



US 20150042490A1

(19) **United States**

(12) **Patent Application Publication**  
**Park et al.**

(10) **Pub. No.: US 2015/0042490 A1**

(43) **Pub. Date: Feb. 12, 2015**

(54) **WIRELESS PORTABLE  
ACTIVITY-MONITORING DEVICE SYNCING**

**Publication Classification**

(71) Applicant: **Fitbit, Inc.**, San Francisco, CA (US)

(51) **Int. Cl.**  
*G08C 17/02* (2006.01)  
*H04L 12/18* (2006.01)  
*H04B 7/26* (2006.01)

(72) Inventors: **James Park**, Berkeley, CA (US); **Heiko Gernot Albert Panther**, Oakland, CA (US); **Barry Christopher Burton**, San Francisco, CA (US); **Eric Nathan Friedman**, San Francisco, CA (US)

(52) **U.S. Cl.**  
CPC *G08C 17/02* (2013.01); *H04B 7/26* (2013.01);  
*H04L 12/189* (2013.01)  
USPC ..... **340/870.16**

(21) Appl. No.: **14/523,919**

(22) Filed: **Oct. 26, 2014**

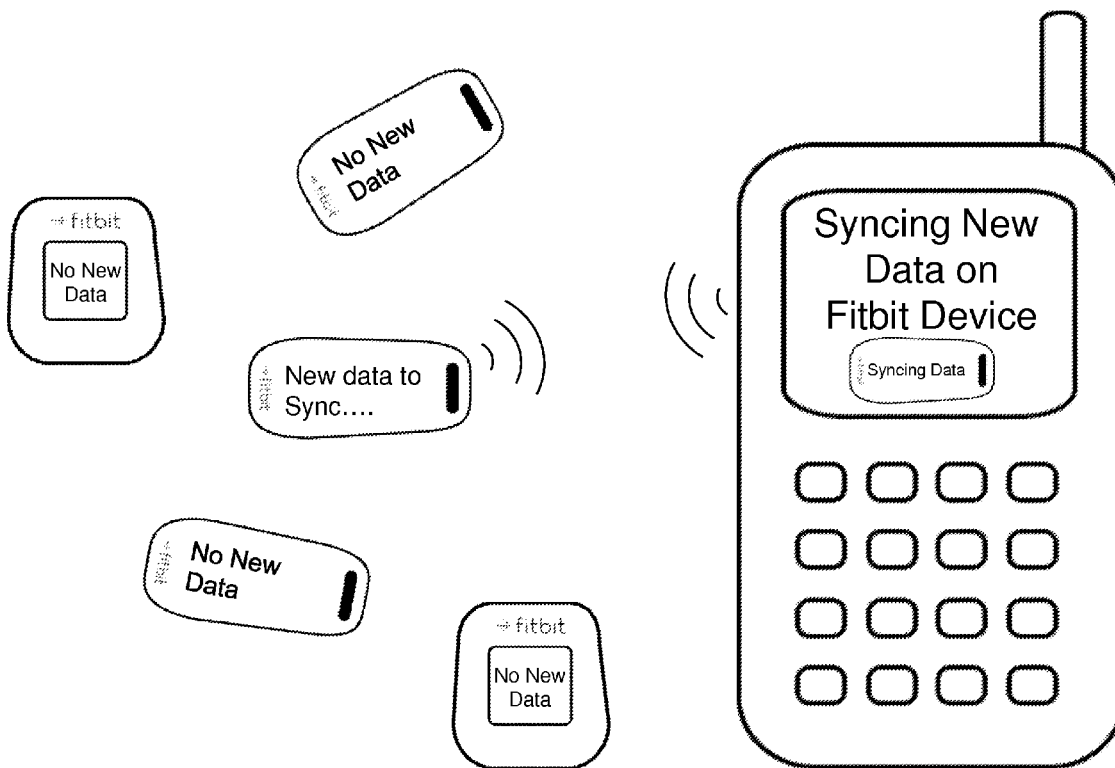
(57) **ABSTRACT**

**Related U.S. Application Data**

(63) Continuation of application No. 14/263,873, filed on Apr. 28, 2014, now Pat. No. 8,892,749, which is a continuation of application No. 14/047,852, filed on Oct. 7, 2013, now Pat. No. 8,745,247, which is a continuation of application No. 13/769,241, filed on Feb. 15, 2013, now Pat. No. 8,738,925.

(60) Provisional application No. 61/749,911, filed on Jan. 7, 2013.

A notification signal, intended to be received by a wireless communication device, is repetitively broadcast by a portable activity-monitoring device that generates user-activity data corresponding to activity of an individual bearing the portable activity-monitoring device. The notification signal conveys information that identifies the portable activity-monitoring device and indicates whether or not the portable activity-monitoring device seeks establishment of a wireless communication link to enable transmission of the user-activity data to the wireless communication device.



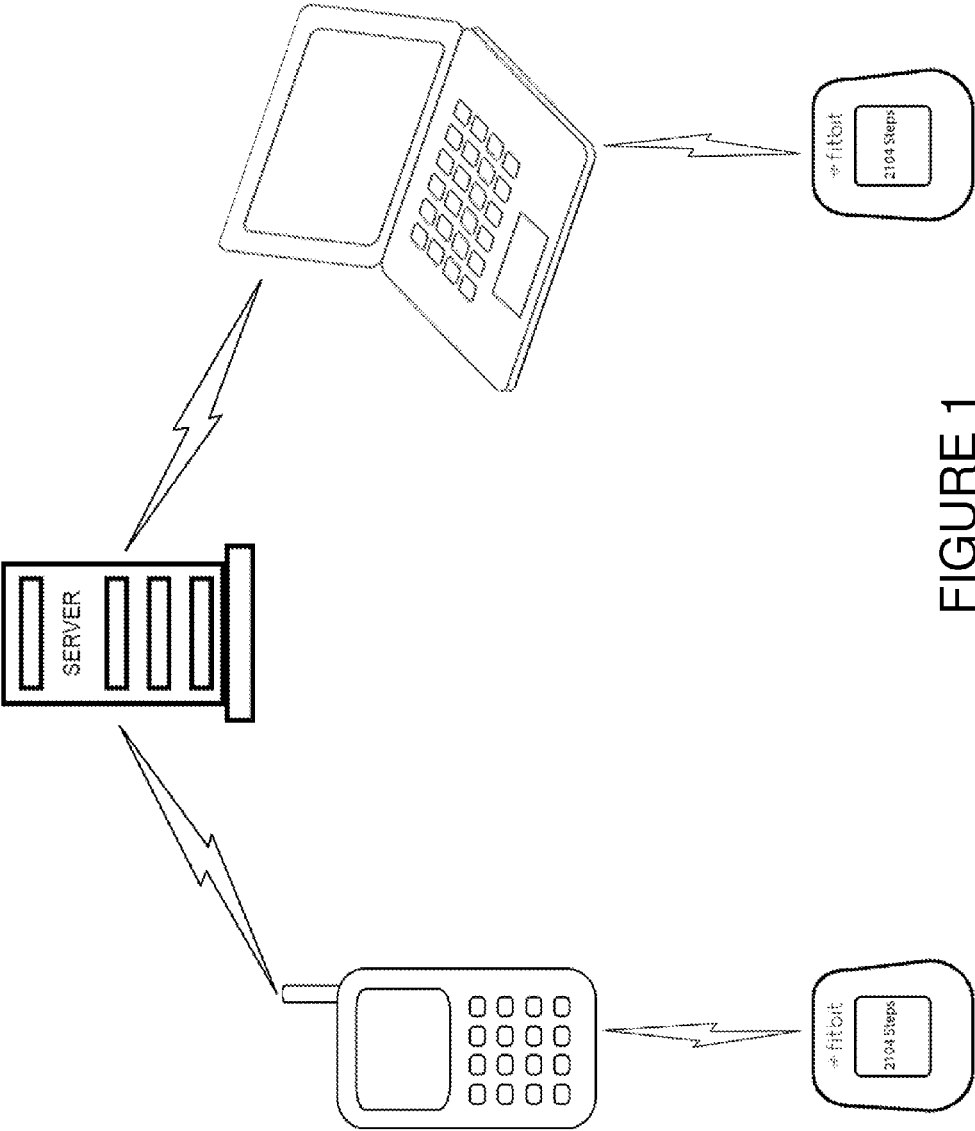


FIGURE 1

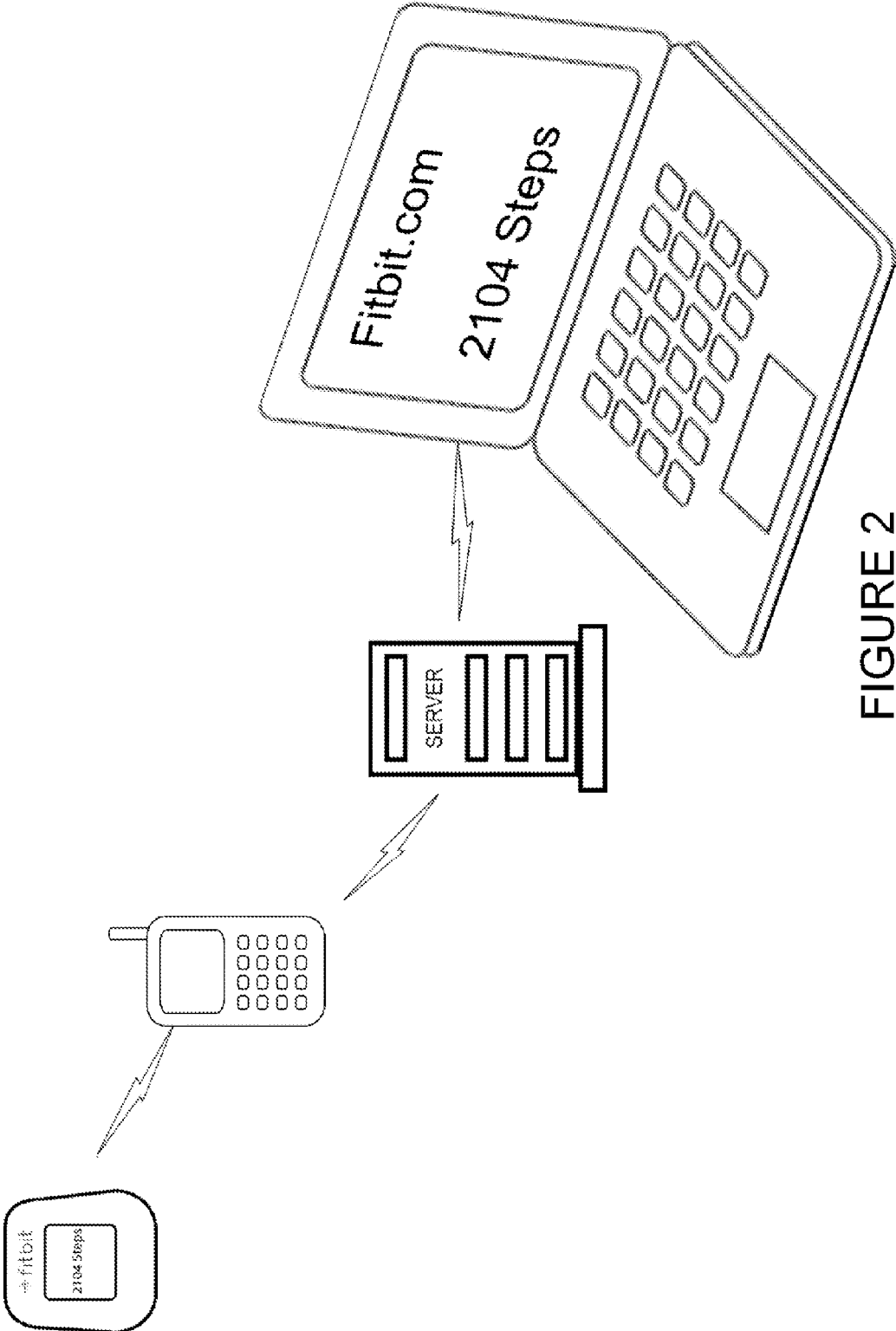


FIGURE 2

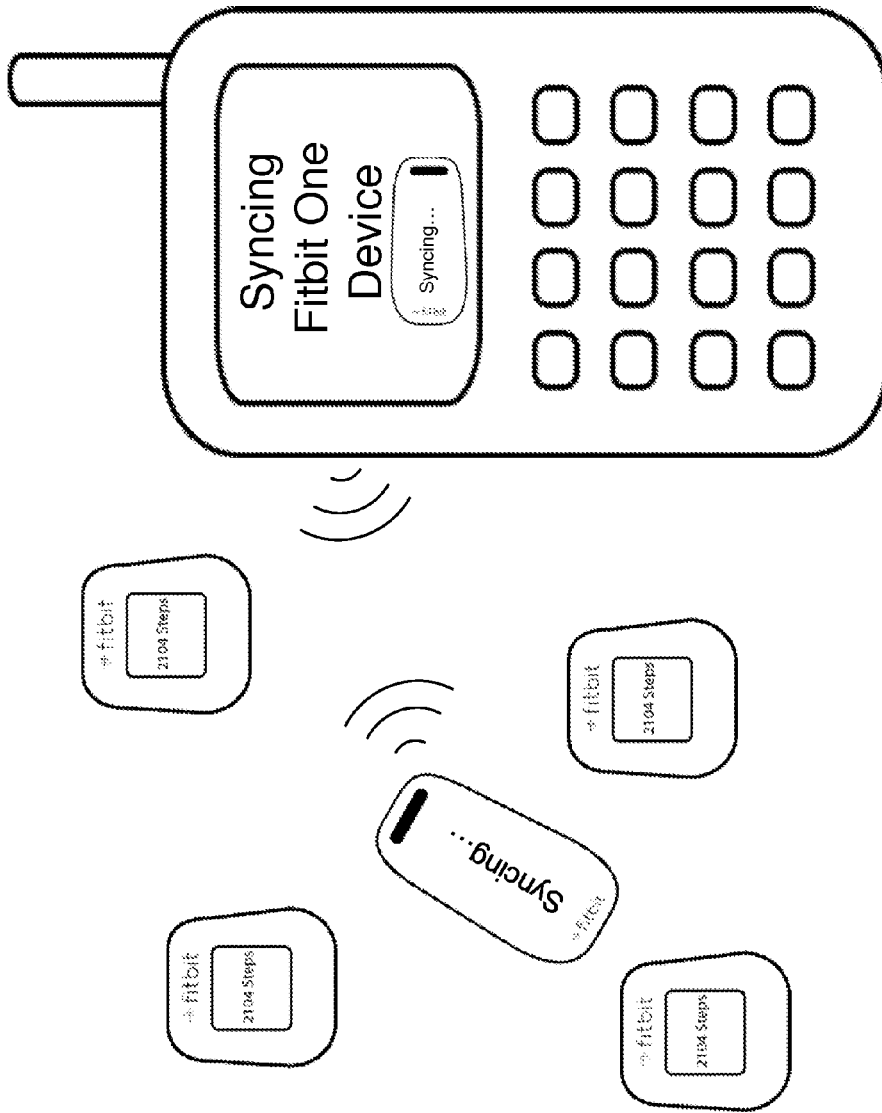


FIGURE 3

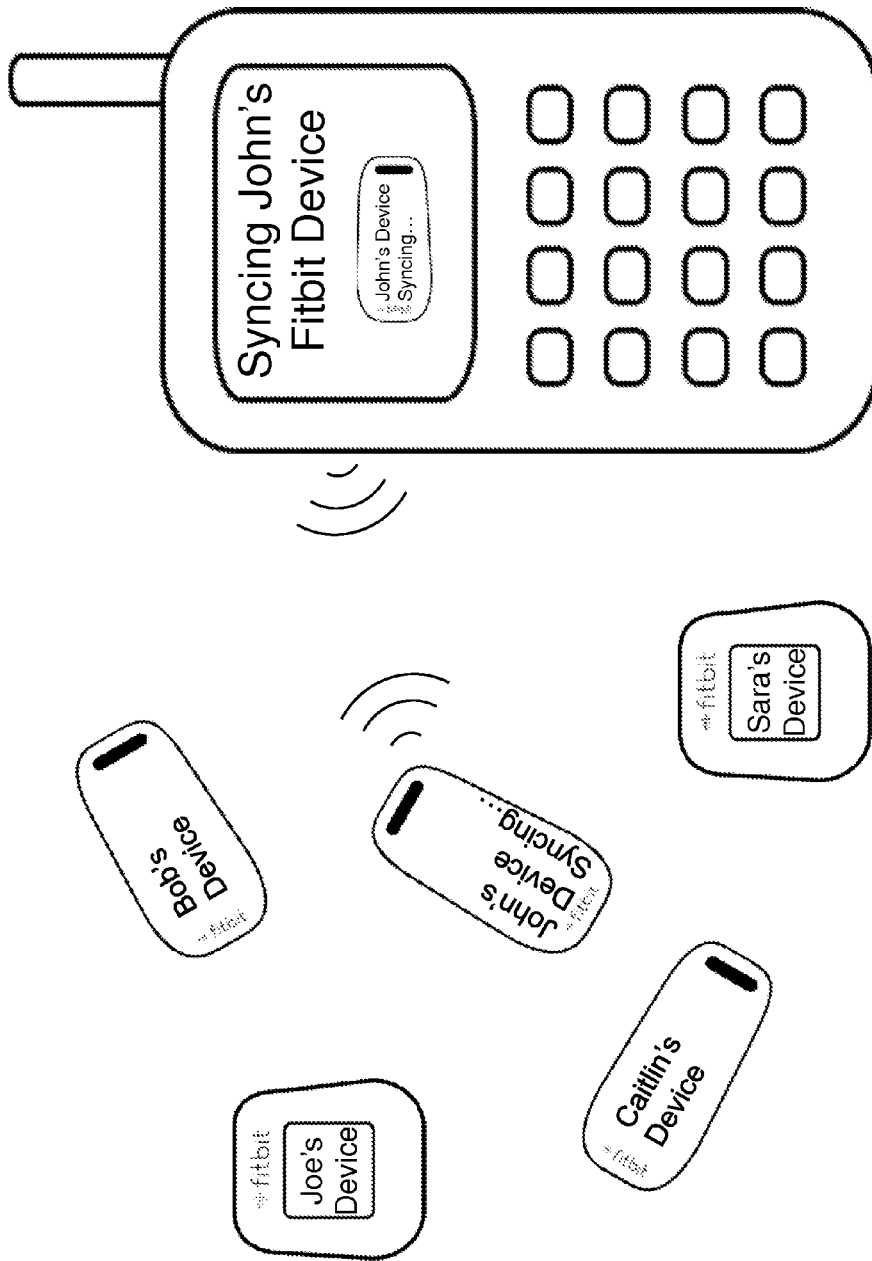


FIGURE 4

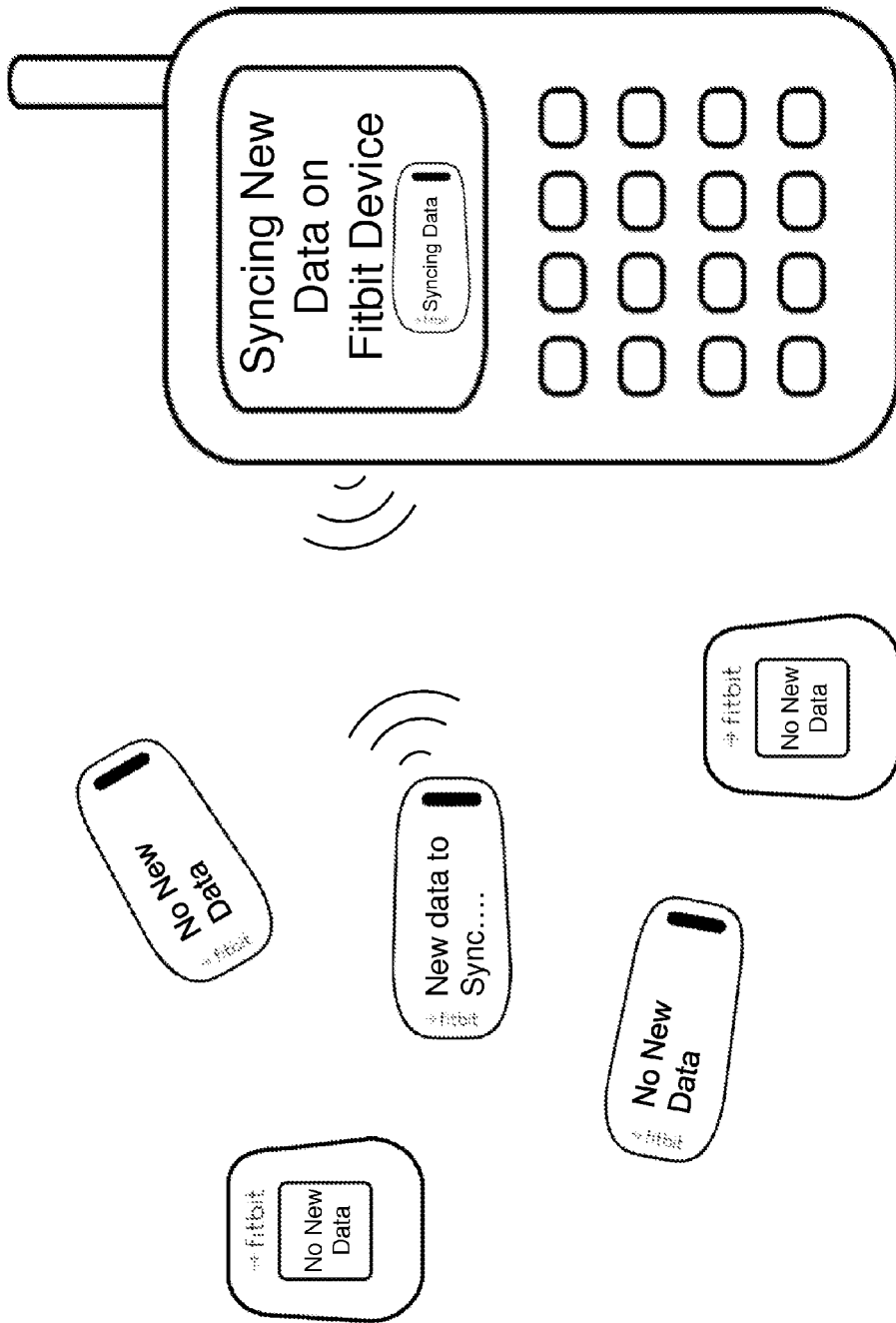


FIGURE 5

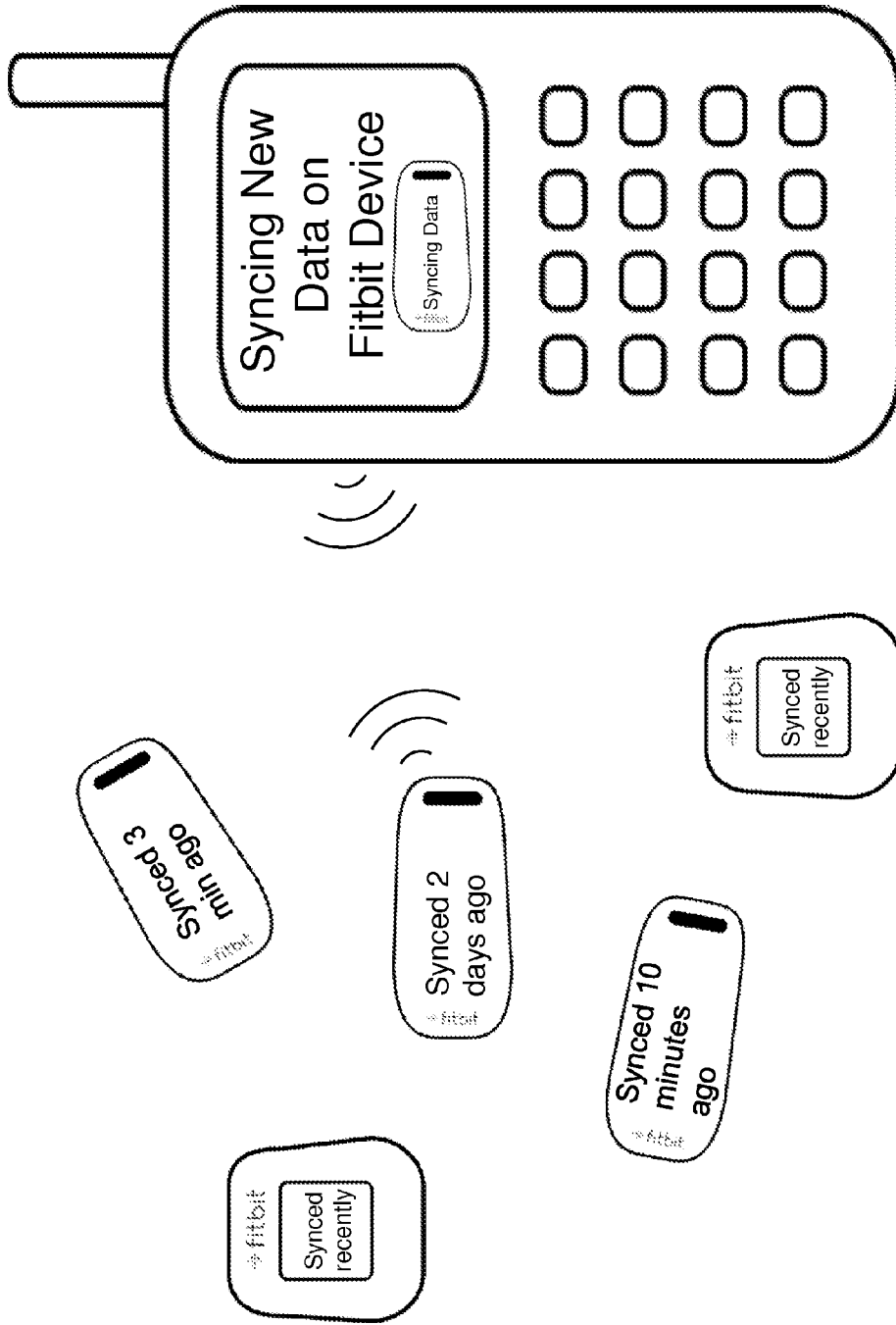


FIGURE 6

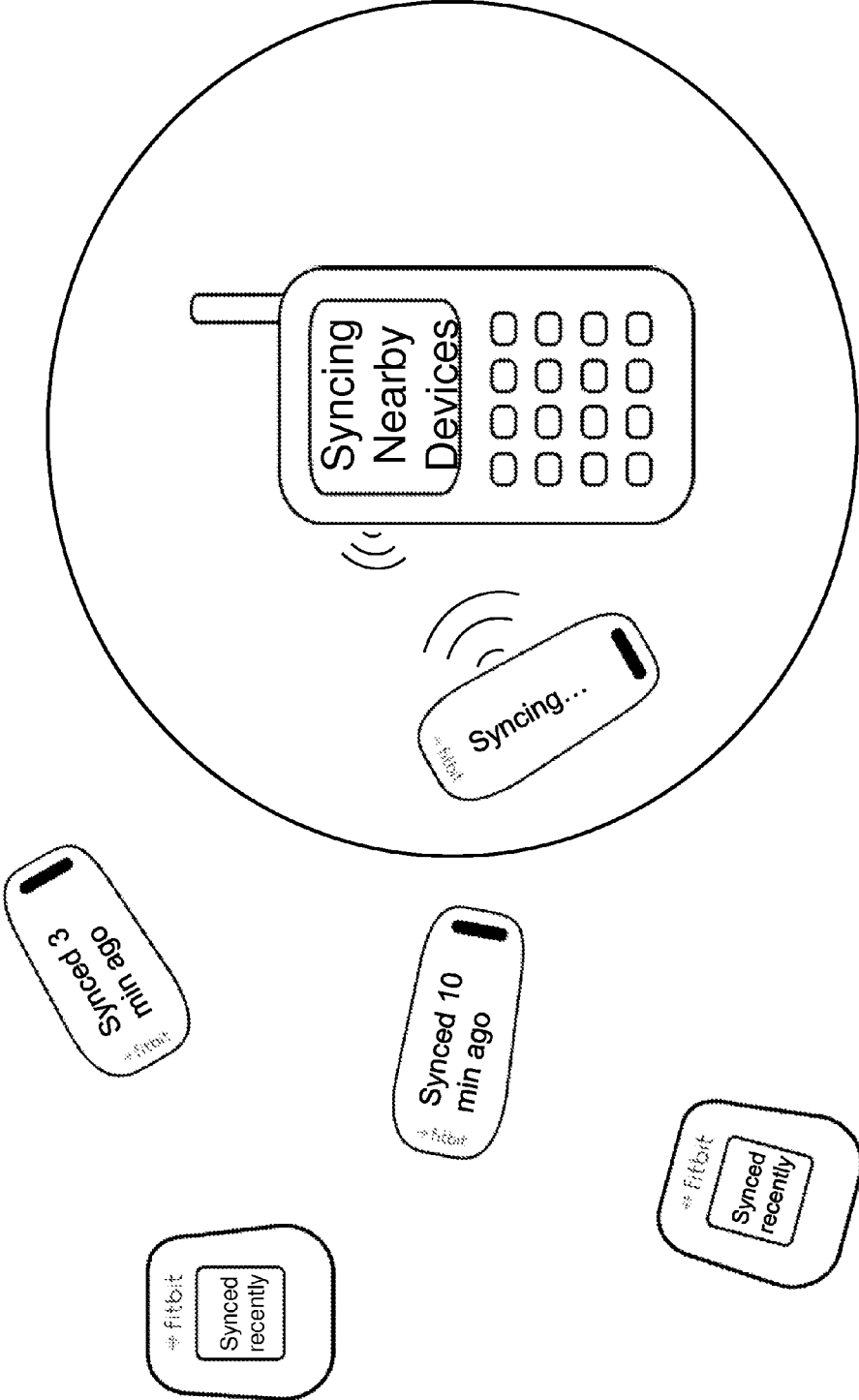


FIGURE 7



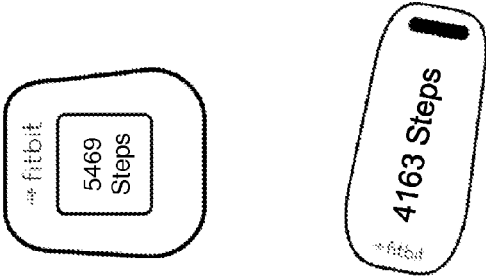
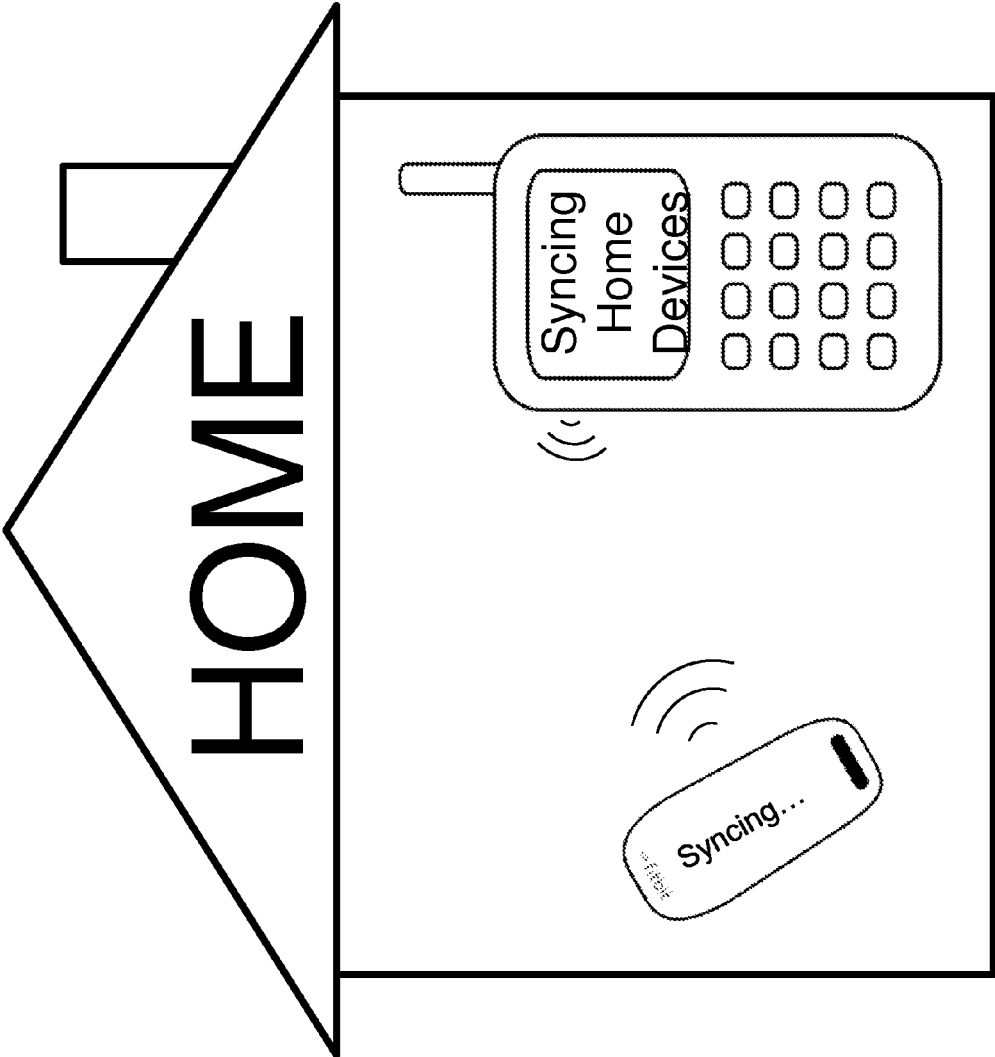


FIGURE 8

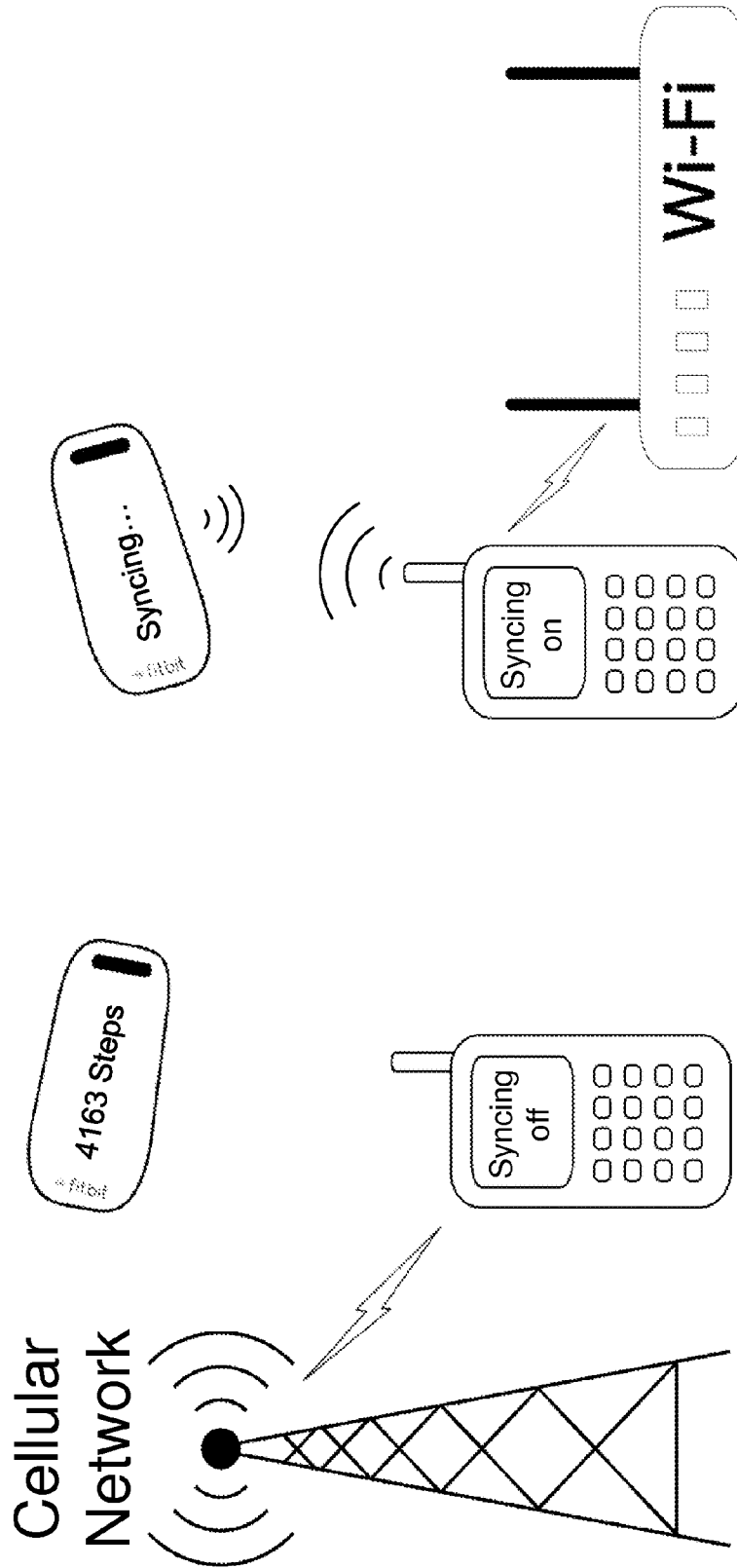


FIGURE 9

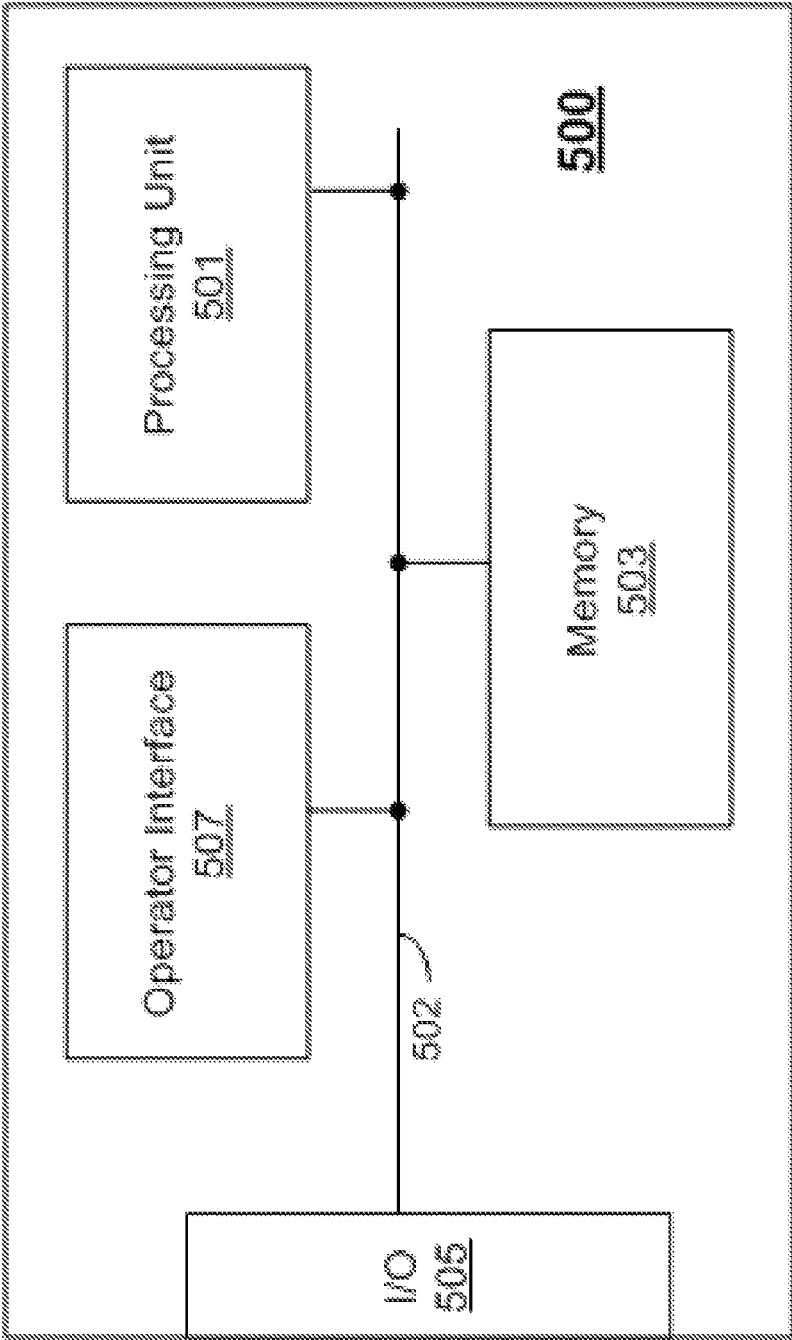


FIGURE 10

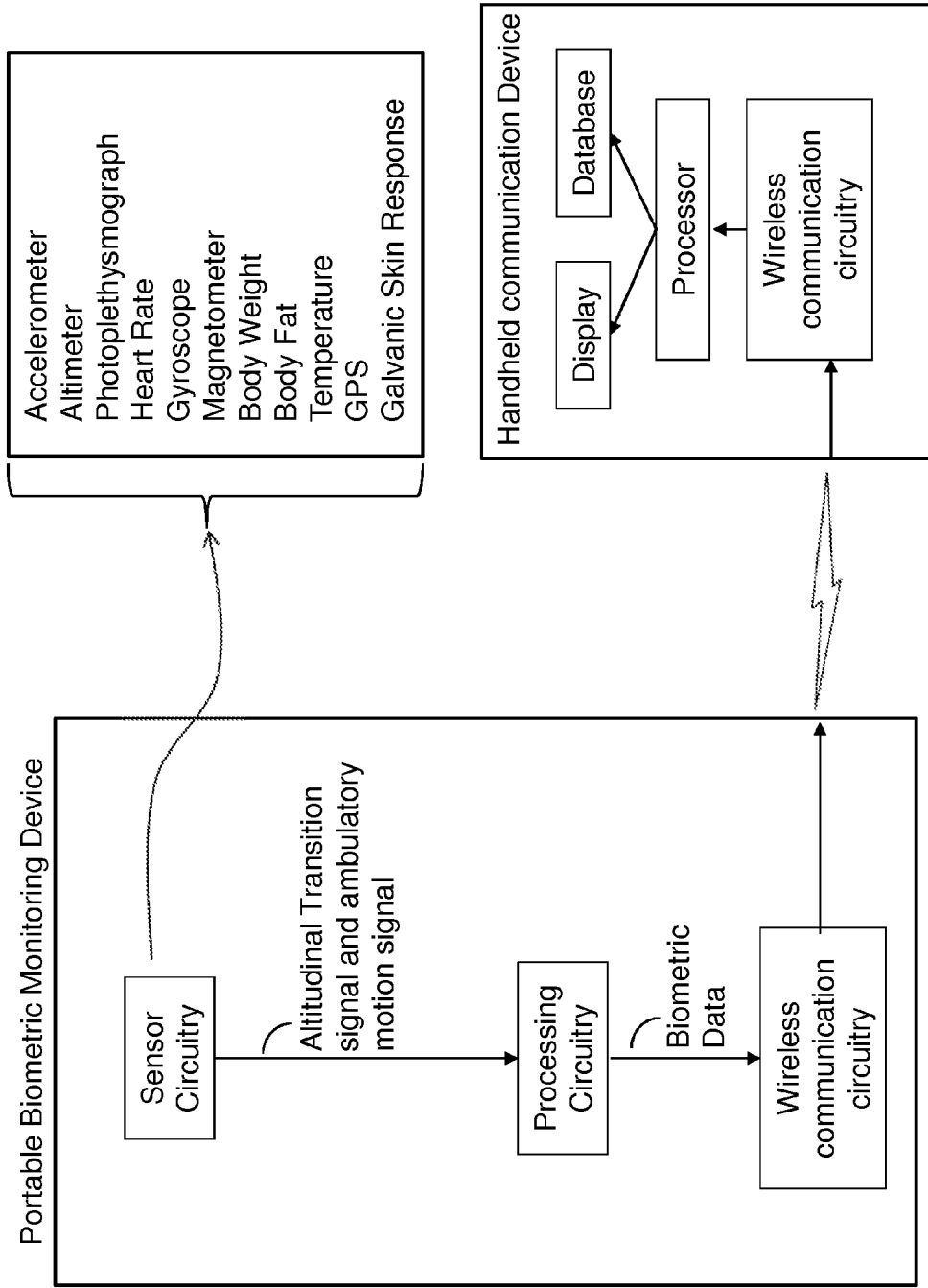


FIGURE 11

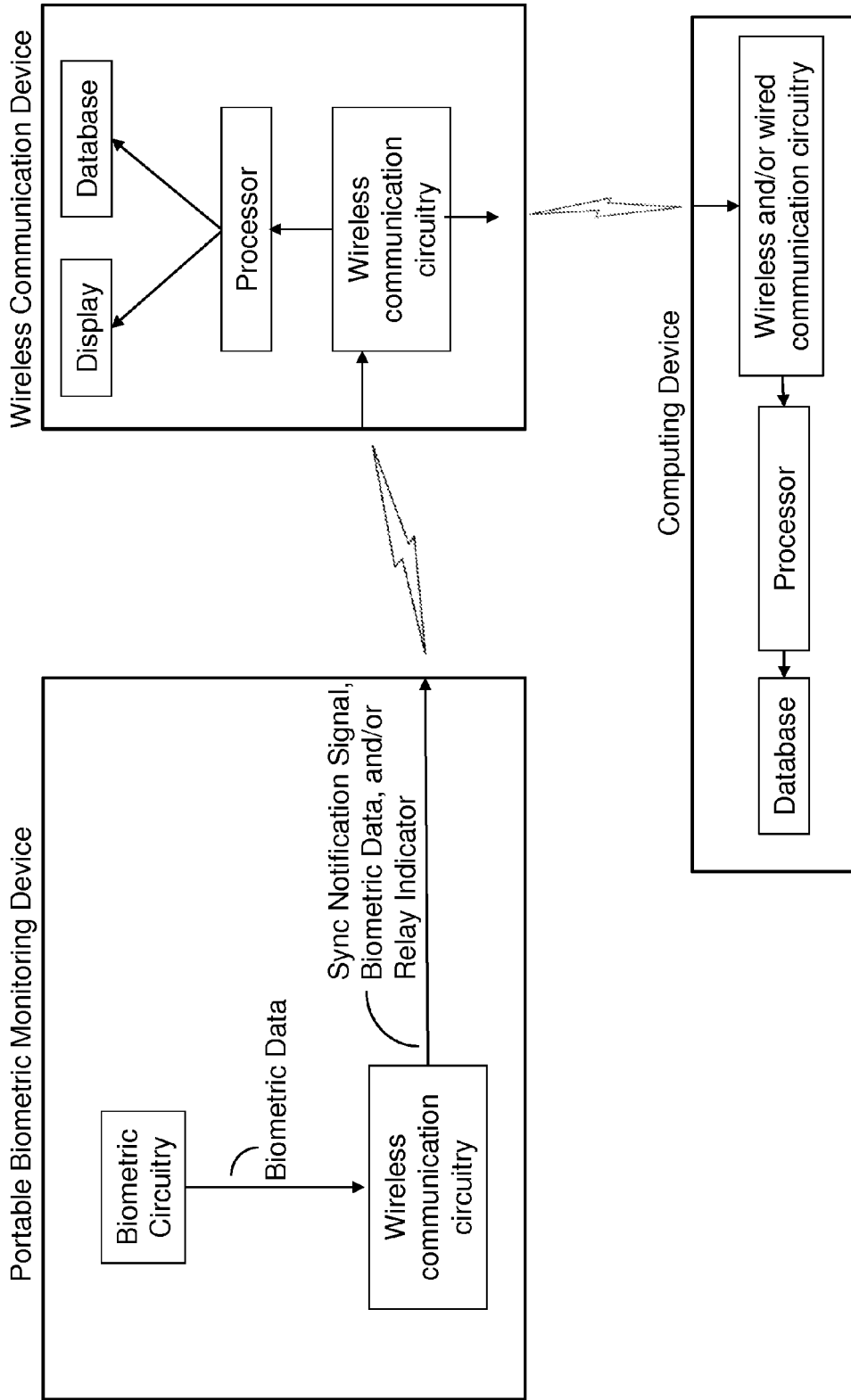


FIGURE 12

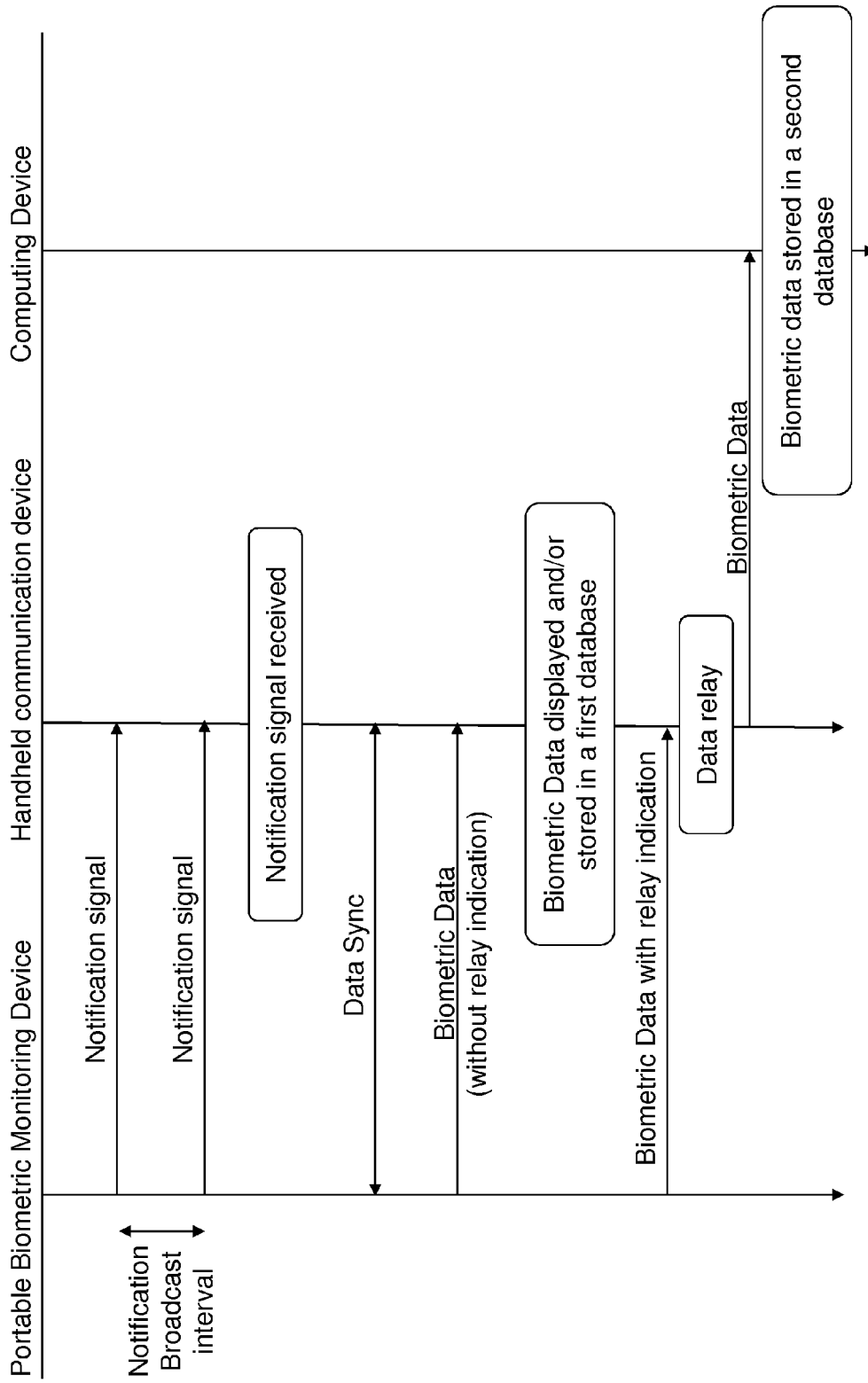


FIGURE 13

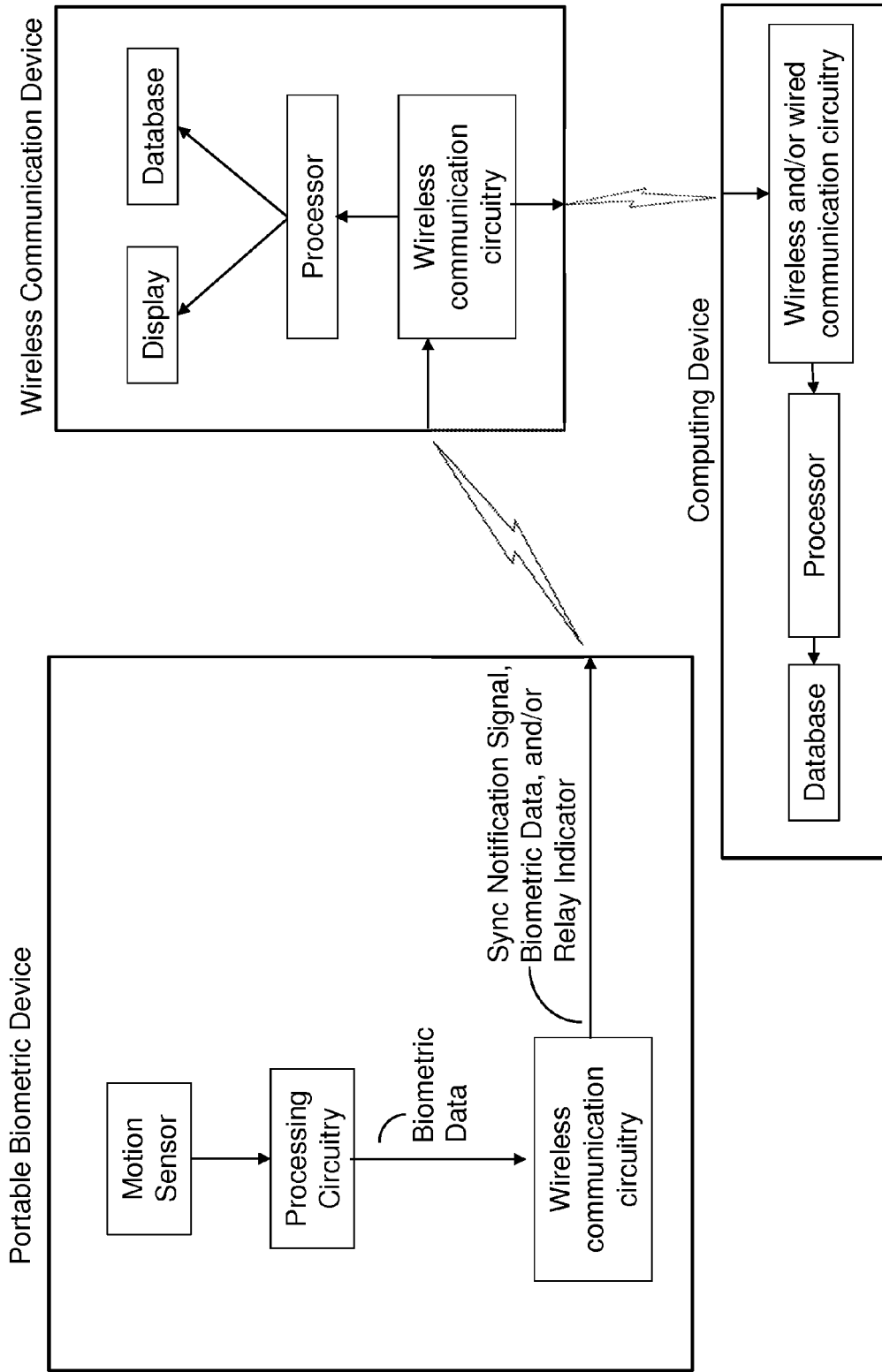


FIGURE 14

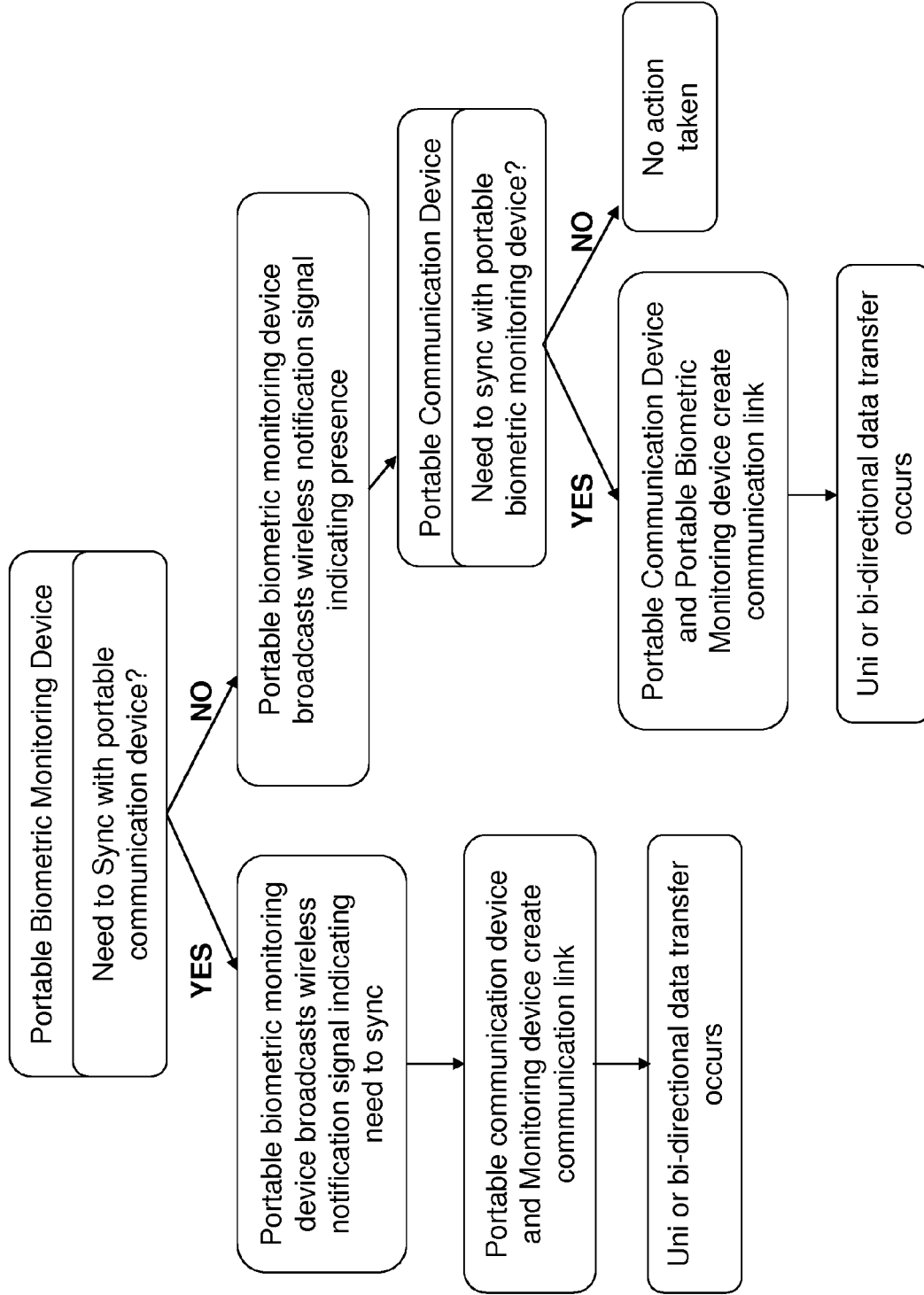


FIGURE 15



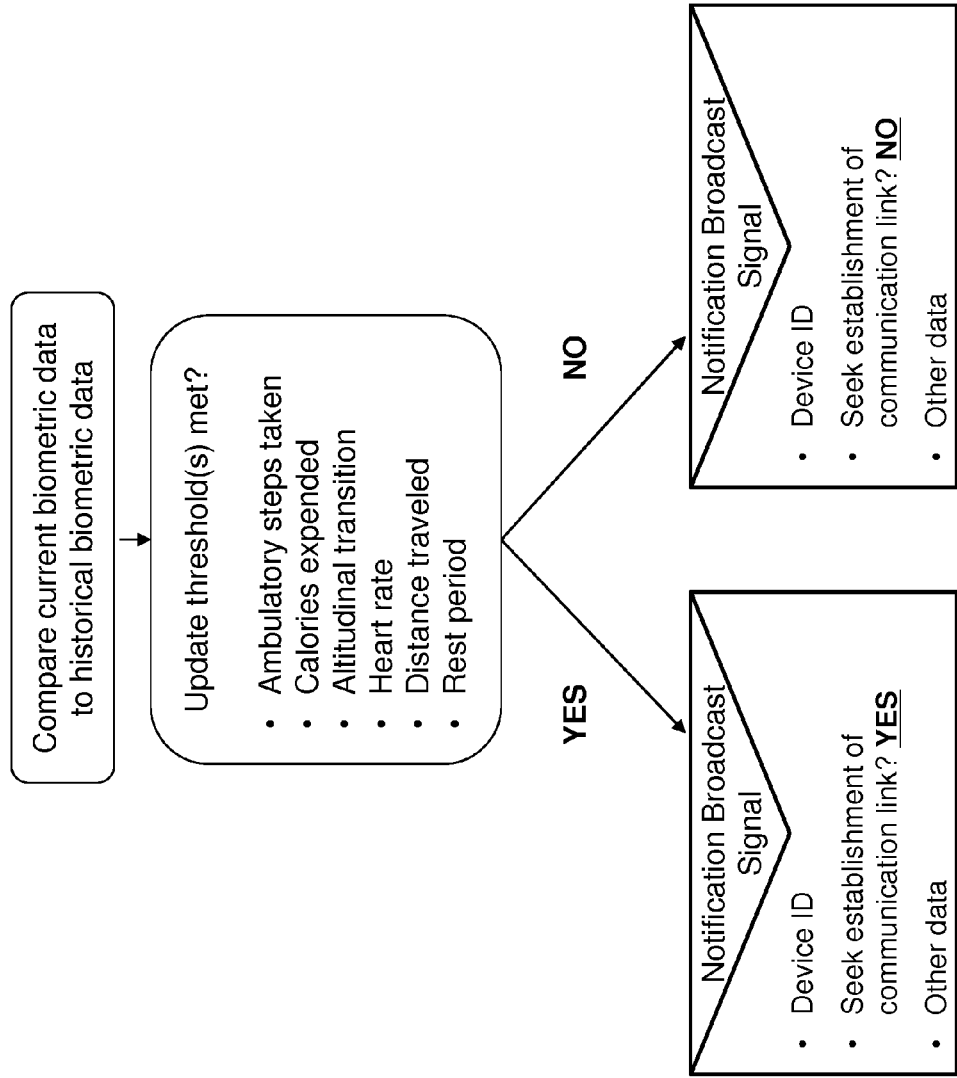


FIGURE 16

Fixed Frequency Broadcast

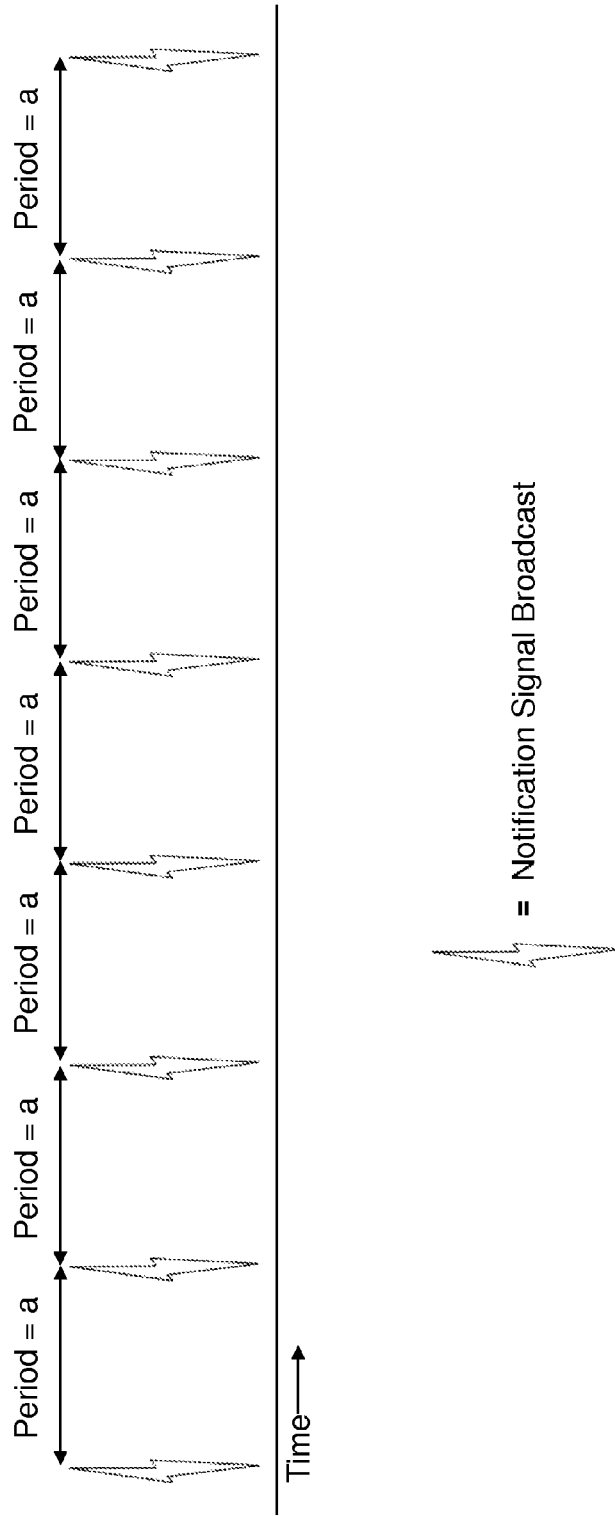


FIGURE 17

Variable Frequency Broadcast

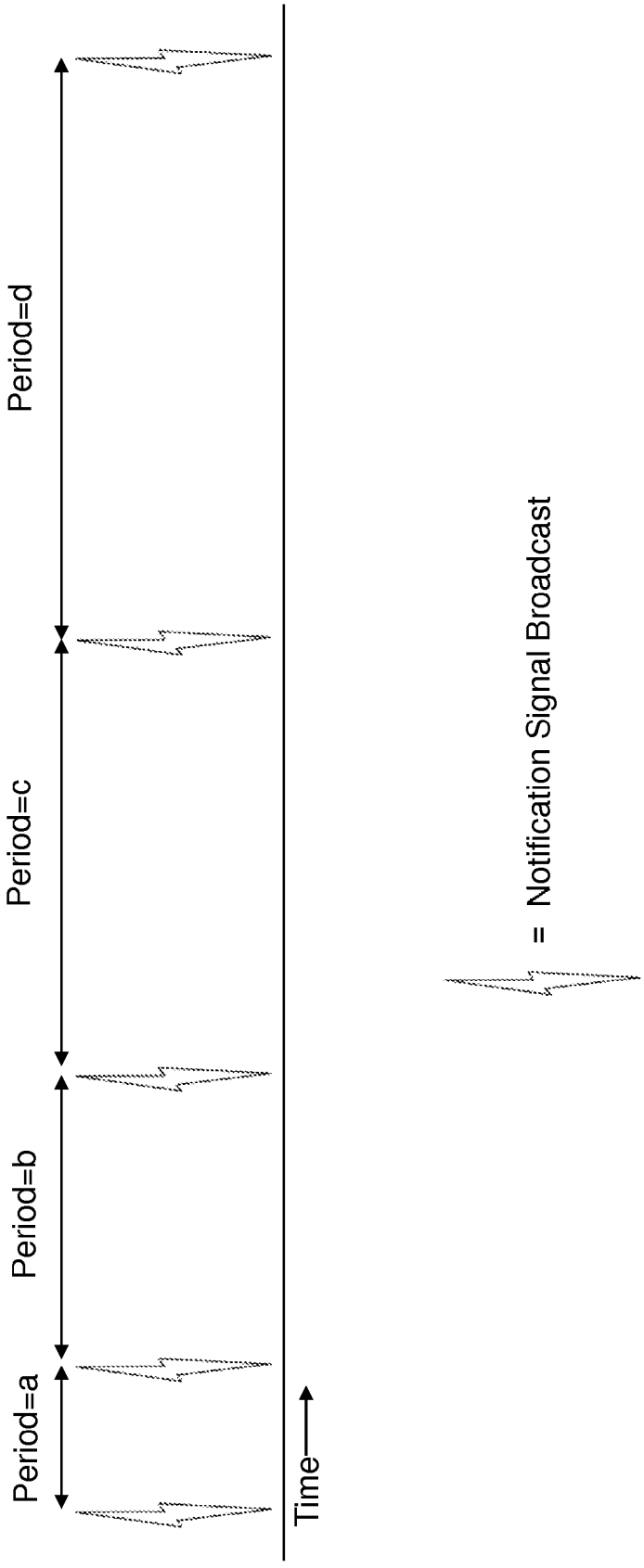


FIGURE 18

Variable and Fixed Frequency Broadcast

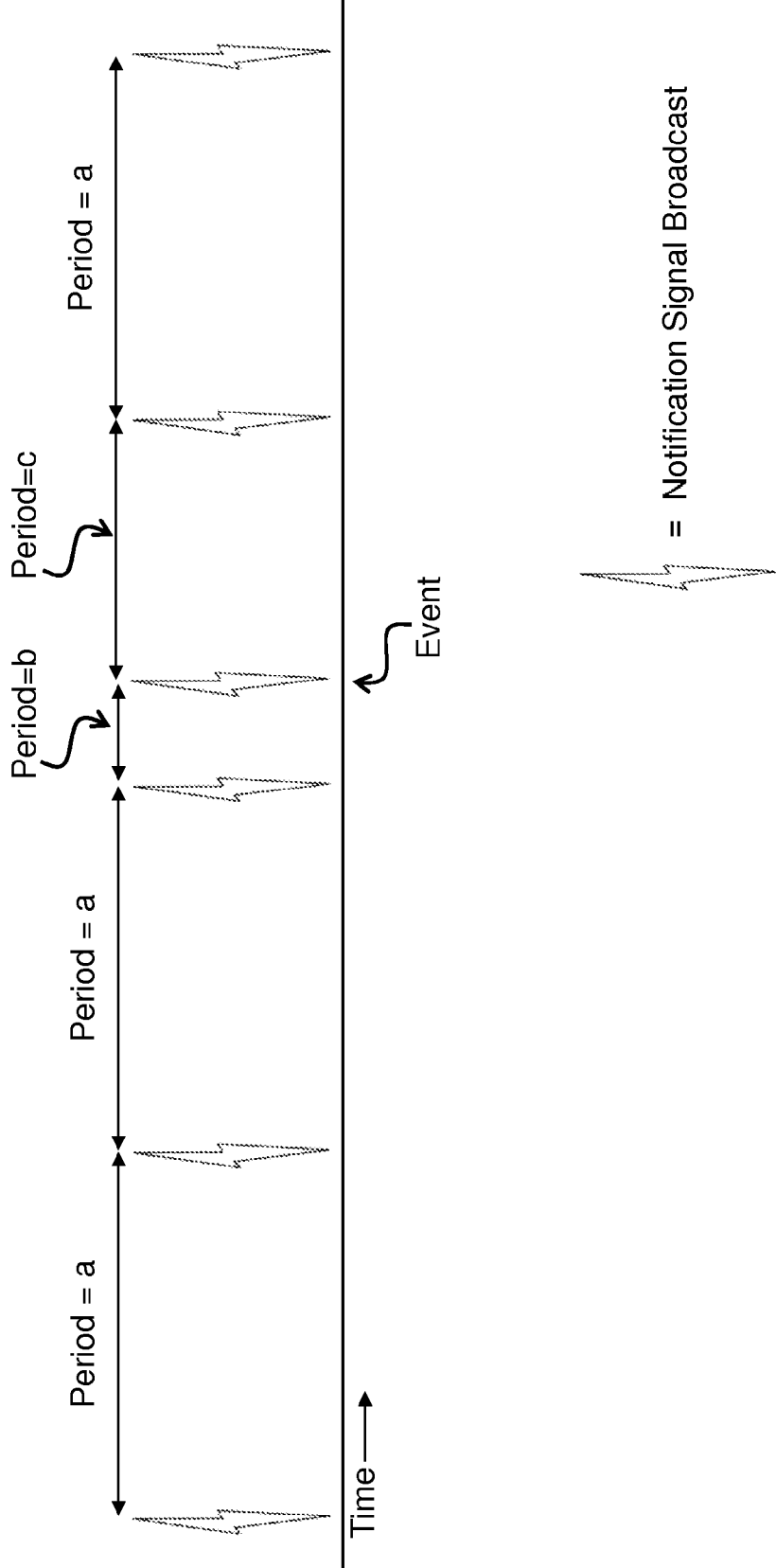


FIGURE 19

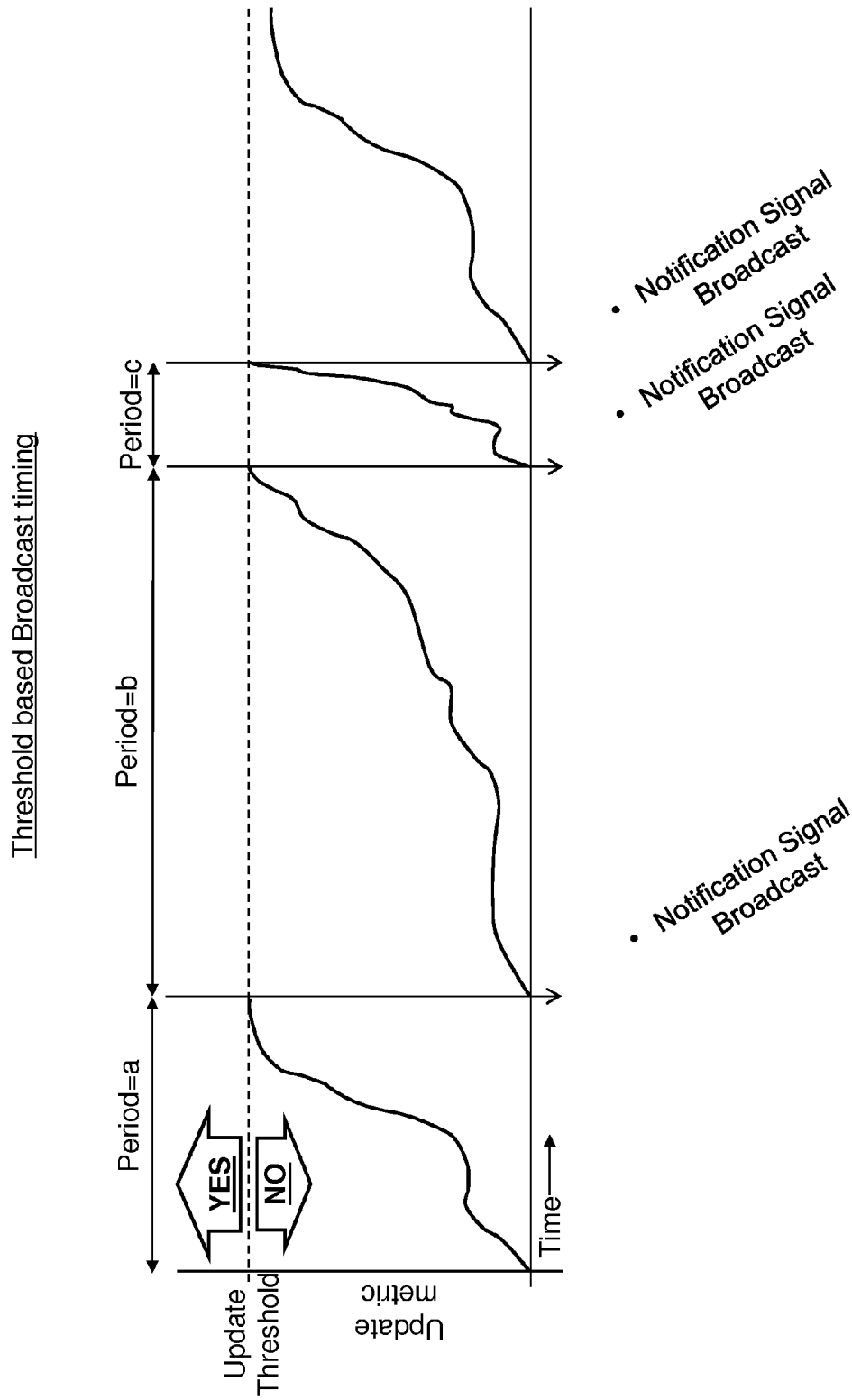


FIGURE 20

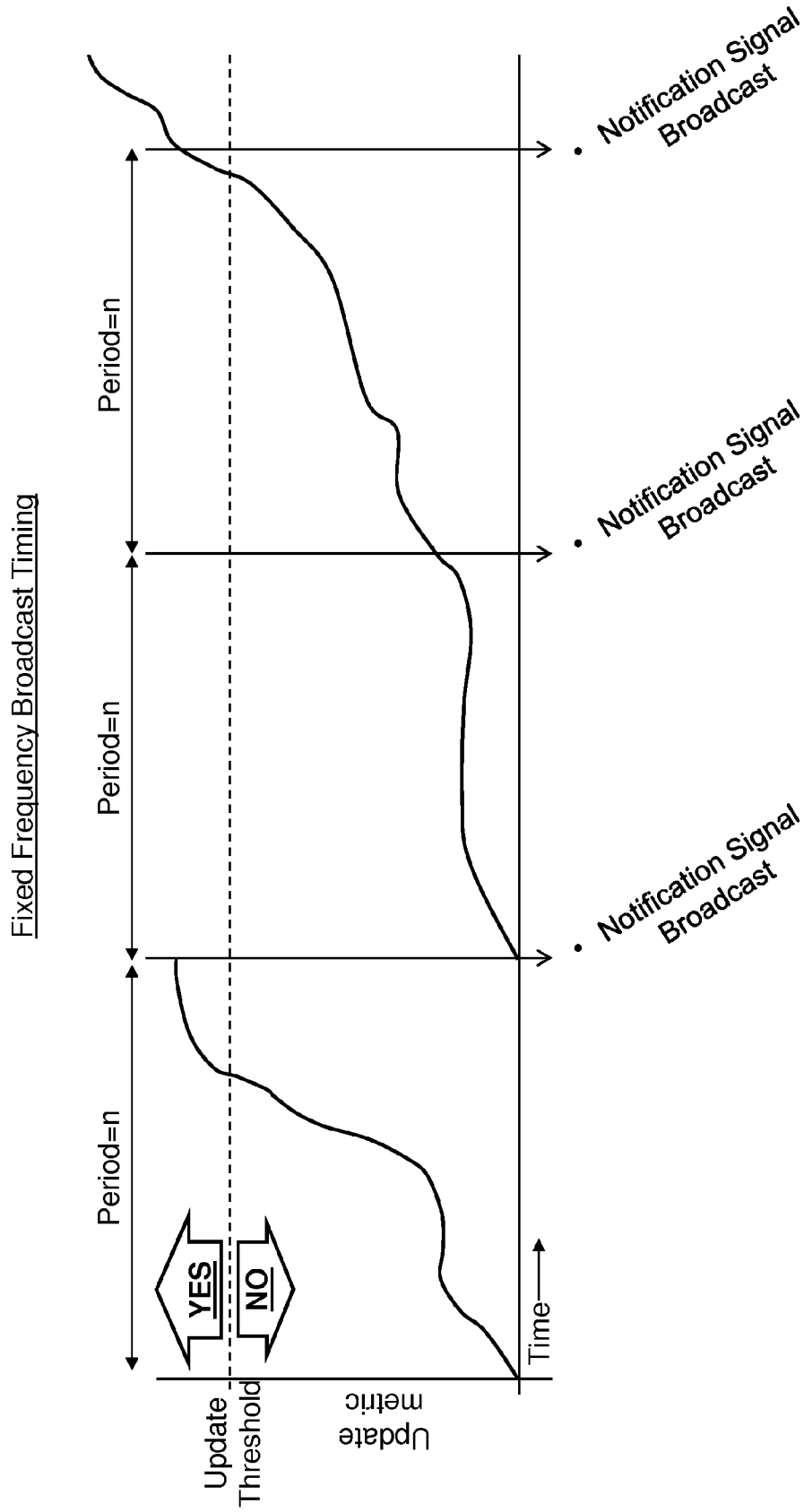


FIGURE 21

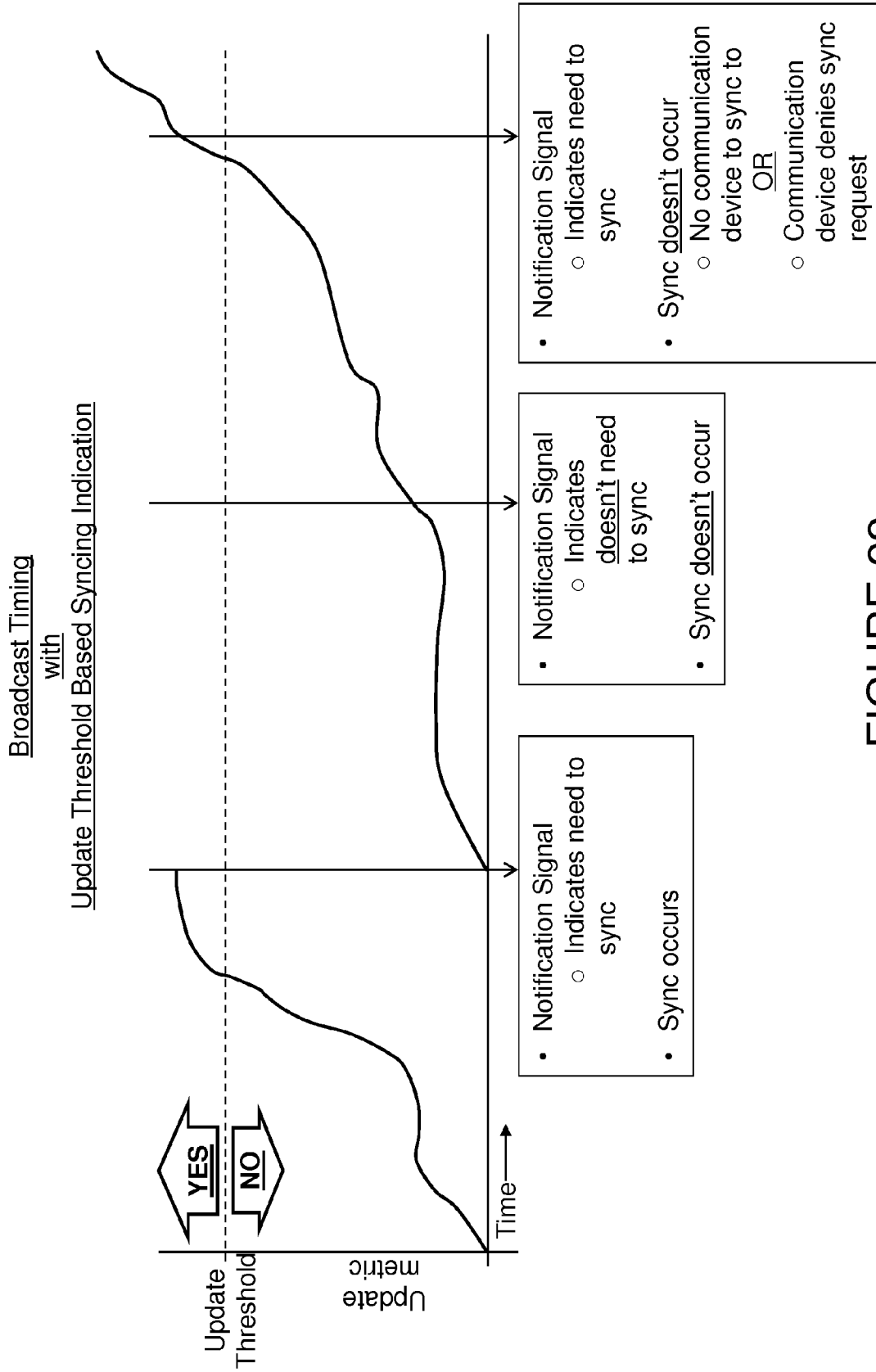


FIGURE 22

## WIRELESS PORTABLE ACTIVITY-MONITORING DEVICE SYNCING

### CROSS REFERENCE TO RELATED APPLICATIONS

**[0001]** This application is a continuation of U.S. patent application Ser. No. 14/263,873 filed Apr. 28, 2014 and entitled “Wireless Portable Activity-Monitoring Device Syncing,” which is a continuation of U.S. patent application Ser. No. 14/047,852 filed Oct. 7, 2013 and entitled “Wireless Portable Activity-Monitoring Device Syncing” (now U.S. Pat. No. 8,745,247), which is a continuation of U.S. patent application Ser. No. 13/769,241 filed Feb. 15, 2013 and entitled “Wireless Portable Biometric Device Syncing” (now U.S. Pat. No. 8,738,925), which claims the benefit of U.S. Provisional Application No. 61/749,911 filed Jan. 7, 2013 and entitled “Systems and Methods for Wireless Portable Biometric Device Syncing.” Each of the foregoing applications is hereby incorporated by reference. U.S. patent application Ser. No. 13/156,304 filed Jun. 8, 2011 and entitled “Portable Monitoring Devices and Methods of Operating Same” is also hereby incorporated by reference.

### BACKGROUND

**[0002]** The use of wired and wireless portable electronic devices continues to grow. Many individuals own and use multiple portable devices, each of which has one or more particular functions, including cell phones, personal digital assistants, navigation devices, and body monitoring or fitness-oriented devices. These devices are often used in addition to non-portable devices such as desktop computers. It is expected that these various devices can communicate with the internet and/or with each other for uploading and downloading data or otherwise transferring data. One example of a portable biometric monitoring device that communicates with the internet and other devices is a monitoring device that is intended to be small and easily worn on or about the body. When monitored data is collected by the device, it is desirable to regularly and frequently transfer the data (sometimes after on-board processing and sometimes before on-board processing) to other computing devices so that the user can easily review the data or possibly operate on it.

**[0003]** Applications or websites accessed from computing devices may allow users to see and interact with their data, providing further motivation to reach their lifestyle goals.

### BRIEF DESCRIPTION OF FIGURES

**[0004]** The various embodiments disclosed herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

**[0005]** FIG. 1 shows how a sensor device may sync data to a server using a portable communication device such as a smartphone or laptop as a network tunnel.

**[0006]** FIG. 2 shows how a sensor device may sync data to a server that subsequently distributes the data to other devices such as a laptop to enable the user to view and interact with their data.

**[0007]** FIG. 3 shows an embodiment where a communication device syncs only a specific type or model of sensor device.

**[0008]** FIG. 4 shows an embodiment where a communication device syncs only the sensor device of a specific owner.

**[0009]** FIG. 5 shows an embodiment where a communication device syncs only with sensor devices which have new data.

**[0010]** FIG. 6 shows an embodiment where a communication device syncs only with sensor devices which have not synced for a defined period of time, in this case, greater than 10 minutes ago.

**[0011]** FIG. 7 shows an embodiment where a communication device syncs only with proximal sensor devices.

**[0012]** FIG. 8 shows an embodiment where a communication device syncs only with sensor devices located in a specific region, in this case a user’s home.

**[0013]** FIG. 9 shows an embodiment where a communication device syncs only with sensor devices when connected to a specific type of network, in this case Wi-Fi and not cellular.

**[0014]** FIG. 10 shows a generalized embodiment of a computing device that may be used to implement a sensor device, communication device (or other client device), and/or server or other device in which the various operations described herein may be executed.

**[0015]** FIG. 11 shows an embodiment where altitudinal transition and or ambulatory motion signals acquired from sensor circuitry are operated on by processing circuitry to generate biometric data. This data is sent via wireless communication circuitry to a hand held communication device having wireless communication circuitry to receive the biometric data wirelessly.

**[0016]** FIG. 12 shows an embodiment where a portable biometric device wirelessly sends data to a wireless communication device that relays the data to a computing device.

**[0017]** FIG. 13 shows one example of communications between a portable biometric device, handheld communication device and computing device.

**[0018]** FIG. 14 shows an embodiment where a portable biometric monitoring device contains a motion sensor wirelessly sends data to a wireless communication device that relays the data to a computing device.

**[0019]** FIG. 15 shows the steps which occur when the portable biometric monitoring device broadcasts a notification signal to proximal communication devices.

**[0020]** FIG. 16 shows how update thresholds or sync criteria are used to determine whether the portable biometric monitoring device indicates that it would like to seek the establishment of a communication link or not in the portable biometric monitoring device’s notification broadcast signal.

**[0021]** FIG. 17 shows fixed frequency notification signal broadcast timing.

**[0022]** FIG. 18 shows variable frequency notification signal broadcast timing.

**[0023]** FIG. 19 shows a mix of variable and fixed frequency notification signal broadcast timing.

**[0024]** FIG. 20 shows a broadcast timing scheme where an update threshold is used to determine the time at which a broadcast occurs.

**[0025]** FIG. 21 shows how a fixed frequency broadcast timing scheme may define a period “n” between notification signal broadcasts.

**[0026]** FIG. 22 shows how the indication of whether or not the portable biometric device seeks the establishment of a communication link with a communication device is determined using an update threshold.



## DETAILED DESCRIPTION

**[0027]** Many users of biometric monitoring devices enjoy the ability to view and interact with their data on portable computing devices, but do not like the hassle of managing the storage and transfer of data to these portable devices. For this reason, a seamless syncing experience that requires little or no user interaction is highly desirable. Techniques disclosed herein describe how the device may automatically determine when it should transfer data, freeing the user from the having to remember when they should transfer data. It is also desirable to have a long battery life, secure data transfer, wireless data transfer and high data transfer speeds. The present invention addresses improvements over the prior art on these and other fronts.

**[0028]** More generally, various methods and systems of wirelessly syncing data to and from biometric monitoring devices are disclosed herein including, for example and without limitation, (1) a communication and/or computing device having a wireless transceiver, (2) a biometric and/or environmental sensor device (for example, an activity monitoring device such as any device described and illustrated in U.S. patent application Ser. No. 13/156,304, entitled “Portable Monitoring Devices and Methods of Operating Same”, filed Jun. 8, 2011) having one or more sensors and active and/or passive wireless transceiver circuitry. The sensor device gathers and stores data during its operation and can sync its stored data to the communication device.

**[0029]** In this document, the term “sync” refers to the action of sending and/or receiving data to and/or from a computing device and/or portable communication device as seen in FIG. 1. “Sync” may also be used in reference to sending and/or receiving data to and/or from another computing device or electronic storage devices including but not limited to a personal computer, cloud based server, and database. In some embodiments, a sync from one electronic device to another may occur through the use of one or more intermediary electronic devices acting as a portal. For example, data from a personal biometric device may be transmitted to a smart phone that relays the data to a server. The data may then be viewed on other server-connected devices as shown in FIG. 2.

**[0030]** In the case where the data is relayed from a portable biometric device to a computing device through a communication device, the data may indicate to the communication device that the data should be relayed. For example, the data transmission may contain a code that tells the communication device to relay the data. In another example, the relay indicator may not be an addenda to the message, but rather something inherent to the data itself. For example, if the data has a certain type of encryption, the encryption type may indicate that the communication device should forward the data to a computing device. Note that being unencrypted may be considered an encryption type.

**[0031]** Syncing may occur through wired and/or wireless connections including but not limited to USB, Wi-Fi, WiMAX, Mobile telephony (i.e. cellular networks), Bluetooth, Bluetooth Smart, NFC, RFID, and ANT.

**[0032]** In this document, the term “communication device” refers to an electronic computing device having a wireless transceiver. Communication devices may include but are not limited to cell phones, smart phones, tablet computers, notebooks, laptops, personal data assistants, and desktop computers.

**[0033]** In this document, the term “client” refers to client software or a client device that primarily acts as an access

portal to a server. The term “server” refers to a server in communication, directly or indirectly, with one or more of the device and the client. In some embodiments, the server may be eliminated from this system, making the client serve the functions of both the client and server.

**[0034]** Devices which are not considered portable biometric devices, but may use syncing methods according to the invention disclosed herein include but are not limited to portable or non-portable devices such as weight scales, body fat scales, exercise equipment, blood glucose meters, pulse oximeters, blood pressure cuffs, and, in one embodiment mobile phones. A weight scale may be used to describe a device which has a platform capable of supporting the weight of a user. The scale may contain a plurality of sensors including, but not limited to Body Impedance or BIA sensors to measure body fat, weight sensors, ambient light sensors, and photoplethysmographic sensors.

**[0035]** The portable biometric monitoring device (also referred to herein simply as “the device”) has a shape and size that is adapted to be easily worn about the body of a user. The device collects one or more types of physiological and/or environmental data from embedded sensors and/or external devices and communicates or relays such information to other devices or other internet-viewable sources. Notably, the device collects data regarding altitudinal transitions (e.g. climbing stairs) and ambulatory motion (e.g. walking or running). In one example, the user is wearing a device which monitors certain conditions through one or more sensors, and collects data from the sensors. For example, the device can calculate the user’s step count from collected data, store the step count, then subsequently transmit user data representative of the step count to an account on a web service (such as [www.fitbit.com](http://www.fitbit.com), for example) where the user data is stored, processed, and viewed by the user. Indeed, the device may monitor, measure or calculate many other physiological metrics in addition to, or in place of, the step count. These include, but are not limited to, energy expenditure, floors climbed or descended, heart rate, heart rate variability, heart rate recovery, location and/or heading (e.g., using global positioning system (GPS) components), elevation, ambulatory speed and/or distance traveled, swimming lap count, bicycle distance and/or speed, blood pressure, blood glucose, skin conduction, skin and/or body temperature, electromyography, electroencephalography, weight, body fat, and respiration rate. The circuitry used to sense and/or calculate these metrics is referred to herein as biometric circuitry. The device may also measure or calculate metrics related to the environment around the user such as barometric pressure, weather conditions, light exposure, noise exposure, and magnetic field.

**[0036]** The device may incorporate one or more user interface and/or feedback methods such as visual methods, auditory methods, or haptic methods (such as touch input or vibration). The device may display the state of one or more of the information types available and/or being tracked. For example, information can be displayed graphically, or conveyed by the intensity and/or color of one or more light emitting diodes (LEDs). The user interface may also be used to display data from other devices or internet sources. The device may also provide haptic feedback to the user through, for instance, the vibration of a motor or a change in texture or shape of the device.

**[0037]** In one embodiment, the device may not have a display. The device may instead communicate information to the user using one of the other user feedback methods described

herein (e.g. one or more LED's, haptic feedback, audio feedback). In another embodiment, the device may not communicate information to the user directly. Instead, the user may view their information on one or more secondary computing devices in direct or indirect communication with the device. In the case that the communication is indirect, data may be transferred from the device to one or more intermediate communication devices (e.g. smart phone) which then forwards the information to the secondary computing device used to view data. For example, data may be transferred from the device through a smartphone to a server that hosts a website containing the user's data. The user can then view their data through a compatible web browser on any internet connected computing device.

**[0038]** An embodiment where a portable biometric device wirelessly sends a sync notification signal to prompt a second nearby wireless communication devices to communicate with the device is shown in FIG. 12. Once a communication link has been established, biometric data may be sent with or without an indication that the data should be relayed to a third computing device. If the wireless transmission does not indicate that the data should be relayed, the data is displayed and/or stored on the second wireless communication device. If the wireless transmission indicates that data should be relayed, the wireless communication device communicates over one or more wired or wireless communication networks to relay the data to a third computing device which stores the data in a database. The relayed data may also be stored or displayed on the wireless communication device.

**[0039]** One example of communications between a portable biometric device, handheld communication device and computing device is illustrated in FIG. 13. Initially the portable biometric device may send a notification signal to notify any nearby handheld communication devices of its presence. Once a handheld communication device receives one of these alerts, the handheld communication device may sync data with the portable biometric device. Biometric data which is sent to the communication device without an indication that the data should be relayed is displayed and/or stored on a first database on the communication device. Data with a relay indication is forwarded onto a computing device where the data is stored in a second database. Relayed data may also be displayed and stored on the communication device.

**[0040]** In one embodiment a portable biometric monitoring device contains a motion sensor. Motion sensor data is operated on by processing circuitry to create biometric data. The portable biometric device wirelessly sends a sync notification signal to prompt a second nearby wireless communication devices to communicate with the device. Once a communication link has been established, biometric data may be sent with or without an indication that the data should be relayed to a third computing device. If the wireless transmission does not indicate that the data should be relayed, the data is displayed and/or stored on the second wireless communication device. If the wireless transmission indicates that the data should be relayed, the wireless communication device communicates over one or more wired or wireless communication networks to relay the data to a third computing device which stores the data in a database as shown in FIG. 14. The relayed data may also be stored and/or displayed on the wireless communication device.

**[0041]** An exemplary set of operations executed when the portable biometric monitoring device intermittently (i.e., periodically or aperiodically) broadcasts a notification signal

to proximal communication devices is shown in FIG. 15. The portable biometric monitoring device may indicate, in the notification signal or a characteristic of the notification signal, whether the portable biometric monitoring device seeks (or requests) to sync or establish a communication link with the communication device. In the case that the portable biometric monitoring device does not seek to establish a communication link with the communication device, the communication device may still take action to establish a communication link and sync or not (e.g., the communication device may itself have data to be transmitted to the portable biometric monitoring device in a sync operation and thus may seek to establish a communication link even if the portable biometric monitoring device does not). In the case that the portable biometric monitoring device does seek to establish a communication link with the communication device, the communication device can decide to accept or reject the portable biometric monitoring device's request to establish a communication link and/or sync.

**[0042]** Data from the portable biometric device such as those disclosed herein may be used by an application or service located on a portable communication device (e.g. smart phone), computing device (e.g. personal computer), portable computing device (e.g. laptop or tablet computer), and/or accessed through a network such as the internet through a network connected browser or application. Users of portable biometric monitoring devices may have accounts on such applications or services which allow them to retrieve data relevant to themselves or other users. An account may enable a user to visualize their data, modify data visualizations, modify or enter additional or existing data, manage their devices, and/or interact with other users. Data synced from the portable biometric monitoring device may be used for account features including but not limited to a leader board where the user is ranked compared to other users such as friends, rankings of members of a group of users, and badge awards to reaching various goals. The user account may also automatically provide recommendations to the user so as to help them reach one or more goals including but not limited to increasing or decreasing their weight, body fat, time asleep, quality of sleep, calorie burn, activity level, resting heart rate, active heart rate, normal heart rate, steps taken, distance walked and/or run, and floors climbed. These recommendations may aid the user in short term and/or long term goals. For example, if a user has been less active over the last month and has started to gain weight, they may be recommended to be more active this month through a notification on their web based account. On a shorter time scale, a user may be recommended to eat less for dinner if they were not very active and had a large lunch earlier in the day. In order for such short term recommendations to be relevant to the user's current state, data synced from their device which help determine the recommendation is preferably transferred frequently and/or whenever there is new data on the device relevant to such a recommendation.

**[0043]** In one embodiment, this communication device may have foreground and background operating system states. In foreground mode, the function or functions that perform the detection of the sensor device and syncing of data is running in the foreground of the operating system of the communication device. In the background mode, this function or functions are running in the background of the operating system of the communication device. Typically functions which are run in the background have no or minimal

visual indications that they are running on the display of the communication device. Often functions which run in the background run when the display of the device is off and/or when the communication device is in a “sleep” or “locked” mode.

**[0044]** Data may be synced to the communication device for the data to be displayed to the user on the communication device. The data may also be stored to a database in the memory of the communication device. In the case that the data is

#### Sensor Device Broadcasts

**[0045]** In order to enable initiation of a data sync operation, a sensor device may continuously or intermittently (i.e., periodically or aperiodically) transmit wireless packets or other information-bearing transmissions referred to herein as notification signals. The frequency of periodic packet transmissions may vary to balance power consumption and the time to detection. These packets may contain information such as the unique identifier of the sensor device, an identifier that indicates the type of sensor device, a unique identifier of the user of the device, and/or data which indicates some internal state of the device. This internal state information may include but is not limited to an indication of (i) whether the device has new data that the device needs to sync, (2) whether the device wants to sync, (iii) the last time that the device has synced, (iv) the battery level of the device, and/or (v) a flag which indicates whether the device has synced within a specified or predetermined time period (e.g., within the last 15 minutes, last hour, etc.). The information in the packets may be separate pieces of data or combined into a single piece of data. For instance, a device identifier represented by a long or short integer may be separate from a sync indicator (itself represented by a bit, or long or short integer) that indicates whether the device has new data that needs to be synced, or the device identifier and sync indicator may be combined within a single short or long integer.

**[0046]** In one embodiment, the sensor device may broadcast a signal with a fixed frequency to any communication devices in the proximity as shown in FIG. 17. In a number of embodiments, for example, the period “a” may be equal to or less than ten seconds. In other embodiments, the period “a” may be greater than ten seconds. This may enable low latency communication link creation while avoiding unnecessary communication between the communication device and the sensor device. Unnecessary communication is undesirable as it consumes power. The communication device may constantly listen for these signals. The signal may indicate to the communication device whether or not the sensor device needs to communicate.

**[0047]** In one embodiment, illustrated in FIG. 18, variable frequency notification signal broadcast timing is used. The period “a,” “b,” “c,” and “d,” may all be different periods of time. In some embodiments, these values may be related algorithmically. In one embodiment, the portable biometric monitoring device may send out a notification signal broadcast at a minimum of every 2 seconds. If the portable biometric monitoring device doesn’t get a response from a communication device, it may increase that interval by 1 minute. There may be a maximum interval of 30 minutes for example. If the device does get a response, the interval may revert to the minimum interval of 2 seconds. This strategy could reduce battery drain when there is no communication device to sync to. Algorithms for changing the frequency other than that

already described may also be used. In other embodiments, the frequency may change based on syncing criteria, update thresholds or user interactions.

**[0048]** In one embodiment, a mix of variable and fixed frequency notification signal broadcast timings are used. The portable biometric monitoring device may broadcast a signal with a period “a” as seen in FIG. 19. In some cases, a broadcast may occur a time period “b” after the last broadcast. The period “b” may be greater or less than “a.” In some embodiments, an event such as reaching a biometric data update threshold may trigger a change in period. After this event, the next broadcast may occur a period “c” later where “c” is less than, equal to or greater than “a.”

**[0049]** The portable biometric monitoring device may need to sync if it has accumulated a certain amount of biometric data. For example, the portable biometric monitoring device may determine that it needs to sync if it has acquired new biometric data and it has been longer than 15 minutes since the last sync. Other criteria or update thresholds (e.g., corresponding to a threshold change in the biometric data acquired) that may be used to determine when a communication link should be established are disclosed herein. FIG. 20 shows a broadcast timing scheme where an update threshold is used to determine the time at which a broadcast occurs. The period “a,” “b,” and “c” may be wholly or in part determined by the amount of time it takes for an update metric to reach a fixed or time varying threshold.

**[0050]** FIG. 21 illustrates how a fixed frequency broadcast timing scheme may define a period “n” between notification signal broadcasts. This period “n” may be independent of the value of an update metric and whether the value is above, below or equal to an update threshold.

**[0051]** The indication of whether or not the portable biometric device seeks the establishment of a communication link with a communication device may be determined by comparing an update metric to an update threshold as seen in FIG. 22. When the time for a broadcast occurs (either with a fixed or variable frequency), the portable biometric device checks to see if an update metric has met an update threshold. If the threshold has been met, then the notification signal will be broadcasted with an indication that the portable biometric monitoring device seeks to establish a communication link and/or sync. If the update threshold has not been met, the notification signal will indicate that the portable biometric monitoring device does not need to establish a communication link and/or sync. Note that in one embodiment the indication does not necessarily determine whether or not a communication link is established and/or sync will occur. The communication device can use the indication as an aid in determining whether or not to establish a communication link and/or sync.

**[0052]** The signal may also notify the communication device that it is available for communication, but does not need to communicate. This allows the communication device to open a communication link with latency equal to the periodicity broadcasted signal. The communication device may need to open a communication link for reasons including but not limited to a user directed pairing, user directed data sync, update of the device firmware, biometric configuration data update (e.g. stride length, height), device configuration data update (e.g. alarm clock settings, display settings).

**[0053]** In one embodiment, the communication device and the sensor device may communicate using the Bluetooth Smart protocol. The sensor device may intermittently broad-

cast one of two UUID's (universally unique identifiers) to the communication device which is constantly listening for broadcasts. The first UUID corresponds to a Bluetooth service which is used to sync new data from the sensor device. This service is configured to start any programs on the communication device necessary to sync the new data from the sensor device. The second UUID corresponds to a Bluetooth service which is only used when a program on the communication device needs to send data to the sensor device.

**[0054]** The communication device may monitor its wireless input sources for incoming wireless packets and analyze any received packets in order to detect the sensor device as the source of their transmission and decide whether to sync with the sensor device. The function or functions within the communication device that monitors input sources for and analyzes packets may be embedded within the operating system of the communication device and/or in an application or applications that are launched by the operating system of the communication device (i.e., the input monitoring and/or packet analysis functions may be implemented by execution, within one or more processors of the communications device, of programmed instructions that form part of the communication device operating system and/or application programs). The packet detection functionality may be automatically launched or executed by the operating system or can be initiated or directed by the user or users of the communication device. If the functionality is partially or fully within an application, application or applications may be launched automatically by the operating system or launched by the user or users of the communication device. The packet detection functionality may also be split between the operating system and applications. The functionality can execute or run in any priority or mode (active, foreground, background, etc.) on any processor within the communication device. The functionality can also run simultaneously with other functions on the same communication device. If the functionality has already been launched (i.e., implemented through execution of programmed instructions), the operating system can choose to execute or re-execute the functionality, which might be resident in volatile or non-volatile storage or memory of the communication device.

**[0055]** Listening (monitoring input sources) for incoming packets may be carried out periodically in order to lower power consumption (e.g., by powering down or otherwise disabling signal reception functions during intervals in which input sources are un-monitored), continuously in order to decrease the time to detection ("detection latency"). Also, the frequency of periodic listening events may be varied to balance power consumption and the time to detection. During a previous interaction, a user or computer, either directly via the user interface of the communication device or via a wired or wireless communication mechanism, may specify which aspects of the contents of a wireless packet or sequence of wireless packets should trigger a data sync by the communication device. Any single piece of information or combination of the information in a wireless packet or sequence of packets may trigger a data sync after receipt and analysis of the packets. When the sync is triggered, the communication device may start and complete the syncing process via functionality that is embedded within the operating system of the communication device or via an application that is launched by the operating system of the communication device. The

initiation, start, and/or completion of a sync may be performed with or without user interaction using techniques described herein.

#### Syncing Criteria

**[0056]** A variety of criteria, when met, may cause the communication device and the sensor device to attempt to sync to each other for example and without limitation:

- [0057]** Device Type Syncing Criteria
- [0058]** Unique Device Syncing Criteria
- [0059]** New Data Syncing Criteria
- [0060]** Goal-Based Data Syncing
- [0061]** Physiological State Syncing Criteria
- [0062]** User Interaction Syncing Criteria
- [0063]** Activity Based Syncing
- [0064]** Timestamp Syncing Criteria
- [0065]** Location Syncing Criteria
- [0066]** Data Connection Type Syncing Criteria

Each of the foregoing "syncing criteria" (or criterion) is discussed in further detail below and may be applied in combination with any other(s) of the syncing criteria to form a new (compound) syncing criteria. While the embodiments below may specify that a single entity including communication device, sensor device, or server may initiate a sync and or determine that a sync should occur, it should be noted that any communication device, sensor device, server, or a combination thereof may initiate a sync and or determine that a sync should occur based on each of the "syncing criteria" (or criterion). Note that the term "update threshold" may refer to one or more syncing criteria.

**[0067]** FIG. 16 shows how update thresholds or sync criteria are used to determine whether the portable biometric monitoring device indicates that it would like to seek the establishment of a communication link or not in the portable biometric monitoring device's notification broadcast signal. In one embodiment, one or more update thresholds (based on the change in biometric data from the value of the biometric data at the last time that the data was synced to the current value of the biometric data) are used to determine whether or not the portable biometric monitoring device seeks the establishment of a communication link. Note that the list of update thresholds is not exhaustive and is meant only to illustrate several possible update thresholds.

#### Device Type Syncing Criteria

**[0068]** In one embodiment, the communication device might only attempt to sync with a certain type of sensor device. In that case, the communication device will listen for a wireless packet or sequence of wireless packets transmitted by a sensor device and analyze the packets to see they contain an identifier that indicates the type of sensor device. If the identifier is found, a device-type syncing criteria is deemed to be met, and the communication device starts and completes the syncing process in response. Other methods may be used to identify the device type. For example, the type of device may be determined by an NFC tag integrated into the device, an RFID integrated into the device, and/or the wireless protocol that the device communicates with (e.g. device type 'A' uses Bluetooth and device type 'B' uses Wi-Fi). One embodiment of device type syncing criteria is shown in FIG. 3.

#### Unique Device Syncing Criteria

**[0069]** In another embodiment, a communication device might only sync if a specific sensor device is detected. In this instance, the communication device will listen for a wireless packet or sequence of wireless packets transmitted by a sensor device and analyze the packets to see if they contain the unique identifier of a specific sensor device and possibly the device type or user identifier of the owner of the sensor device. One such embodiment is illustrated in FIG. 4. The communication device may also only listen for the user identifier of the owner of the sensor device. When proper information is found in a wireless packet or sequence of wireless packets, unique-device syncing criteria is deemed to be met and the communication device starts and completes the syncing process in response. Other methods may be used to identify a unique device. In another embodiment, the type of device may be determined by an NFC tag integrated into the device or an RFID integrated into the device.

#### New Data Syncing Criteria

**[0070]** In another embodiment, a communication device may be configured to sync only if a specific sensor device has a certain amount of new data to be synced as illustrated in FIG. 5 and FIG. 6. The sensor device might indicate this state, for example, if new data has been collected by the sensor device since the last time it synced with a communication device. In this instance, the communication device will listen for a wireless packet or sequence of packets transmitted by a sensor device and analyze them to see if they contain an indication that the sensor device wants or needs to sync. In some cases, a packet or packets might contain both the unique identifier of a device or device owner and an indication that the sensor device has new data that the sensor device wants to sync. In some other cases, the device might transmit a packet or packets that only contain the identifier of the device or owner and changes the device or owner identifier based on whether the sensor device has new data that the sensor device wants to sync. In either case, when such information is found in a wireless packet or sequence of wireless packets, a new-data syncing criteria is deemed to be met and the communication device starts and completes the syncing process in response.

**[0071]** The sensor device may determine whether it needs to sync or not based on information other than the acquisition of new data including but not limited to the charge state of the device, the operating mode of the device (e.g. battery saving or sleep mode), the state of the motion detector (e.g. whether the motion detector detects motion above a certain level or not), the state of other sensors such as heart rate, GSR, proximity, heat flux and temperature sensors. This other information may serve as a proxy for the acquisition of new data. For example, if the charge state of the sensor device is low, it is likely that the user has been acquiring new data with the device.

#### Goal-Based Data Syncing

**[0072]** The sensor device may determine whether or not it needs to sync based on goals of the user. The user may set these goals themselves or they may be set automatically. The sensor device could use the type of goal to determine when it should sync. For example, if the user has a goal based on the number of floors that they have climbed, the device may sync only when it detects that the user has climbed one or more

floors. The criteria for meeting a goal may also be used by the device to determine when it should sync. For example, if a user's goal is to burn 2,000 calories, the device may try to sync when the user has reached 50%, 75%, and 100% of their goal. This would ensure that the user can see a reasonably precise measure of the progress to their goal on computing devices, portable communication devices, and/or web-based accounts associated with their device.

#### Physiological State Syncing Criteria

**[0073]** The device may determine whether or not it needs to sync based on the current or historical physiological state of the user. In one embodiment where the device can detect the sleep state of the user, the device may sync when the user wakes up. Alternatively, the device may sync immediately before or after the user wakes up. This would allow the user to see up to date data on their communication device or other server connected device immediately after waking up. In another embodiment, the device may sync if a user transitions from a sedentary to non-sedentary state or vice versa. For example, the device may sync when the user gets to work and when the user leaves work. In another embodiment, the device may sync not at the transition of one state to another, but while the user is in one state. For example, if the user has an elevated heart rate for a period greater than 10 minutes, the device may try to sync. This may enable a user to monitor their data during a run on their smartphone for example.

#### User Interaction Syncing Criteria

**[0074]** The sensor device may also sync based on when a user interacts with a communication device which displays synced data or data derived from synced data. In one embodiment, the server, communication device, sensor device or some combination of the three may determine, based on historical data when the user views synced data or information derived from synced data on their communication device. In one example, the device may sync to the user's communication device every time the user wakes up their communication device from sleep mode or turns on their communication device. This would allow the user to see the most up to date information when checking their data on the communication device. In another example, if a user always checks their smart phone at lunch time to see how many steps they walked that morning, the communication device may learn this habit and sync data immediately before the user's lunch time so that the most up to date step count is displayed. In another example, the user may always perform the same gesture or movement before checking their sensor device data. The communication may learn what gesture or motion is performed before the user checks their data and tell the device to sync whenever that gesture or motion is performed. In other cases, this gesture or motion sync criteria may be preprogrammed (not learned) to cause the sensor device to sync. For example, the sensor device may sync to a smart phone whenever the user reaches into their pocket to pull out their smartphone.

#### Activity Based Syncing

**[0075]** The sensor device may determine whether or not it needs to sync based on the activity of the user. In one embodiment, for example, the sensor device includes a motion sensor and may be configured (e.g., through a programmable setting) not to attempt to sync when the motion sensor detects that the

user is active. This may allow the sensor device to reduce the power consumption due to failed or unnecessary syncing attempts. For example, if the user goes for a run with their device and they usually sync the device to a laptop, the device does not need to attempt a sync during the run as the user won't be using the laptop during the run. Conversely, the detection of motion may signal the device to sync in some cases. For example, if a user goes for a hike and they want to monitor their progress during the hike on a smart phone, the device may sync whenever the device detects motion which has a signature of hiking. Finally, in some cases a defined period of motion or lack thereof may be used to determine the syncing strategy. For example, the device may attempt to sync if it has detected motion for 15 minutes or longer.

**[0076]** In another embodiment, the user may interact with the device to indicate that the user is engaged in an activity. In some cases, the user may specify, as part of this interaction, the class or type of activity (e.g. walking, hiking, swimming, working out etc.) which is about to begin, in progress, or has recently ended. The sensor device may use these interactions (e.g., in the form of user input provided via any practicable user interface of the sensor device or a device communicatively coupled to the sensor device) to help determine an optimal or otherwise preferred time to sync. For example, the sensor device may sync at the beginning of a run (including prior to the run, for example, when the user provides input indicating an intent to begin a run) so that the client or server can notify friends that the user is running or planning to run to further encourage exercise. The sensor device may refrain from further sync attempts until it detects (or is notified through user interaction) that the user has completed the run.

#### Device or Owner Identifier Use as a Sync Flag

**[0077]** In a number of embodiments, the sensor device is capable of changing the device identifier and/or owner identifier based on the device's intent to sync, a particularly useful feature in cases where a mobile communication device listens for and initiates sync operations solely based on device or service unique identifiers. Typically, such a mobile communication device might initiate a sync whenever the sensor device came within range or stayed within range, thus potentially syncing more frequently than desirable and consuming undue power. By enabling the sensor device to dynamically change its device, service or owner identifier, however, and to set such identifier(s) to values recognized by the mobile communication device only when new data is available to sync, the mobile communication device would only initiate a sync when necessary, since the mobile communication device would only listen for identifiers that indicated that the sensor device needed to sync. This operation also enables the sensor device sync to co-exist and sync optimally with other communications devices that could base their decisions to sync on using more information contained in a sensor device's wireless packets.

#### Timestamp Syncing Criteria

**[0078]** In another instance, a communication device might attempt to sync with a sensor device only if a certain period of time has elapsed since the sensor device last synced with a communication device. In this instance, the communication device will listen for a wireless packet or sequence of packets transmitted by a sensor device and analyze them to see if they contain either a timestamp of the last sync time of the sensor

device or an indicator of the elapsed time of the last sync (past minute, past 15 minutes, etc.). The communication device may decide based on the timestamp or elapsed time whether it wants to start and complete the syncing process.

#### Location Syncing Criteria

**[0079]** In another instance, a communication device might determine whether or not to sync a sensor device based on the absolute locations of the communication device and/or sensor device, and/or locations of the communication device and sensor device relative to one another. An illustration of this embodiment is shown in FIG. 7. Location of the communication device and/or sensor device may be determined through a plurality of means including but not limited to signal strength (e.g. RSSI) of a wireless signal such as, NFC, RFID, GPS, Wi-Fi, Zigbee, Ant+, Bluetooth, BTLE (Bluetooth Low Energy), or other radio network communication, optical detection through machine vision, audio signals, optical data transmission, or the spectral signature of a light source on the device. Sensor devices without built in GPS could be assumed to be in the same location as the client (e.g., communications device) syncing them; until heard from again they could be assumed to remain in the same place. In one embodiment, the location criteria for syncing may be the proximity of the sensor device to the communication device. In this case, the criteria is not based on the absolute location of either device, but instead, the relative locations of the communication and sensor devices. In another embodiment, the criteria for syncing may include the absolute position of the sensor device. For example, the communication device may allow any device to sync if they are in the user's home as seen in FIG. 8.

#### Data Connection Type Syncing Criteria

**[0080]** The connection or set of connections that the communication device is connected to may be used as criteria for syncing and/or the type of syncing. For example, if the communication device is connected to a cellular network, the communication device may not sync any sensor devices so that the user minimizes their cellular network data usage (e.g. to avoid overage charges for example). When the communication device comes into contact with a Wi-Fi network, the communication device may then allow sensor devices to sync. In another embodiment, the type of sync may change depending on the network type that the communication device is connected to. This embodiment is illustrated in FIG. 9.

**[0081]** In another embodiment, the communication device may only sync high level data when it is connected to a cellular network. When connected to a Wi-Fi network the communication device may sync detailed data. In another embodiment, the communication device may sync data to local storage on the communication device when the communication device is not in contact with any networks. When the communication device comes into contact with a network, the communication device may then complete the upload of data to the server. Note that data connections other than Wi-Fi and cellular may be used in connection type syncing criteria including but not limited to other wireless networks such as NFC, RFID, GPS, Wi-Fi, Zigbee, Ant+, Bluetooth, BTLE and wired connections such as LAN and USB.

#### Multiple Syncing Criteria

**[0082]** More than one criteria for syncing may be met simultaneously or met within a certain time window of each

other. Algorithms or programs for determining what action should be taken in such a case may reside on and be executed within the communication device, or a third party device in communication with the communication device such as a server. In one embodiment, each criterion for syncing or not syncing may be given a priority. For example, device identity criteria may have a higher priority than new data criteria so that no sync would occur for a sensor device not meeting the identity criteria, even if that sensor device has met the new data criteria. In practice, this may be useful when a user wants his or her personal sensor device to sync exclusively to the user's communication device (i.e., not to the communication device of another). Even if a sensor device is broadcasting its need to sync because it has new data, the user's communication device will decline to sync if the sensor device is not owned by the owner of the communication device.

**[0083]** In another embodiment, each or any of the above-described syncing criterion (or criteria) may be combined into meta-criteria; criteria which is only met when a set of sub-criteria are met. In one example a communication device might only sync if a sensor device has a specific identity and has new data that the sensor device wants to sync. The sensor device might indicate this state if there is new data collected by the sensor device since the last time it synced with a communication device. In this instance, the communication device will listen for a wireless packet or sequence of packets transmitted by a sensor device and analyze them to see if they contain an indication that the sensor device wants or needs to sync. In some cases, a packet or packets might contain both the unique identifier of a sensor device or identifier of the owner of the device and an indication that the sensor device has new data that it wants to sync. In some other cases, the device might transmit a packet or packets that only contain the identifier of the device or owner and change the device or owner identifier based on whether the sensor device has new data that it wants to sync. When proper information is found in a wireless packet or sequence of wireless packets, the communication device starts and completes the syncing process. Such a technique may be employed to allow a communication device to sync exclusively with the sensor device associated with the owner of the communication device at a time when this sensor device has new data to sync.

**[0084]** Note that meta-criteria and criteria that are met simultaneously or met within a certain time window of each other may have a prioritization structure similar to that discussed for criteria earlier in this disclosure.

#### Sensor Device Syncing Settings

**[0085]** The communications device may communicate with servers located on private networks or public networks such as the Internet. Through an interface located on a server or a communications device that may communicate with that server, a user may change settings, data or behavior on or of a sensor device, for example by providing instructions to program or otherwise load configuration data or settings into one or more configuration registers of the sensor device. These changes may include but are not limited to parameters for algorithms, time and alarm settings, personal biometric information (weight, height, age, gender, base metabolic rate, etc.), settings for the user interface (which UI screens to show, what information to show on each screen, the order of screens, etc.). Once a change is made, this change may be synced to a sensor device.

#### User Manipulation of Syncing Settings

**[0086]** The user of the communication device and/or sensor device may be able to change settings which determine how and when syncing occurs. The user may be able to change these settings on the sensor device (i.e., by providing input directly or indirectly that results in programming or loading of configuration values into one or more configuration registers of the sensor device), communication device, server, and or website in communication with one or more of the former. The user may be able to change or create the criterion, criteria, meta-criteria, and prioritize criteria and meta-criteria. In one embodiment, for example, a user may be able to set their phone to be a syncing hotspot or node for only their device or all devices. In another embodiment, the user may be able to combine criteria to create their own, more complex, criteria structure. For example, a user may allow their communication device to sync any device that has a location associated with their house when their communication device is in contact with Wi-Fi. The user may also choose to have their communication device always sync his or her own sensor device regardless of connection type and device location.

#### Server Initiated Syncing

**[0087]** In some cases, the server may determine when it is necessary for the sensor device to sync. In such a case, the communications device may gather a list of nearby sensor devices by listening for all wireless packets transmitted by nearby sensor devices for a period of time. The communications device may then query a server on private or public network to see if any of the sensor devices on the list have changes that needs to be synced. The server returns indication of which sensor devices have changes that need to be synced. The communication device then may automatically or upon direction by a user initiate syncing of the changes to the sensor devices in sequence or in parallel. Note that any of the criteria or meta-criteria disclosed herein may be aided or completed determined by the server instead of or in addition to the communication device and/or sensor device.

#### Syncing Security

**[0088]** Transmitted data may be encrypted when the communication device (one example of a client) is used as a tunnel between the sensor device and server. A secret key which enables decryption and encryption is shared between the device and server, but not the client. This prevents the client or an eavesdropping third party from being able to intercept and read the data. The encryption also allows any sensor device to sync to the server through any client without authentication, even if the client is untrusted, without fear of the client being able to read any of the transmitted data.

**[0089]** In some embodiments, it may be desirable for the client to be able to read data directly from the sensor device. For example, a user may have a smartphone application which permits data from the sensor device to be viewed. In order for the application to provide the user with a visualization of the data sent from the sensor device, the application should be able to read the data which is normally encrypted. Transferring data directly to the client instead of through the client to the server can also increase the speed with which data is transferred, allowing more immediate user interaction and visualization of data. Additionally, it may be desirable for the user to be able to sync, view and interact with data from the user's sensor device when the user's client is not connected to

the server. For example, a user may want to sync his or her device to the user's smart phone (the communication device in this example) when the smart phone is out of range of any cellular network and not connected to the server.

**[0090]** Before sending data directly from the device to the client, it may first be determined that the client is a trusted entity. In order to trust the client, the server and/or device may perform an authentication of the client. In one embodiment, it may be undesirable to share the secret key (normally shared only with the device and the server) with the client. In order to authenticate the client without sharing the secret key, a secondary key may be generated using the main secret key, hereafter referred to as the derived key. This derived key may be generated by the server and sent to the client. The device may then use challenge-response authentication to determine if the client has a valid derived key. If this authentication is successful, the sensor device may then send unencrypted data to the client. Alternatively, the device and client may negotiate a session key after authentication of the client. Data would then be transferred encrypted between the device and client using the session key for encryption and decryption.

**[0091]** After being authenticated, the client may be given a token which allows the client to communicate directly with the sensor device without being authenticated again. This token may expire after a condition or set of conditions is met including but not limited to a certain number of data transfer sessions, a certain amount of data is transferred, and or after a certain period of time. The use of the token allows the client to transfer data from the sensor device without being connected to the server for authentication. This is useful in cases such as those already described where a user wants to sync a sensor device to a client (e.g. smart phone) which does not have connectivity to a remote server through a cellular network for example.

**[0092]** Although a specific security protocol is described herein, numerous variations of this protocol and/or alternative security protocols may be employed in connection with sensor device syncing. For example, instead of using a derived key, a key which is independent of the main secret key and known by both the server and the sensor device may be used. Additionally nonces may be used in one or more of the steps described in these protocols to help reduce the possibility of replay attacks.

#### Multiple Channel Syncing

**[0093]** The communication used between the sensor device and communication device, communication device and server, and/or communication device and server (directly) may make use of more than one channel. The use of more than one channel may enable further optimization of security, speed, and latency.

**[0094]** In one embodiment, the sensor device may have one communication channel with the communication device which is used to transfer data at high speed. The communication device may be considered a network sink in this case. A second communication channel may be formed with the communication device to transfer data to a server. This second communication channel uses the communication device as a network tunnel between the sensor device and server. A multichannel communication scheme may afford a variety of advantages such as having communication which may occur at multiple speeds and/or security levels. The communication channel between the sensor device and the communication device may be used to rapidly transfer high level data

intended to be immediately displayed to the user. For example, in the case where the sensor device acts as a pedometer, the total number of steps that the user has taken in the day may be transferred through the high-speed channel. The second communication channel may be used to transfer more detailed data such as the log of steps taken each minute during the day to a server. The data may be encoded so that the communication device cannot parse it, adding a level of security to prevent the user or a third party from corrupting or manipulating the data with the communication device.

**[0095]** In another embodiment, a secondary communication channel may use a different wireless communication standard than the first communication channel. This secondary channel may be used to securely store or transmit data. In one embodiment, one channel may be used to transmit authentication data and a second channel using a different wireless standard may be used to transmit sensor data. For example, an NFC or RFID tag may transfer data that uniquely identifies the device. This tag may be write-protected so that the unique identity of the device is incorruptible.

#### Dynamic Communication Link Configuration

**[0096]** The configuration of the communication between the client and the device may be dynamically changed to optimize for highest data throughput and lowest energy usage. Changes to the low level communication parameters may occur after communication is established and while other communication over the connection is occurring. In one embodiment, it may be desirable for the client to determine how the communication link should be configured, but the client may not be able to configure all aspects of the communication link, namely the low level configurations. For example, in an implementation (or configuration) in which only the sensor device is able to configure certain aspects of the communication link, a special communication interface may be created to allow the client to communicate to the sensor device information needed to configure the communication link. In one embodiment, the type of communication used in dynamic communication link configuration may be Bluetooth or Bluetooth SMART.

#### Connection Oriented Syncing

**[0097]** In order to simplify the mechanism to accomplish syncing without using significant sensor and communication device power and to form a temporary strong relationship between sensor device and client where no other client may communicate with or interfere with the sensor device, a connection oriented approach may be employed. In one embodiment, the client connects to a sensor device, scales up communication speed, syncs, then remains connected but scales down communication speed so that the sensor device spends less energy than it normally would if it was wirelessly sending out packets at a higher communication speed. The client then listens for an indication on a specific sensor device data characteristic. When this indication is present, a message is sent to the communication device indicating that there is new data to sync. In one embodiment, the message may also inform the client of characteristics of the new data or even include the new data inline (i.e., as part of the message) if the volume of new data is small. If needed, the client scales up the communication link speed and performs a sync of all the data.

**[0098]** Another advantage of temporary client ownership of a sensor device communication link is that stateful trans-



actions become possible. This enables the communication device to serve as not only a display for the sensor device but also an interactive terminal for it. In one embodiment, the user would like to change an alarm on the sensor device. The client could read the current state of alarms on the sensor device, hold the communication link open so that no one else may change the alarms, allow the user to edit the alarms on the client, and then finally write any alarm changes back to the sensor device.

#### Implementation of Sensor Device, Communication Device and Other Considerations

**[0099]** FIG. 10 illustrates a generalized embodiment of a computing device **500** that may be used to implement a sensor device (client device), communication device, and/or server or other device in which the various operations described above may be executed (e.g., in a distributed manner between the sensor device and communication device). As shown, computing device **500** includes a processing unit **501**, memory **503** for storing program code executed by the processing unit to effect the various methods and techniques of the above-described embodiments, and also to configuration data or other information for effecting various programmed or configuration settings in accordance with the embodiments described above. Note that the processing unit itself may be implemented by a general or special purpose processor (or set of processing cores) and thus may execute sequences of programmed instructions to effectuate the various operations associated with sensor device syncing, as well as interaction with a user, system operator or other system components.

**[0100]** Still referring to FIG. 10, computing device **500** further includes one or more input and/or output (I/O) ports **505** for receiving and outputting data (e.g., various wireless communications interfaces in accordance with communications standards described above), and a user interface **507** to present (display) and receive information to a human or artificial operator and thus enable an operator to control server-side and/or client-side inputs in connection with the above-described syncing operations. Though not shown, numerous other functional blocks may be provided within computing device **500** according to other functions it may be required to perform (e.g., one or more biometric sensors, environmental sensors, etc., within a sensor device, as well as one or more wireless telephony operations in a smartphone, and wireless network access in a mobile computing device, including a smartphone, tablet computer, laptop computer, etc.) and the computing device itself may be a component in a larger device, server or network of devices and/or servers. Further, the functional blocks within computing device **500** are depicted as being coupled by a communication path **502** which may include any number of shared or dedicated buses or signaling links. More generally, the functional blocks shown may be interconnected in a variety of different architectures and individually implemented by a variety of different underlying technologies and architectures. With regard to the memory architecture, for example, multiple different classes of storage may be provided within memory **503** to store different classes of data. For example, memory **503** may include non-volatile storage media such as fixed or removable magnetic, optical, or semiconductor-based recording media to store executable code and related data, volatile storage media such as static or dynamic RAM to store more transient information and other variable data.

**[0101]** The various methods and techniques disclosed herein may be implemented through execution of one or more sequences of instructions (i.e., software program(s)) within processing unit **501**, or by a custom-built hardware ASIC (application-specific integrated circuit), or programmed on a programmable hardware device such as an FPGA (field-programmable gate array), or any combination thereof within or external to processing unit **501**.

**[0102]** Any of the various methodologies disclosed herein and/or user interfaces for configuring and managing same may be implemented by machine execution of one or more sequences instructions (including related data necessary for proper instruction execution). Such instructions may be recorded on one or more computer-readable media for later retrieval and execution within one or more processors of a special purpose or general purpose computer system or consumer electronic device or appliance, such as the system, device or appliance described in reference to FIG. 10. Computer-readable media in which such instructions and data may be embodied include, but are not limited to, non-volatile storage media in various forms (e.g., optical, magnetic or semiconductor storage media) and carrier waves that may be used to transfer such instructions and data through wireless, optical, or wired signaling media or any combination thereof. Examples of transfers of such instructions and data by carrier waves include, but are not limited to, transfers (uploads, downloads, e-mail, etc.) over the Internet and/or other computer networks via one or more data transfer protocols (e.g., HTTP, FTP, SMTP, etc.).

**[0103]** Various aspects and features of embodiments disclosed herein are set forth, for example and without limitation, in the following numbered clauses:

**[0104]** 1. A portable biometric device comprising:

**[0105]** sensor circuitry to detect altitudinal transition and ambulatory motion of an individual bearing the portable biometric device and output one or more signals corresponding to the altitudinal transition and ambulatory motion;

**[0106]** processing circuitry to receive the one or more signals from the sensor circuitry, generate biometric data relating to an activity of the individual based on the one or more signals, and output information including the biometric data; and

**[0107]** wireless circuitry, coupled to the processing circuitry, to receive the information and to wirelessly transmit the information via a first wireless communication link to a handheld communication device.

**[0108]** 2. The portable biometric device of clause 1 wherein the processing circuitry to generate the biometric data relating to the activity of the individual comprises processing circuitry to generate, as part of the biometric data, one or more values that indicate a number of stair-steps climbed by the individual.

**[0109]** 3. The portable biometric device of clause 1 wherein the sensor circuitry comprises an altimeter to detect the altitudinal transition and a motion sensor to detect ambulatory motion.

**[0110]** 4. The portable biometric device of clause 1 wherein the processing circuitry to generate the biometric data relating to the activity of the individual comprises processing circuitry to generate, as part of the biometric data, one or more values that indicate an amount of energy expended by the individual in connection with the altitudinal transition and ambulatory motion.

- [0111] 5. A method of operation within a portable biometric device, the method comprising:
- [0112] detecting altitudinal transition and ambulatory motion of an individual bearing the portable biometric device;
  - [0113] generating biometric data relating to an activity of the individual based on the altitudinal transition and ambulatory motion; and
  - [0114] wirelessly transmitting the biometric data via a first wireless communication link to a handheld communication device.
- [0115] 6. The method of clause 5 wherein generating the biometric data relating to the activity of the individual based on the altitudinal transition and ambulatory motion comprises generating one or more values that indicate a number of stair-steps climbed by the individual.
- [0116] 7. The method of clause 5 further wherein detecting the altitudinal transition and ambulatory motion of the individual bearing the portable biometric device comprises detecting the altitudinal transition via an altimeter of the portable biometric device and detecting the ambulatory motion via a motion sensor of the portable biometric device.
- [0117] 8. The method of clause 5 wherein generating the biometric data relating to an activity of the individual based on the altitudinal transition and ambulatory motion comprises generating one or more values that indicate an amount of energy expended by the individual in connection with the altitudinal transition and ambulatory motion.
- [0118] 9. A portable biometric device comprising:
- [0119] biometric circuitry to generate biometric data corresponding to activity of an individual bearing the portable biometric device; and
  - [0120] wireless circuitry, coupled to the biometric circuitry, to:
    - [0121] transmit an notification signal following each of a sequence of intervals to alert a nearby wireless communication device of the presence of the portable biometric device,
    - [0122] establish a wireless communication link with the wireless communication device, and
    - [0123] transmit the biometric data to the wireless communication device via the wireless link.
- [0124] 10. The portable biometric device of clause 9 wherein the wireless circuitry to establish the wireless communication link with the wireless communication device comprises wireless receiver circuitry to receive one or more signals from the wireless communication device indicating that the wireless communication device has received the notification signal.
- [0125] 11. The portable biometric device of clause 9 wherein the wireless circuitry to establish the wireless communication link with the communication device comprises wireless receiver circuitry to receive one or more signals from the wireless communication device providing information to be used in establishing the wireless communication link.
- [0126] 12. The portable biometric device of clause 9 wherein the wireless circuitry to transmit the notification signal following each of a sequence of intervals comprises wireless transmit circuitry to transmit the notification signal at regular intervals.
- [0127] 13. The portable biometric device of clause 9 wherein sequence of intervals comprises a non-uniform sequence of intervals.
- [0128] 14. The portable biometric device of clause 13 wherein a sub-sequence of intervals within the non-uniform sequence of intervals comprises intervals of progressively longer duration.
- [0129] 15. The portable biometric device of clause 14 wherein the non-uniform sequence of intervals comprises intervals that grow progressively longer until either (i) the wireless communication device responds to the notification signal transmitted following one of the intervals or (ii) a maximum-duration interval transpires.
- [0130] 16. A method of operation within a portable biometric device, the method comprising:
- [0131] generating biometric data corresponding to activity of an individual bearing the portable biometric device;
  - [0132] wirelessly transmitting an notification signal following each of a sequence of intervals to alert a nearby wireless communication device of the presence of the portable biometric device;
  - [0133] establishing a wireless communication link with the wireless communication device; and
  - [0134] wirelessly transmitting the biometric data to the wireless communication device via the wireless link.
- [0135] 17. The method of clause 16 wherein establishing the wireless communication link with the wireless communication device comprises receiving one or more signals from the wireless communication device indicating that the wireless communication device has received the notification signal.
- [0136] 18. The method of clause 16 wherein establishing the wireless communication link with the communication device comprises receiving one or more signals from the wireless communication device providing information to be used in establishing the wireless communication link.
- [0137] 19. The method of clause 16 wherein wirelessly transmitting the notification signal following each of a sequence of intervals comprises wirelessly transmitting the notification signal at regular intervals.
- [0138] 20. The method of clause 16 wherein sequence of intervals comprises a non-uniform sequence of intervals.
- [0139] 21. The method of clause 20 wherein a sub-sequence of intervals within the non-uniform sequence of intervals comprises intervals of progressively longer duration.
- [0140] 22. The method of clause 21 wherein the non-uniform sequence of intervals comprises intervals that grow progressively longer until either (i) the wireless communication device responds to the notification signal transmitted following one of the intervals or (ii) a maximum-duration interval transpires.
- [0141] 23. A portable biometric device comprising:
- [0142] a motion sensor to detect motion of an individual bearing the portable biometric device and output a signal corresponding to the detected motion;
  - [0143] processing circuitry to receive the signal from the motion sensor, generate biometric data relating to an activity of the individual based on the signal, and output information including (i) the biometric data and (ii) an indication that the information is to be relayed over a wireless communications network; and

- [0144] wireless circuitry, coupled to the processing circuitry, to receive the information and to transmit the information via a first wireless communication link to a handheld communication device that acts, in response to the indication that the information is to be relayed, to re-transmit the information via a second wireless communication link without displaying the information on a user interface of the handheld communication device.
- [0145] 24. The portable biometric device of clause 23 wherein the processing circuitry to generate the biometric data comprises processing circuitry to determine, as at least part of the biometric data, a number of ambulatory steps taken by the individual.
- [0146] 25. The portable biometric device of clause 23 wherein the indication that the information is to be relayed over the wireless communications network comprises encryption of the biometric data.
- [0147] 26. The portable biometric device of clause 23 wherein the indication that the information is to be relayed over the wireless communications network comprises a control value that is distinct from the biometric data.
- [0148] 27. The portable biometric device of clause 23 wherein the first wireless communication link is a shorter-range wireless communication link than the second wireless communications link.
- [0149] 28. The portable biometric device of clause 23 wherein the second wireless communication link is established via the wireless communications network.
- [0150] 29. The portable biometric device of clause 23 wherein the wireless communications network comprises at least one of a WiFi communications network, WiMax communications network, or mobile telephony network.
- [0151] 30. A method of operation within a portable biometric device, the method comprising:
- [0152] detecting motion of an individual bearing the portable biometric device and output a signal corresponding to the detected motion;
- [0153] generating information including (i) biometric data that relates to an activity of the individual indicated by the signal, and (ii) an indication that the information is to be relayed over a wireless communications network; and
- [0154] wirelessly transmitting the information via a first wireless communication link to a handheld communication device that acts, in response to the indication that the information is to be relayed, to re-transmit the information via a second wireless communication link without displaying the information on a user interface of the handheld communication device.
- [0155] 31. The method of clause 30 wherein generating information including biometric data that relates to an activity of the individual comprises determining, as at least part of the biometric data, a number of ambulatory steps taken by the individual.
- [0156] 32. The method of clause 30 wherein generating information including the indication that the information is to be relayed over the wireless communications network comprises encrypting the biometric data.
- [0157] 33. The method of clause 30 wherein generating information including the indication that the information is to be relayed over the wireless communications network comprises including, within the information, a control value that is distinct from the biometric data.
- [0158] 34. The method of clause 30 wherein the first wireless communication link is a shorter-range wireless communication link than the second wireless communications link.
- [0159] 35. The method of clause 30 wherein the second wireless communication link is established via the wireless communications network.
- [0160] 36. The method of clause 30 wherein the wireless communications network comprises at least one of a WiFi communications network, WiMax communications network, or mobile telephony network.
- [0161] 37. A handheld communication device comprising:
- [0162] first circuitry to wirelessly receive first biometric data transmitted by a portable biometric device via a first wireless communication link, the first biometric data relating to activity of an individual bearing the portable biometric device;
- [0163] a user-interface including a display; and
- [0164] second circuitry to receive the first biometric data from the first circuitry and to perform a function using the first biometric data in connection with updating a first database of biometric information, the second circuitry being coupled to the user-interface to disable the display during a time period that encompasses a first interval in which the second circuitry performs the function in connection with updating the first database of biometric information.
- [0165] 38. The handheld communication device of clause 37 further comprising a memory to store the first database of biometric information, and wherein the second circuitry to receive the first biometric data from the first circuitry, perform the function using the first biometric data, and disable the display comprises processing circuitry, coupled to the first circuitry, user-interface and memory, to update the first database of biometric information during the first interval using the first biometric data.
- [0166] 39. The handheld communication device of clause 38 wherein the first circuitry is further to wirelessly receive second biometric data transmitted by the portable biometric device relating to activity of the individual bearing the portable biometric device, and wherein the data processing circuitry is further to update the first database of biometric information based on the second biometric data concurrently with presenting information on a predominant portion of the display pertaining to a function of the handheld communication device that is unrelated to the first database of biometric information or the first or second biometric data.
- [0167] 40. The handheld communication device of clause 37 wherein the second circuitry to perform a function using the first biometric data in connection with updating the first database of biometric information comprises:
- [0168] third circuitry to wirelessly transmit the first biometric data, during the first interval and via a second wireless communication link, to a computing device that maintains the first database of biometric information; and
- [0169] processing circuitry, coupled to the first circuitry, user-interface and third circuitry, to enable the first biometric data to be transferred from the first circuitry to the third circuitry and to disable the display during the time period that encompasses the first interval.
- [0170] 41. The handheld communication device of clause 40 wherein the first circuitry is further to wirelessly receive

- second biometric data transmitted by the portable biometric device relating to activity of the individual bearing the portable biometric device, the third circuitry is further to wirelessly transmit the second biometric data over the second wireless communication link during a second interval, and the processing circuitry is further to present, on a predominant portion of the display during the second interval, information pertaining to any of a plurality of functions of the handheld communication device that is unrelated to the first database of biometric information or the first or second biometric data.
- [0171] 42. The handheld communications device of clause 40 wherein at least one of the functions of the handheld communications device is wireless telephony.
- [0172] 43. A method of operation within a handheld communication device having a user-interface, the method comprising:
- [0173] wirelessly receiving first biometric data transmitted by a portable biometric device via a first wireless communication link, the first biometric data relating to activity of an individual bearing the portable biometric device;
- [0174] performing, during a first interval, a function using the first biometric data in connection with updating a first database of biometric information; and
- [0175] disabling a display of the user-interface during a time period that encompasses the first interval.
- [0176] 44. The method of clause 43 further wherein the first database of biometric information is stored within a memory of the handheld communication device, and wherein performing a function using the first biometric data in connection with updating the first database of biometric information comprises updating the first database of biometric information using the first biometric data.
- [0177] 45. The method of clause 44 further comprising:
- [0178] wirelessly receiving second biometric data transmitted by the portable biometric device relating to activity of the individual bearing the portable biometric device;
- [0179] updating the first database of biometric information based on the second biometric data; and
- [0180] concurrently with updating the first database of biometric information based on the second biometric data, presenting information on a predominant portion of the display pertaining to a function of the handheld communication device that is unrelated to the first database of biometric information or the first or second biometric data.
- [0181] 46. The method of clause 43 wherein performing a function using the first biometric data in connection with updating the first database of biometric information comprises wirelessly transmitting the first biometric data, during the first interval and via a second wireless communication link, to a computing device that maintains the first database of biometric information.
- [0182] 47. The method of clause 46 further comprising:
- [0183] wirelessly receiving second biometric data transmitted by the portable biometric device relating to activity of the individual bearing the portable biometric device;
- [0184] wirelessly transmitting the second biometric data to the computing device that maintains the first database of biometric information; and
- [0185] concurrently with wirelessly transmitting the second biometric data to the computing device, presenting information on a predominant portion of the display pertaining to any of a plurality of functions of the handheld communication device that is unrelated to the first database of biometric information or the first or second biometric data.
- [0186] 48. The method of clause 47 wherein at least one of the functions of the handheld communications device is wireless telephony.
- [0187] 49. A system for wirelessly transferring biometric data to a computing device, the system comprising:
- [0188] a first portable biometric monitoring device to generate first biometric data and wirelessly transmit the first biometric data via a first wireless communication link;
- [0189] a handheld communication device to wirelessly receive the first biometric data via the first wireless communication link and wirelessly re-transmit the first biometric data to the computing device via a second wireless communication link.
- [0190] 50. The system of clause 49 wherein the first biometric device comprises sensor circuitry to detect altitudinal transition and ambulatory motion of an individual bearing the portable biometric device, and wherein the first biometric data includes information corresponding to the altitudinal transition and ambulatory motion.
- [0191] 51. The system of clause 49 wherein the handheld communication device comprises a display that is disabled during receipt and re-transmission of the first biometric data.
- [0192] 52. The system of clause 49 wherein the handheld communications device comprises a display and processing circuitry to present, on a predominant portion of the display and concurrently with re-transmission of the first biometric data, information pertaining to any of a plurality of functions of the handheld communication device that is unrelated to the first biometric data.
- [0193] 53. A method of wirelessly transferring biometric data to a computing device, the method comprising:
- [0194] generating first biometric data within a portable biometric monitoring device;
- [0195] wirelessly transmitting the first biometric data from the portable biometric monitoring device via a first wireless communication link;
- [0196] wirelessly receiving the first biometric data within handheld communication device via the first wireless communication link; and
- [0197] wirelessly re-transmitting the first biometric data from the handheld communication device to the computing device via a second wireless communication link.
- [0198] 54. The method of clause 53 wherein the first biometric device comprises sensor circuitry to detect altitudinal transition and ambulatory motion of an individual bearing the portable biometric device, and wherein the first biometric data includes information corresponding to the altitudinal transition and ambulatory motion.
- [0199] 55. The method of clause 53 further comprising disabling a display of the handheld communication device during receipt and re-transmission of the first biometric data.
- [0200] 56. The method of clause 53 further comprising presenting, on a predominant portion of a display of the handheld communications device concurrently with re-

transmission of the first biometric data, information pertaining to any of a plurality of functions of the handheld communication device that is unrelated to the first biometric data.

[0201] The section headings provided in this detailed description are for convenience of reference only, and in no way define, limit, construe or describe the scope or extent of such sections. Also, while various specific embodiments have been disclosed, it will be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the disclosure. For example, features or aspects of any of the embodiments may be applied in combination with any other of the embodiments or in place of counterpart features or aspects thereof. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

What is claimed is:

1. A portable activity-monitoring device comprising: monitoring circuitry to generate user-activity data corresponding to activity of an individual bearing the portable activity-monitoring device; and communication circuitry, coupled to the monitoring circuitry, to intermittently broadcast a notification signal to be received by a wireless communication device, the notification signal conveying information that identifies the portable activity-monitoring device and that indicates whether or not the portable activity-monitoring device seeks establishment of a wireless communication link to enable transmission of the user-activity data to the wireless communication device.
2. The portable activity-monitoring device of claim 1 further comprising logic circuitry to determine whether a change in the user-activity data exceeds one or more update thresholds and wherein the communication circuitry to intermittently broadcast the notification signal comprises circuitry to broadcast, within the notification signal, sync information in either a first state or a second state according to whether the logic circuitry determines that the change in the user-activity data exceed the one or more update thresholds.
3. The portable activity-monitoring device of claim 2 wherein the logic circuitry to determine whether the change in the user-activity data exceeds one or more update thresholds comprises circuitry to determine the change in the user-activity data between two points in time and to compare the change to the one or more update thresholds.
4. The portable activity-monitoring device of claim 3 wherein the earlier of the two points in time corresponds to a state of the user-activity data most recently transmitted by the portable activity-monitoring device as part of a data synchronization operation.
5. The portable activity-monitoring device of claim 2 wherein the one or more update thresholds reflect at least one of the following in connection with the activity of the individual: a threshold number of ambulatory steps taken, a threshold number of calories expended, a threshold altitudinal transition, a threshold heart rate, a threshold distance traveled, or a threshold rest period.
6. The portable activity-monitoring device of claim 1 wherein the communication circuitry to intermittently broadcast the notification signal comprises circuitry to broadcast, within the notification signal, sync information in either a first state or a second state depending at least in part on the user-activity data.

7. The portable activity-monitoring device of claim 6 wherein the circuitry to broadcast the sync information in the first state or the second state based at least in part on the user-activity data comprises circuitry to broadcast the sync information in the first state if the user-activity data indicates that a predetermined threshold has been exceeded.

8. The portable activity-monitoring device of claim 7 wherein the predetermined threshold corresponds to at least one of ambulatory steps taken, calories expended, altitudinal transition, heart rate, distance traveled, or rest period.

9. The portable activity-monitoring device of claim 1 wherein, if the information indicates that the portable activity-monitoring device seeks establishment of the wireless communication link, the communication circuitry is further to establish the wireless communication link with the wireless communication device and transmit the user-activity data to the wireless communication device via the wireless communication link.

10. The portable activity-monitoring device of claim 1 wherein, if the information indicates that the portable activity-monitoring device does not seek establishment of the wireless communication link, the communication circuitry is further to establish the wireless communication link with the wireless communication device in response to receiving a communication from the wireless communication device indicating that the wireless communication device seeks establishment of the wireless communication link to enable transmission of information to the portable activity-monitoring device.

11. The portable activity-monitoring device of claim 10 wherein the communication circuitry is further to receive the information from the wireless communication device, the information including at least one of the following: additional user-activity data to be synchronized with the user-activity data generated by the monitoring circuitry, information to be applied to control an operational aspect of the monitoring circuitry, information to be applied to control an operational aspect of the communication circuitry, information to be applied to control an aspect of user-activity data generation within the monitoring circuitry, information to be applied to configure a visual, auditory or haptic output of the portable activity-monitoring device.

13. The portable biometric device of claim 1 wherein the communication circuitry to intermittently broadcast the notification signal comprises circuitry to broadcast the notification signal at uniform intervals.

13. The portable biometric device of claim 12 wherein each of the uniform intervals has a duration of less than 10 seconds such that each notification signal is broadcast less than 10 seconds after a previously broadcast notification signal.

14. The portable biometric device of claim 1 wherein the communication circuitry to intermittently broadcast the notification signal comprises circuitry to broadcast the notification signal at non-uniform intervals.

15. The portable activity-monitoring device of claim 1 wherein wireless communication device comprises a mobile telephone.

16. A method of operation within a portable activity-monitoring device, the method comprising:

- generating user-activity data corresponding to activity of an individual bearing the portable activity-monitoring device; and
- intermittently broadcasting a notification signal to be received by a wireless communication device, the noti-

fication signal conveying information that identifies the portable activity-monitoring device and that indicates whether or not the portable activity-monitoring device seeks establishment of a wireless communication link to enable transmission of the biometric data to the wireless communication device.

**17.** The method of claim **16** further comprising determining whether a change in the user-activity data exceeds one or more update thresholds, and wherein intermittently broadcasting the notification signal comprises broadcasting, within the notification signal, sync information in either a first state or a second state according to whether the change in the user-activity data is determined to exceed the one or more update thresholds.

**18.** The method of claim **17** wherein determining whether the change in the user-activity data exceeds one or more update thresholds comprises determining the change in the user-activity data between two points in time and to comparing the change to the one or more update thresholds.

**19.** The method of claim **18** wherein the earlier of the two points in time corresponds to a state of the user-activity data most recently transmitted by the portable activity-monitoring device as part of a data synchronization operation.

**20.** The method of claim **17** wherein the one or more update thresholds reflect at least one of the following in connection with the activity of the individual: a threshold number of ambulatory steps taken, a threshold number of calories expended, a threshold altitudinal transition, a threshold heart rate, a threshold distance traveled, or a threshold rest period.

**21.** The method of claim **16** wherein intermittently broadcasting the notification signal comprises broadcasting, within the notification signal, sync information in either a first state or a second state depending at least in part on the user-activity data.

**22.** The method of claim **21** wherein broadcasting the sync information in either the first state or the second state depending at least in part on the user-activity data comprises broadcasting the sync information in the first state if the user-activity data indicates that a predetermined threshold has been exceeded.

**23.** The method of claim **22** wherein the predetermined threshold corresponds to at least one of ambulatory steps taken, calories expended, altitudinal transition, heart rate, distance traveled, or rest period.

**24.** The method of claim **16** further comprising, if the information indicates that the portable activity-monitoring device seeks establishment of the wireless communication link, establishing the wireless communication link with the

wireless communication device and transmitting the user-activity data to the wireless communication device via the wireless communication link.

**25.** The method of claim **24** further comprising, if the information indicates that the portable activity-monitoring device does not seek establishment of the wireless communication link, establishing the wireless communication link with the wireless communication device in response to receiving a communication from the wireless communication device indicating that the wireless communication device seeks establishment of the wireless communication link to enable transmission of information to the portable activity-monitoring device.

**26.** The method of claim **16** further comprising receiving the information from the wireless communication device, the information including at least one of the following: user-activity data to be synchronized with the user-activity data generated by the portable activity-monitoring device, information to be applied to control an aspect of generating the user-activity data, information to be applied to control an aspect of wireless broadcasting, information to be applied to control an aspect of wireless communication, or information to be applied to configure a visual, auditory or haptic output of the portable activity-monitoring device.

**27.** The method of claim **16** wherein intermittently broadcasting the notification signal comprises broadcasting the notification signal at uniform intervals.

**28.** The method of claim **16** wherein intermittently broadcasting the notification signal comprises broadcasting the notification signal at non-uniform intervals.

**29.** The method of claim **16** wherein intermittently broadcasting a notification signal to be received by a wireless communication device comprises intermittently broadcasting a notification signal to be received by a wireless communication device having a mobile telephone function.

**30.** A portable activity-monitoring device comprising:  
means for generating user-activity data corresponding to activity of an individual bearing the portable activity-monitoring device; and

means for intermittently broadcasting a notification signal to be received by a wireless communication device, the notification signal conveying information that identifies the portable activity-monitoring device and that indicates whether or not the portable activity-monitoring device seeks establishment of a wireless communication link to enable transmission of the user-activity data to the wireless communication device.

\* \* \* \* \*