
Total unreturned travel passes
Total travel passes returned inside fence
Total travel passes returned outside fence

Benefits of the Travel Pass Service

- 1) Eliminates direct contact between the enrollee and user;
- 2) Automates enrollee check in from travel;
- 3) Increases enrollee accountability by automatically obtaining location information when the enrollee checks in; and
- 4) Allows the user to efficiently manage and monitor travel passes by reviewing the travel pass reports.

12. Tether

The Tether device may be paired with the Shadowtrack® mobile app via Bluetooth®, for example. In the event that Bluetooth® is disconnected, a verification call is prompted to ensure the enrollee is with their mobile device and verify Bluetooth® connection with the Tether device is re-established. A non-compliance notification will be sent to the user if Bluetooth® signal is lost or there is any attempt to tamper with or cut the Tether device strap. The user will also be notified when a signal from the Tether device is not received within a given a period of time or the enrollee is found to be outside of the designated monitoring area

12.1 the Tether Allows the Agency to:

- A. Verify the enrollee has their mobile phone and Bluetooth® is connected with the Tether device via a verification call when a Bluetooth® disconnection alert is received
- B. Confirm the Tether device Bluetooth® is re connected to the enrollee mobile device
- C. Combat possible enrollee removal or tamper of the device by sending an alert to the user when a signal from the device is not received within a given period of time
- D. Confirm the enrollee is at the required monitoring location
- E. Improve efficiency with detection of a Tether device low battery and detection of a low battery on the enrollee mobile telephone

12.2 Tether Platform Functionality

- A. Pairs with any mobile device that has Bluetooth® capability
- B. Incorporates voice verification and live video interaction in the event of a non-compliance alert
- C. Detection of Bluetooth® disconnection or inactivity during a specified period of time
- D. Detection of Tether device tampering
- E. Ability to review Tether compliance for the enrollee via the Shadowtrack® application and the user mobile app
- F. Ability to print and export compliance history
- G. Location verification performed continuously
- H. Alert to the user if enrollee is found to be outside of a designated area
- I. Sends an alert to the user when the Tether device battery is low
- J. Allows the user to send an alert to the enrollee when low battery of their mobile phone is detected

12.3 Benefits of the Tether Device

- Prevents false non-compliance by allowing the user to initiate a voice verification or live video request in the event of a non-compliance.
- Ensure enrollee accountability by verifying the Bluetooth® on the Tether device is connected
- Allows the user to be proactive by sending out alerts when a low battery on the Tether or mobile device is detected

13. Additional Application Services

- A. Import data management
- B. Import data via Excel file
- C. Application protocol interface (API)
- D. Much faster and efficient than previous versions
- E. Universal “Google-like” quick search capabilities to search for users by name, enrollee by name, telephone number, call number, ID number, and by entity name
- F. Spanish and English Text-to-speech technology converts typed phrases to voice
- G. Ability to assign multiple Users to one enrollee
- H. Ability to move a User to a different Entity
- I. Ability to move a User’s entire caseload
- J. Automatic password expiration feature for users. The feature allows the agency to require a password reset for each user upon their first login and every (x) number of days
- K. Customizable compliance tab option for users so they can filter by compliance data they prefer to see
- L. Customizable entity settings
 - User IP Address tracking that includes the following, date and time of each login, IP Address, User agent string, Browser, and Browser version

Surety

Shadowtrack® Surety Management Service (SMS) provides an electronic solution to surety companies for managing the powers they guarantee for their agencies. The SMS service allows surety companies to easily import their inventory of powers in the Shadowtrack® application. The surety company can assign those powers to various agencies, and then continue to track the progress of those powers once they have been assigned. Surety companies can also utilize this service to document and manage licenses, appointments, and contracts per agency. The SMS service includes detailed settlement reports that aid the surety company in keeping track of agency balances as well as all other aspects of surety management.

Bail

Shadowtrack® Bail management service (BMS) allows bail companies to manage their bonds and defendants. This service allows bond companies to work in conjunction with

the surety company if desired. This service can also be paired with Shadowtrack® other monitoring services including location verification using the ShadoWatch™ or mobile App, custom notifications, and Shadowtrack® participant pay solution. Bail companies can execute powers, enter detailed court information, assign bonds to agents, and keep track of defendant balances.

Watch/Bracelet

The present invention also includes a watch as shown in FIGS. 1-16. It can be used with the method and system described above. Preferably, the watch is sized for fitting comfortably on a human user’s wrist or ankle. However, other suitable means of attaching the watch to the user can be used.

The smartwatch can have the features as described above when referring to the mobile device or smartphone.

In various embodiments of the present invention, the smartwatch incorporates features described in this specification, including but not limited to one or more of the following features: Wi-Fi, GPS receiver; Network location technology; color display; tamperproof band; tamperproof watch; water-proof; motion sensors; vibration alerts; messaging; heart rate detection; blood pressure detection; ability of user to communicate with participant by using two-way voice or electronic messaging; QR activation allowing convenient and effortless activation process for users in the field; management through ShadowtrackONE™ total corrections platform; inductive charging; IP67 waterproof rating; ability to call emergency personnel; send notifications; two-way facial recognition; light sensor; software to permit biometric identification of individual wearing device; software to permit communication between device and third party or third party device; camera; microphone; interactive screen; a panic alert button; interior tracking, which is the ability to track individuals within a structure using wifi technology when GPS is not available as well as the ability to alert the user if an enrollee has a low battery on the ShadoWatch device or if the ShadoWatch device has been turned off or the battery has died.

In one or more embodiments, the ShadoWatch™ supervisor is notified any time there is a change in monitoring status of the user. In one or more embodiments, notifications are sent to a user when the participant arrives at work, school or any other location where additional arrival verification, either at one location or through a building, is necessary.

Using the ShadoWatch™ device as shown in FIGS. 1-16, the Shadowtrack® platform can be used to help reduce the risk of an abduction typical in certain foreign countries. For example, in the event of a hostage attempt, The ShadoWatch™ device will establish communication with the central monitoring facility to alert trained operators of the hostage attempt in progress. An alert is generated either by the victim, a tamper is detected by the device or the victim is outside of their safe zone. Once communication is established, the central station operator will ask the victim if they are okay via the two-way-voice function of the device. If the victim is in a hostage situation and responds by saying that all is okay, the operator will respond by asking them what their secret passphrase is. The victim has the option of responding with the phrase associated with a false alarm and that all is okay or a phrase associated with an actual kidnapping or hostage event. If the phrase matches the hostage passphrase on file, the operator will respond with by stating, “thank you Mr. or Mrs. Jones, I have verified your passphrase is correct, have a good day.” In the meantime, authorities will have been dispatched.

39

An embodiment of the present invention may include one or more of the following features:

Ability to initiate on demand requests for voice verification, interviews, location verification, facial recognition, and sobriety

Ability to send notifications via text to speech, text, email, and voicemail.

Ability to schedule one time and recurring notifications to one or multiple participants

Ability to integrate agencies caseload management systems

Automated email compliance notifications at the frequency the user desires

Ability to transfer one or more users to another entity

Ability to mass transfer one or more participants to another user or entity

Multiple custom schedule templates for fast and easy participant enrollments

Automatic transcription of audio recording

Multiple reports library as well as custom reports

Ability to view future scheduled events up to ninety days (90) in advance

Ability to create tasks for both users and participants

Custom protocols

Unlimited number of interview questions

Interview questions available in any language

Automated interview reminders

Participant mobile App

User (Officer) mobile App

Ability to locate one or multiple participants via the ShadoWatch™

Facial recognition in the event of a voice verification failure

Ability to view location tracking history via a map with location coordinates

Offender pay solution

Integration with lab or testing facilities

Also incorporated herein by reference are my U.S. patent application Ser. No. 16/041,490, filed 20 Jul. 2018, and my U.S. Provisional Patent Application Ser. No. 62/534,961, filed 20 Jul. 2017.

All measurements disclosed herein are at standard temperature and pressure, at sea level on Earth, unless indicated otherwise. All materials used or intended to be used in a human being are biocompatible, unless indicated otherwise.

The foregoing embodiments are presented by way of example only; the scope of the present invention is to be limited only by the following claims.

The invention claimed is:

1. A method of monitoring an individual, comprising the steps of:

a) providing an individual with a first wearable device and a second wearable device;

b) connecting the first wearable device and second wearable device using a wireless tether;

c) using software to set a maximum allowable distance between the first wearable device and the second wearable device;

d) connecting the first wearable device and the second wearable device to a cellular network;

e) connecting the first wearable device and the second wearable device to an internet service provider;

f) obtaining Global Positioning System (GPS) location data by the first wearable device and by the second wearable device;

40

g) obtaining internet location data from the internet router by the first wearable device and the second wearable device;

h) transmitting the GPS location data and internet location data from the first wearable device and the second wearable device to one or more servers; and

i) comparing the GPS location data and internet location data from the first wearable device and the second wearable device to determine whether the first wearable device and the second wearable device are within the maximum allowable distance.

2. The method of claim 1 wherein the first wearable device is a tamperproof wristwatch and the second wearable device is an ankle bracelet.

3. The method of claim 1 wherein the internet location data is Wireless Fidelity (WiFi) location data that is obtained at predetermined intervals.

4. The method of claim 1 wherein both the GPS location data and the internet location data is obtained at predetermined intervals.

5. The method of claim 4 wherein the GPS location data and/or the internet location data is obtained at least every minute.

6. The method of claim 4 wherein the first wearable device and the second wearable device connect to the internet service provider using an internet router.

7. The method of claim 4 wherein the GPS location data and/or the internet location data is obtained at least every 5 seconds.

8. The method of claim 4 wherein the GPS location data and/or the internet location data is obtained every second.

9. The method of claim 4 further comprising sending an alert to a supervising officer if it is determined that the individual is not within the set geolocation area.

10. The method of claim 1, further comprising the steps of:

j) receiving additional location data from the first wearable device and the second wearable device if it is determined that the first wearable device and second wearable device are not within the maximum allowable distance of each other; and

k) sending an alert if the additional location data does not demonstrate that the first wearable device and the second wearable device are within the maximum allowable distance of each other.

11. The method of claim 10 further comprising the step of:

l) sending connection data by the first wearable device and the second wearable device to the one or more servers as to whether the first wearable device and the second wearable device are connected to each other.

12. The method of claim 11 wherein the connection data is transmitted at least every minute.

13. The method of claim 10 wherein the GPS location data and internet location data are obtained at least every 30 seconds.

14. The method of claim 10 wherein the GPS location data and internet location data are obtained at least every minute.

15. A system for monitoring whether an individual is within a set location, comprising the steps of:

a) providing an individual with at least two wearable devices;

b) connecting said wearable devices to each other using a radiofrequency tether;

c) using software to set a geolocation area, wherein the geolocation area is a maximum allowable distance between the wearable devices;

d) connecting the wearable devices to a cellular network;

41

- e) connecting the wearable devices to an internet service provider using a WiFi router;
- f) obtaining GPS location data by the wearable devices at least every minute;
- g) obtaining WiFi router location data from the WiFi router by the wearable devices at least every minute;
- h) transmitting the GPS location data and WiFi location data from the wearable devices to one or more servers by the cellular network or internet service provider if the wearable devices are without a cellular network connection;
- i) comparing the GPS location data and WiFi location data from the wearable devices to determine whether all location data is within the geolocation area;
- j) receiving additional location data from the wearable devices if it is determined that not all location data is within the geolocation area; and
- k) sending an alert if the additional location data is not all within the geolocation area.

16. The system of claim **15** wherein at least one of the wearable devices comprise:

- a casing which is water-resistant;
- a tamper-proof band;
- a screen;
- a speaker;
- a microphone;
- software to permit biometric identification of the individual wearing the device;
- software to permit communication between the device and a third party or a third party device; and/or
- a camera.

17. A system for helping to prevent kidnapping, comprising:

- a computer network;
- a central monitoring facility;
- a communications network;

42

a first communication device; and
a second communication device;
wherein the first communication device is a wearable device comprising:

- a global positioning system (GPS) receiver;
- a wireless telephone communicator; and
- a panic alert button; and

wherein the second communication device is an ankle monitor; and

wherein the first and second communication devices establish communication with the central monitoring facility;

wherein the first and second communication devices are connected to a Wireless Fidelity (WiFi) router;

wherein the first and second communication devices obtain and transmit GPS location data and WiFi location data at predetermined intervals;

wherein the GPS location data and the WiFi location data from the wearable device and the ankle monitor is reviewed to determine whether all location data is within a set geolocation area, wherein the set geolocation area is a maximum allowable distance between the wearable device and the ankle monitor; and

wherein if not all location data from the wearable device and the ankle monitor is within the set geolocation area in at least two subsequent transmissions of location data, a triggering event takes place and an alert is sent to the central monitoring facility to alert trained operators of a potential hostage attempt/kidnapping in progress.

18. The system of claim **17** wherein a said predetermined interval is a time period of about 5 minutes.

19. The system of claim **17** wherein a said predetermined interval is a time period of about 1 minute.

20. The system of claim **17** wherein a said predetermined interval is a time period of about 10 seconds.

* * * * *