US 20110137520A1

(19) United States

(12) Patent Application Publication

Rector et al.

(10) Pub. No.: US 2011/0137520 A1

(43) Pub. Date: Jun. 9, 2011

(54) **DEVICES, SYSTEMS AND METHODS FOR CONTROLLING PERMITTED SETTINGS ON A VEHICLE**

(75) Inventors: **Jay Daryl Rector**, Loganville, GA (US); **John Potts Davis, III**, Marietta, GA (US); **Justin Michael Anthony McNamara**, Atlanta, GA (US)

(73) Assignee: **AT&T MOBILITY II LLC**, Atlanta, GA (US)

(21) Appl. No.: **12/632,375**

(22) Filed: **Dec. 7, 2009**

Publication Classification

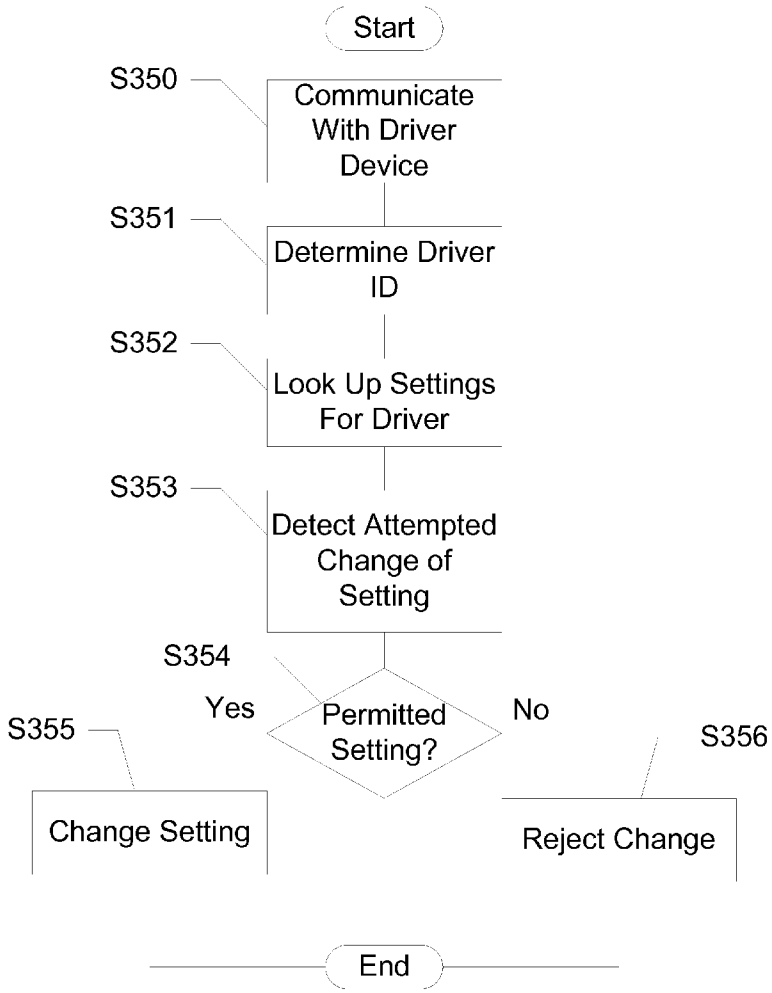
(51) **Int. Cl.**

G06F 7/00	(2006.01)
H04M 3/00	(2006.01)
G08B 21/00	(2006.01)

(52) **U.S. Cl.** **701/36**; 701/1; 701/70; 455/418; 340/667

(57) **ABSTRACT**

Devices, systems, and methods are disclosed for altering permitted settings of a vehicle according to a driver identified through short range wireless communication. The vehicle captures a unique identifier from a wireless communication device of the driver of the vehicle. This unique identifier is used to reference a database to determine the identity of the driver as well as settings for the driver created by a controlling authority. The controlling authority may be, for instance, a parent or employer of the driver. The settings may limit certain devices within the vehicle and/or the vehicle itself. Speed control settings, radio settings, wireless communication device settings, and various other settings are all possible to limit distractions to the driver. Further, the settings may be influenced by the number or identities of passengers within the vehicle.



TOYOTA EXHIBIT 1006

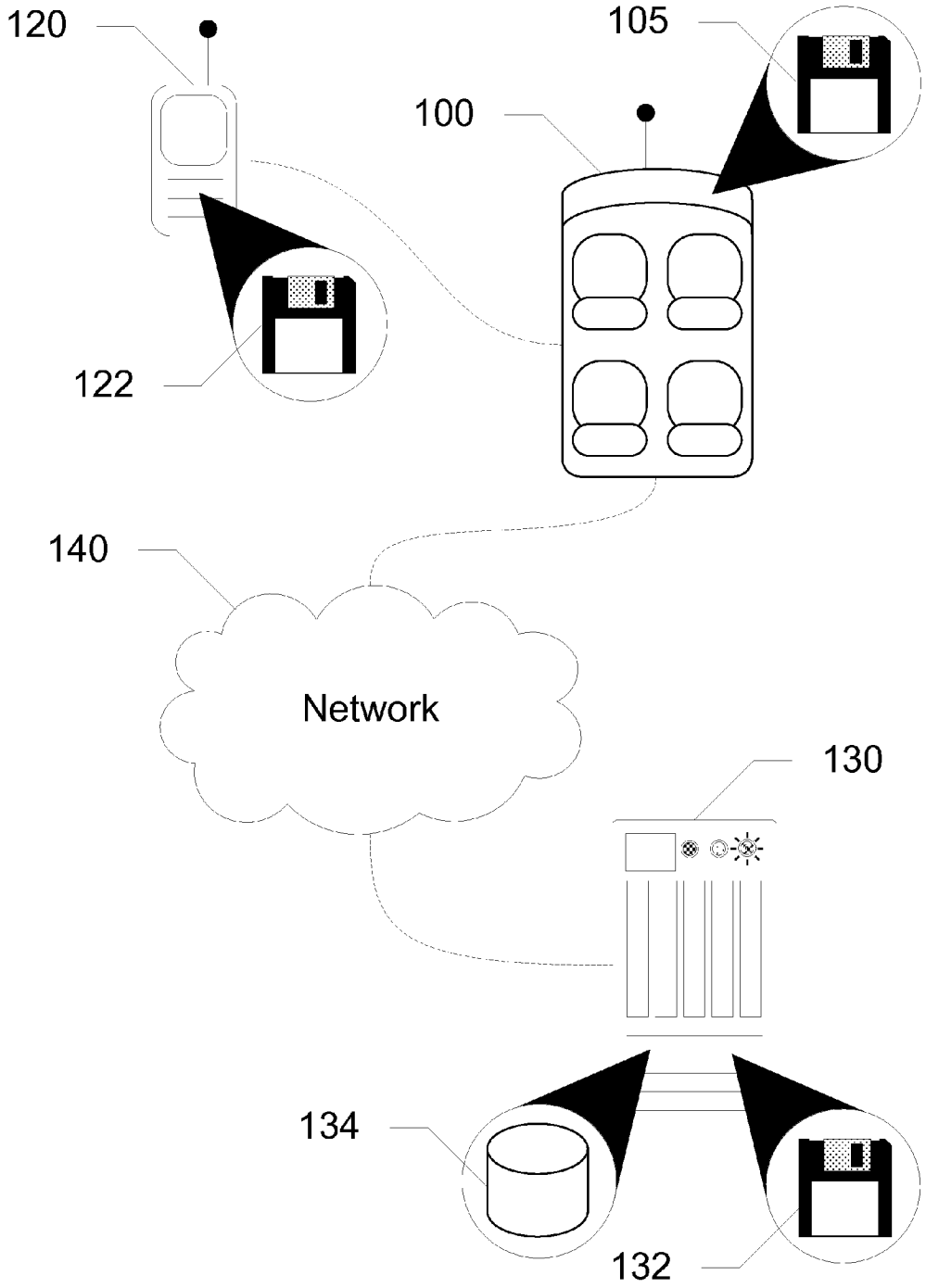


Figure 1

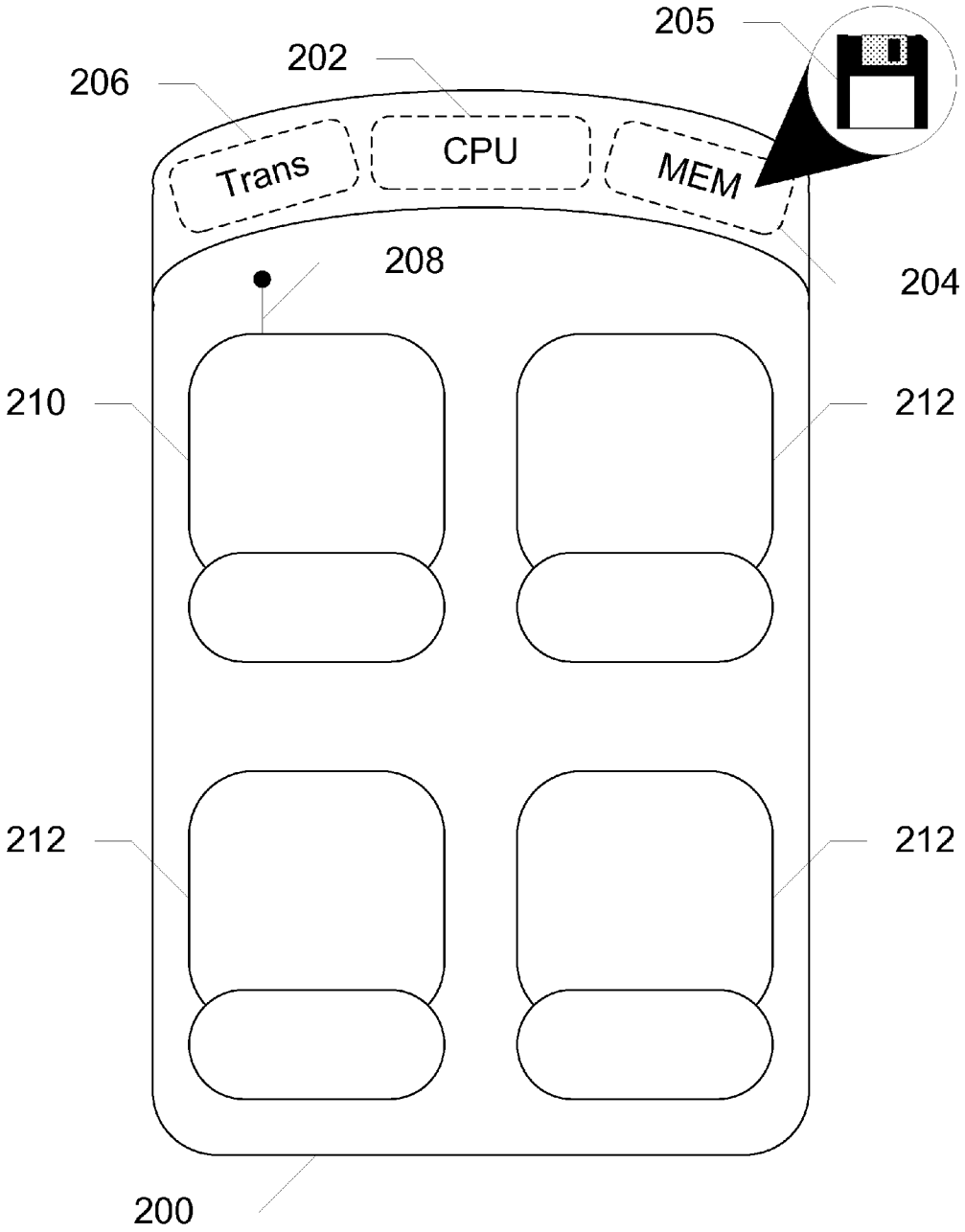


Figure 2

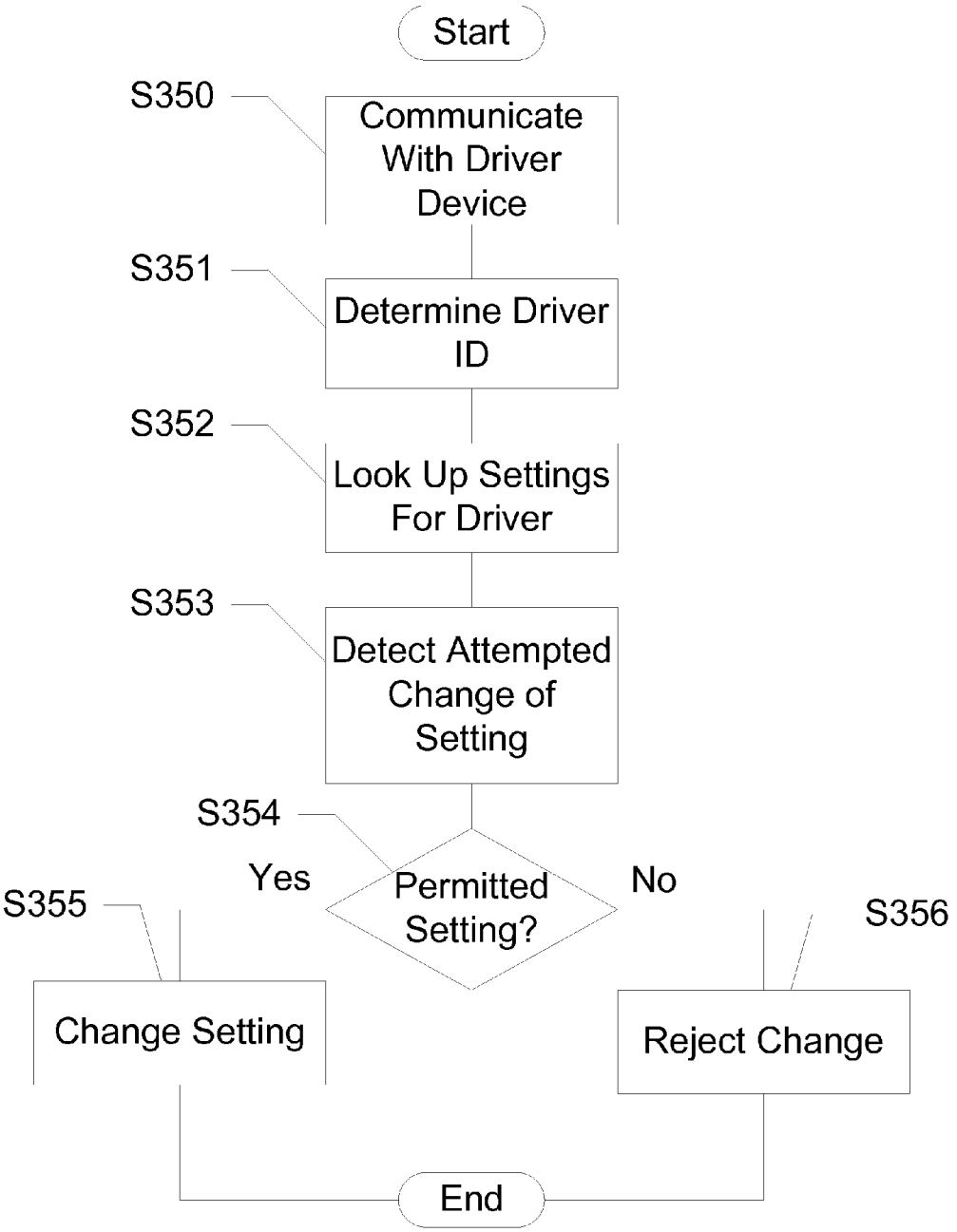

Start
S350
Communicate With Driver Device
S351
Determine Driver ID
S352
Look Up Settings For Driver
S353
Detect Attempted Change of Setting
S354
Permitted Setting?
Yes
No
S355
Change Setting
S356
Reject Change
End

Figure 3

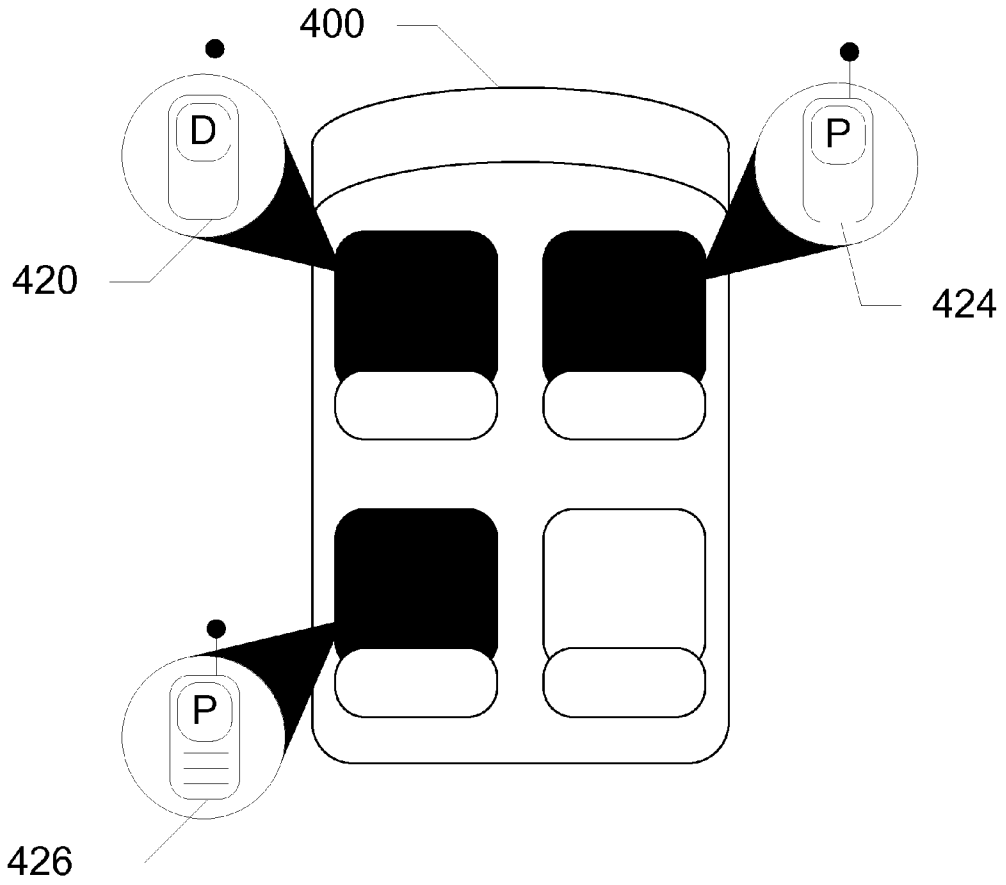


Figure 4

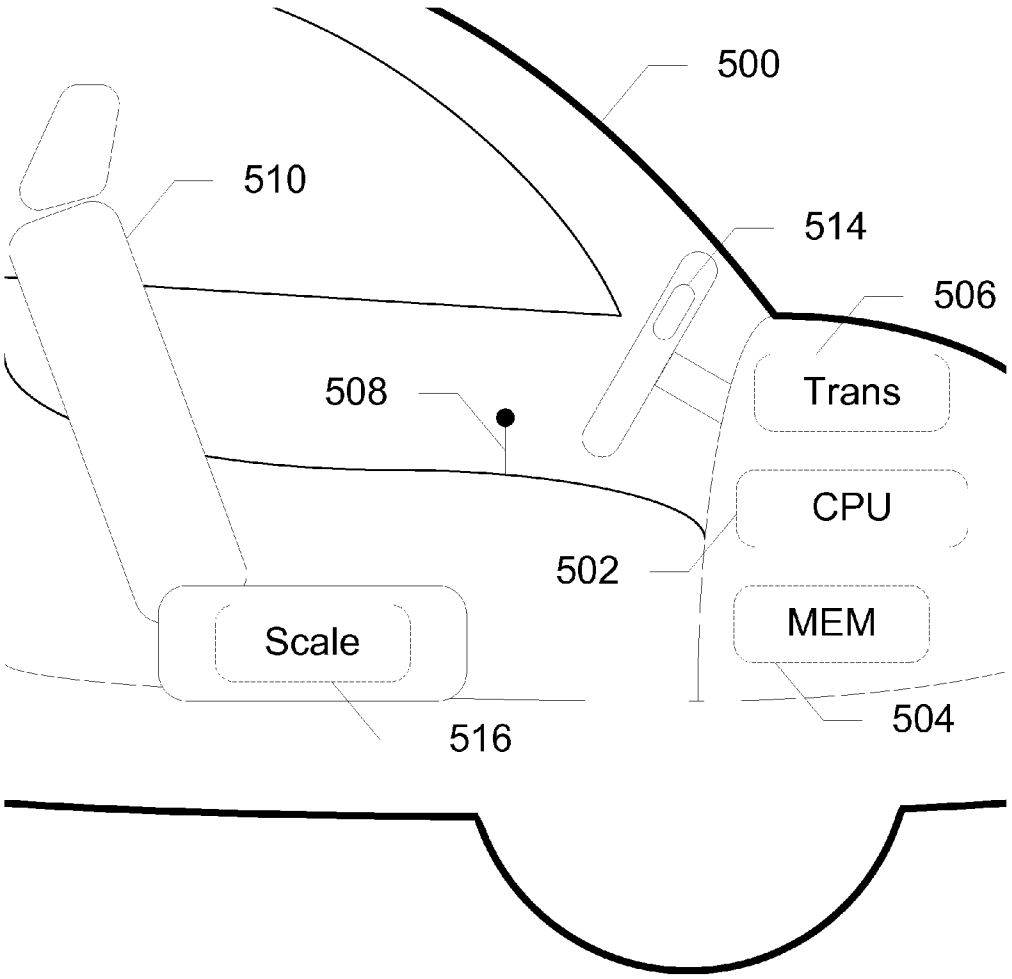


Figure 5

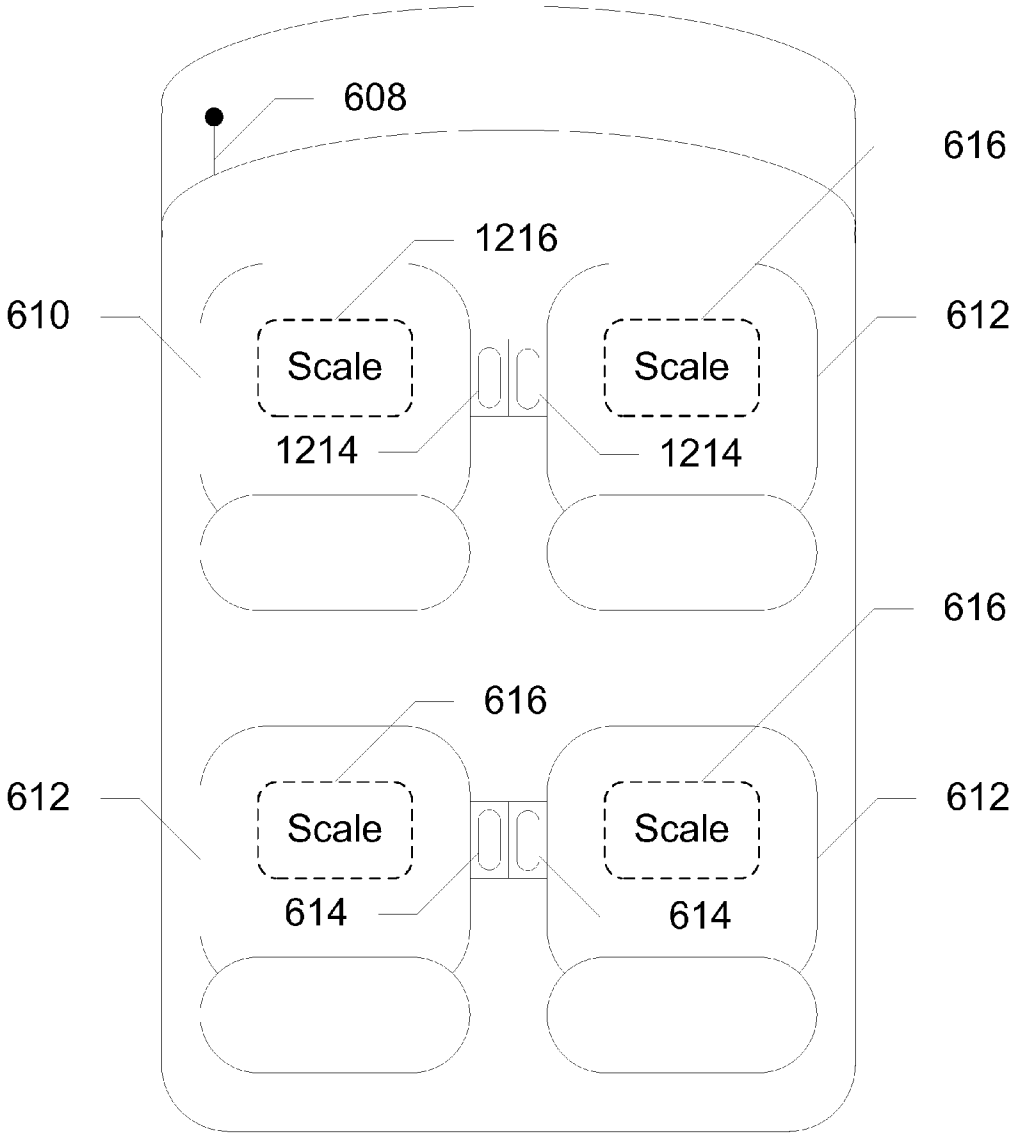

608
616
1216
610
612
Scale
Scale
1214
1214
616
616
612
612
Scale
Scale
614
614

Figure 6

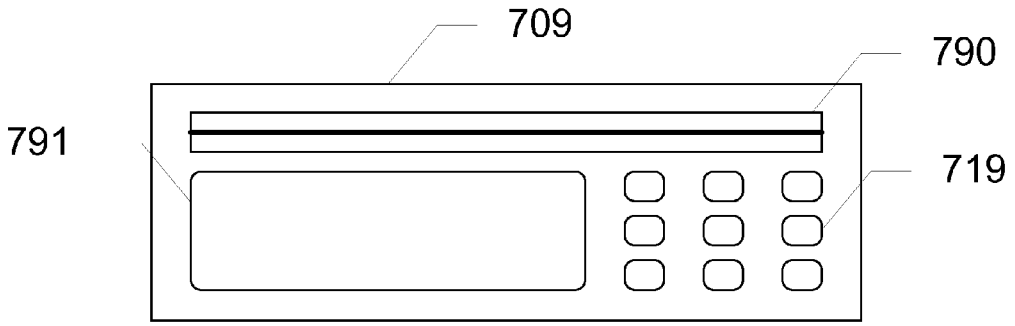


Figure 7A

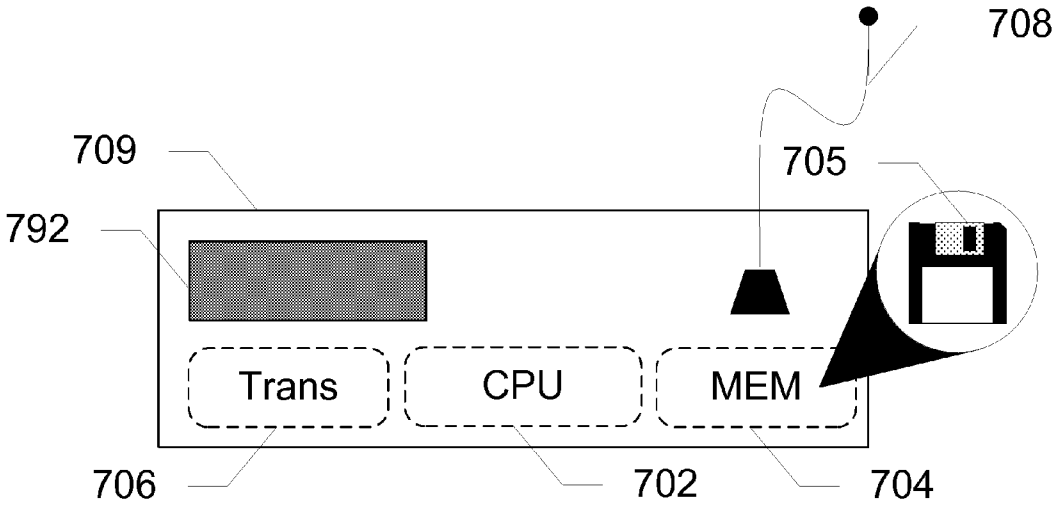


Figure 7B

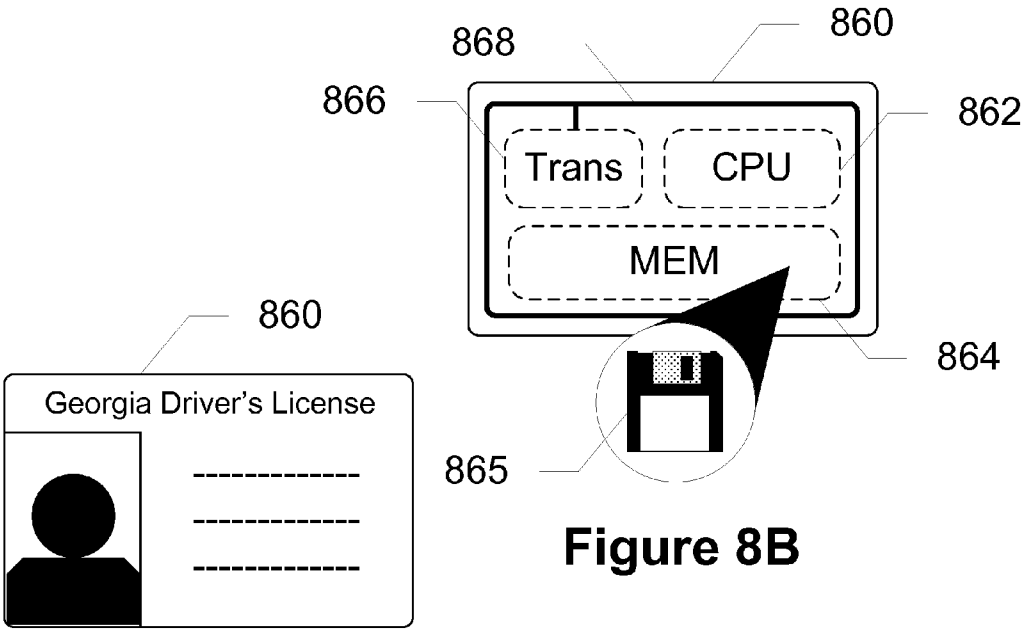


Figure 8B

Figure 8A

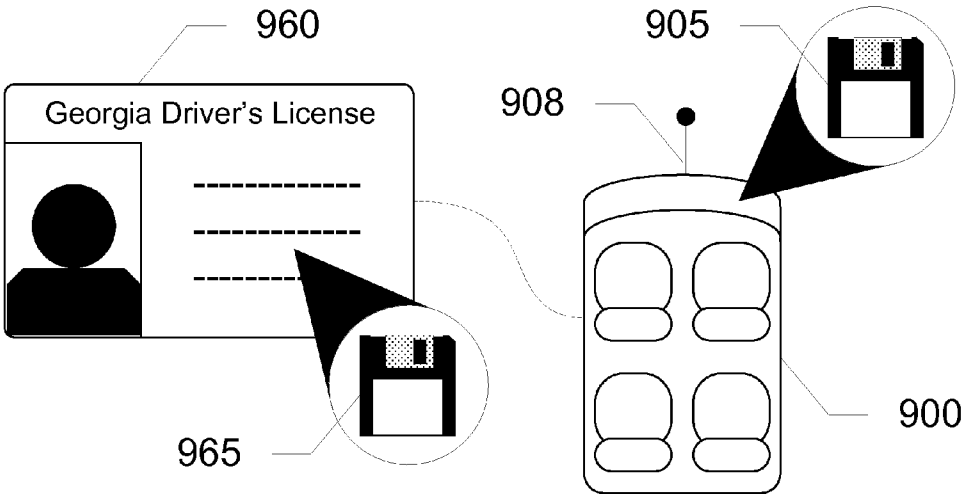


Figure 9

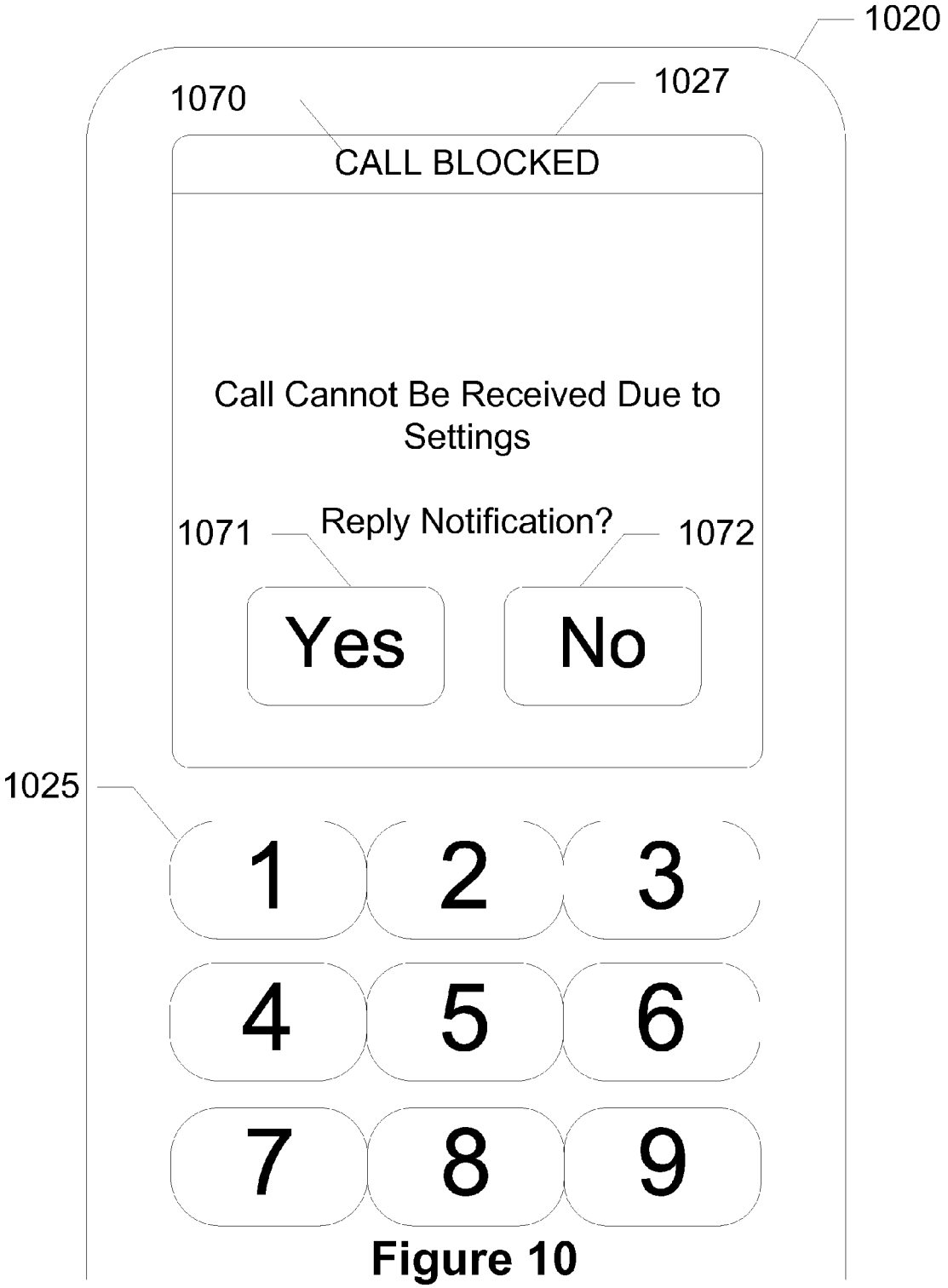

1020
1070
1027
CALL BLOCKED
Call Cannot Be Received Due to Settings
Reply Notification?
1071
1072
Yes
No
1025
1
2
3
4
5
6
7
8
9

Figure 10

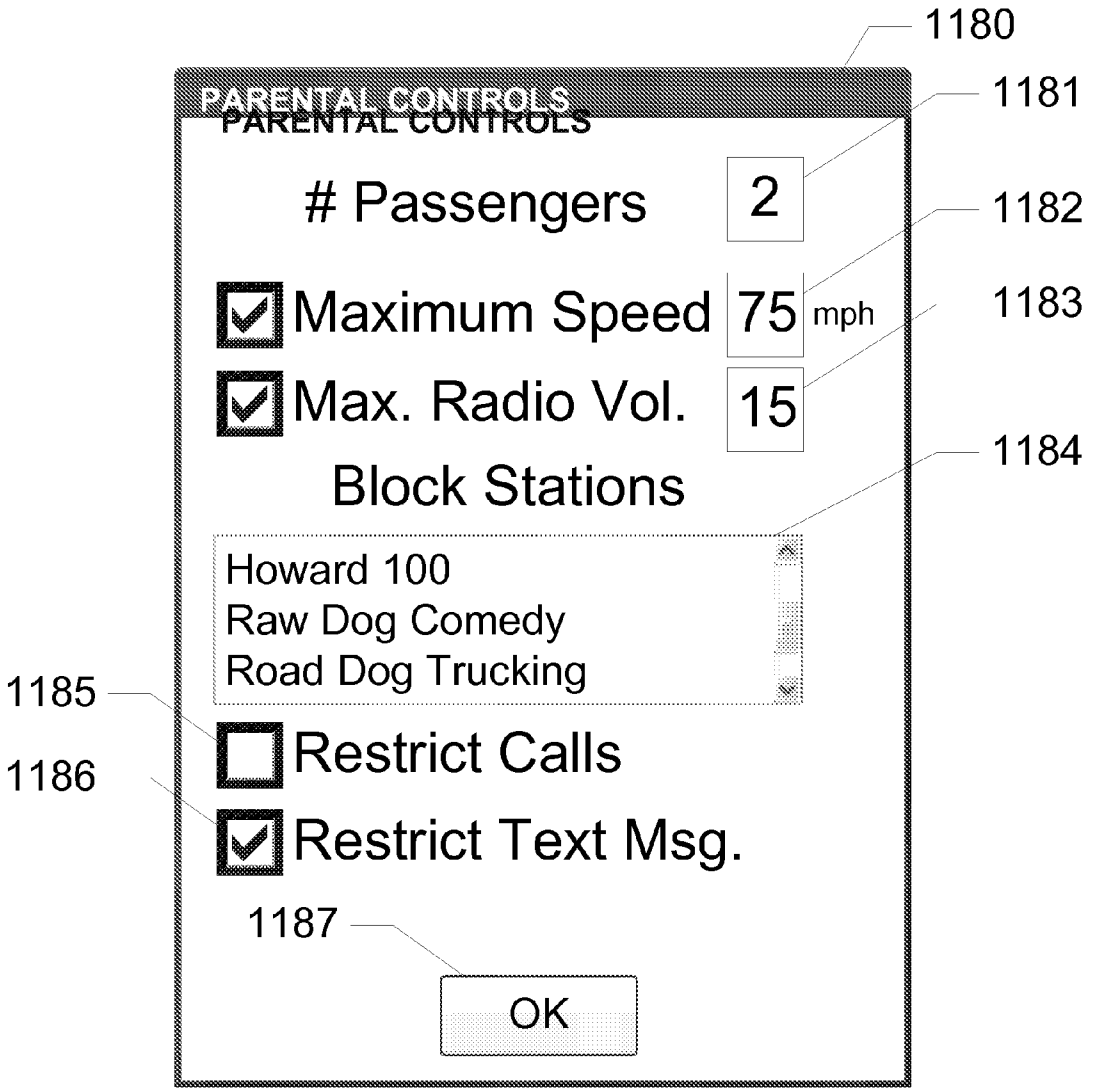

1180
PARENTAL CONTROLS
1181
Passengers
2
1182
Maximum Speed
75
mph
1183
Max. Radio Vol.
15
1184
Block Stations
Howard 100
Raw Dog Comedy
Road Dog Trucking
1185
Restrict Calls
1186
Restrict Text Msg.
1187
OK

Figure 11

DEVICES, SYSTEMS AND METHODS FOR CONTROLLING PERMITTED SETTINGS ON A VEHICLE

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] The present invention relates to vehicle driver identification. More specifically, the present invention relates to altering permitted settings of a vehicle based upon a driver.

[0003] 2. Background of the Invention

[0004] Car crashes are the leading cause of death for teens in the United States, with accidents while driving causing 36% of all deaths in this age group. The risk of a crash is much higher during the first years a teenager is able to drive. Teenage drivers tend to underestimate hazardous driving situations and are less able than more experience drivers to recognize dangerous situations.

[0005] Along with their lack of mature driving habits, teenagers often create many distractions while driving. Listening to loud music may prevent a teenager from noticing an emergency vehicle or oncoming car. Having teen male passengers in the car has been shown to increase the likelihood of high risk driving behaviors among teenage male drivers. Talking on the phone while driving is estimated to increase the risk of a crash fourfold. These extra distractions cause parents to worry, and, while very dangerous, may be very preventable.

[0006] Present-day technology can alleviate some of these distractions. Notably, microelectronic devices are becoming more and more ubiquitous. By coupling processors, memories, and transceivers to these devices, almost any handheld object can become a wireless communication device capable of transmitting and receiving data over a network. It is easy to set up a personal-area network with a few such devices incorporated into various everyday objects. However, this functionality is currently not being exploited to its full level.

[0007] What is needed is a means for identifying a driver of a vehicle in order to place restrictions or otherwise create settings for the driver.

SUMMARY OF THE INVENTION

[0008] The present invention addresses the above-identified issues by altering permitted settings of a vehicle according to a driver identified through short range wireless communication. In exemplary embodiments, a smart vehicle captures a unique identifier from a wireless communication device of the driver of the smart vehicle. This unique identifier is used to reference a database to determine the identity of the driver as well as settings for the driver created by a controlling authority. The controlling authority may be, for instance, a parent or employer of the driver. The settings may limit certain devices within the smart vehicle and/or the smart vehicle itself. Speed control settings, radio settings, wireless communication device settings, and various other settings are all possible to limit distractions to the driver. Further, the settings may be influenced by the number or identities of passengers within the smart vehicle.

[0009] In one exemplary embodiment, the present invention is a system for controlling a driver's settings, the system including a network; a smart vehicle in communication with the network; a wireless communication device in communication with the smart vehicle; a settings server on the network, the settings server including a user account for a user of the wireless communication device, the user account including permitted settings for the user; a client logic on the smart vehicle to retrieve a unique identifier from the wireless communication device and transmit the unique identifier to the settings server; and a server logic on the settings server to associate the unique identifier with the user account, determine the permitted settings for the user, and transmit the permitted settings to the client logic, wherein the client logic limits functions of the smart vehicle based upon the permitted settings.

[0010] In another exemplary embodiment, the present invention is a method for controlling a driver's settings, the method including requesting a unique identifier from a wireless communication device in communication with a smart vehicle; receiving the unique identifier from the wireless communication device and determining an identity of a driver in possession of the wireless communication device based upon the unique identifier; referencing settings corresponding to the identity of the driver; and implementing the settings, wherein the settings are chosen by a controlling authority and include one or more of permitted speed settings, permitted radio settings, and permitted use of the wireless communication device.

[0011] In yet another exemplary embodiment, the present invention is a smart vehicle, including a vehicle; a processor coupled to the vehicle; a memory in communication with the processor; a transceiver in communication with the processor; an antenna coupled to the transceiver; and a client logic on the memory to retrieve a unique identifier from a wireless communication device, determine an identity of a user of the wireless communication device based upon the unique identifier, determine permitted settings for the user, the permitted settings created by a controlling authority, and implement the permitted settings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. **1** shows a system for controlling a driver's settings, according to an exemplary embodiment of the present invention.

[0013] FIG. **2** shows a smart vehicle, according to an exemplary embodiment of the present invention.

[0014] FIG. **3** shows a method of controlling a driver's settings on a smart vehicle, according to an exemplary embodiment of the present invention.

[0015] FIG. **4** shows a smart vehicle with multiple occupants, each with a wireless communications device, according to an exemplary embodiment of the present invention.

[0016] FIG. **5** shows secondary means for verifying a driver's identity, according to an exemplary embodiment of the present invention.

[0017] FIG. **6** shows a smart vehicle including biometric sensors, according to an exemplary embodiment of the present invention.

[0018] FIGS. **7**A and **7**B show an aftermarket smart vehicle upgrade, according to an exemplary embodiment of the present invention.

[0019] FIGS. **8**A and **8**B show a contactless smart card embedded in a driver's license, according to an exemplary embodiment of the present invention.

[0020] FIG. **9** shows a smart vehicle detecting a driver's license, according to an exemplary embodiment of the present invention.

[0021] FIG. **10** shows a call block notification transmitted to a wireless communication device, according to an exemplary embodiment of the present invention.

[0022] FIG. **11** shows a screenshot of the creation of settings for a driver, according to an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0023] The following detailed description discloses devices, systems, and methods for identifying a driver within a vehicle using short range wireless communications in order to alter permitted settings of the vehicle. In exemplary embodiments a smart vehicle captures a unique identifier from a wireless communication device of the driver of the smart vehicle. This unique identifier is used to reference a database to determine the identity of the driver as well as settings for the driver created by a controlling authority. The controlling authority may be, for instance, a parent or employer of the driver. The settings may limit certain devices within the smart vehicle and/or the smart vehicle itself. Speed control settings, radio settings, wireless communication device settings, and various other settings are all possible to limit distractions to the driver. Further, the settings may be influenced by the number or identities of passengers within the vehicle.

[0024] "Wireless communication device", as used herein and throughout this disclosure, refers to any electronic device capable of wirelessly sending and receiving data. A wireless communication device may have a processor, a memory, a transceiver, an input, and an output. Examples of such devices include cellular telephones, personal digital assistants (PDAs), portable computers, etc. A wireless communication device also includes smart cards, such as contactless integrated circuit cards (CICC). The memory stores applications, software, or logic. Examples of processors are computer processors (processing units), microprocessors, digital signal processors, controllers and microcontrollers, etc. Examples of device memories that may comprise logic include RAM (random access memory), flash memories, ROMS (read-only memories), EPROMS (erasable programmable read-only memories), and EEPROMS (electrically erasable programmable read-only memories).

[0025] "Logic" as used herein and throughout this disclosure, refers to any information having the form of instruction signals and/or data that may be applied to direct the operation of a processor. Logic may be formed from signals stored in a device memory. Software is one example of such logic. Logic may also be comprised by digital and/or analog hardware circuits, for example, hardware circuits comprising logical AND, OR, XOR, NAND, NOR, and other logical operations. Logic may be formed from combinations of software and hardware. On a network, logic may be programmed on a server, or a complex of servers. A particular logic unit is not limited to a single logical location on the network.

[0026] Wireless communication devices communicate with each other and with other elements via a network, for instance, a wireless network, or a wireline network. A "network" can include broadband wide-area networks, local-area networks, and personal area networks. Communication across a network is preferably packet-based; however, radio and frequency/amplitude modulations networks can enable communication between communication devices using appropriate analog-digital-analog converters and other elements. Examples of radio networks include WiFi and BLUETOOTH® networks, with communication being enabled by hardware elements called "transceivers." A CICC, for instance, has an RFID transceiver. Wireless communication devices may have more than one transceiver, capable of communicating over different networks. For example, a cellular telephone can include a GPRS transceiver for communicating with a cellular base station, a WiFi transceiver for communicating with a WiFi network, and a BLUETOOTH® transceiver for communicating with a BLUETOOTH® device. A network typically includes a plurality of elements that host logic for performing tasks on the network.

[0027] In modern packet-based wide-area networks, servers may be placed at several logical points on the network. Servers may further be in communication with databases and can enable communication devices to access the contents of a database. A settings server is an example of such a server. A settings server can include several network elements, including other servers, and is part of a network, for example, a cellular network. A settings server hosts or is in communication with a database hosting an account for a user of a wireless communication device. The "user account" includes several attributes for a particular user, including a unique identifier of the wireless communication device(s) owned by the user, relationships with other users, driver settings, and other information.

[0028] A "vehicle," as used herein and throughout this disclosure, includes cars, trucks, and buses, as well as aircrafts and watercrafts.

[0029] For the following description, it can be assumed that most correspondingly labeled structures across the figures (e.g., **132** and **232**, etc.) possess the same characteristics and are subject to the same structure and function. If there is a difference between correspondingly labeled elements that is not pointed out, and this difference results in a non-corresponding structure or function of an element for a particular embodiment, then that conflicting description given for that particular embodiment shall govern.

[0030] FIG. **1** shows a system for controlling a driver's settings, according to an exemplary embodiment of the present invention. In this embodiment, the system includes a smart vehicle **100** with a client logic **105**, a wireless communication device **120** with a wireless logic **122**, a network **140**, and a settings server **130** with a server logic **132** and a database **134**. Smart vehicle **100** is in communication with wireless communication device **120** and with settings server **130** over network **140**. Wireless communication device **120** is shown outside smart vehicle **100** for purposes of showing the flow of communication only. It is to be understood that wireless communication device **120** is used by the driver of smart vehicle **100**. Wireless communication device **120** may be, for instance, a cellular telephone or a contactless smart card. Smart vehicle **100** transmits a request to wireless communication device **120**, and wireless logic **122** responds with a unique identifier of wireless communication device **120**. In the case of a cellular telephone, the unique identifier may be an MSISDN, IMSI, MAC address, etc. In the case of a contactless smart card, the unique identifier can be any alphanumeric, hexadecimal, or other unique string of characters. Client logic **105** on smart vehicle **100**, via an antenna and transceiver, receives the unique identifier from wireless communication device **120** and determines the identity of the driver.

[0031] Client logic **105** transmits the unique identifier and location to settings server **130** via network **140**. This transmission may occur via WiFi, GPRS, or other protocols capable of communicating such information across a wide-area network such as the Internet. Settings server **130**

includes settings for the driver that is associated with the unique identifier transmitted from wireless communication device **120**. The settings, at least in part, are set by a controlling authority, such as a parent or superior of the driver. The settings may be set by the controlling authority through a web browser, by text message, by a dedicated application on the authority's wireless communication device, etc. Server logic **132** matches the driver's identity with corresponding settings from database **134** on settings server **130**. The settings may include driver created settings as well as controlling authority settings, such as parental controls, based upon the driver's identity. The driver created settings may include seat and mirror positions, programmed radio stations, temperature controls, etc. The controlling authority settings may include a maximum speed of smart vehicle **100**, radio controls, wireless communication device controls, passenger based controls, etc.

[0032] The maximum allowed speed of smart vehicle **100** may be set by the controlling authority. For instance, a parent may not want his or her child to drive above seventy miles per hour. The parent uploads this setting to the settings server using a wireless communication device in communication with settings server **130** over network **140**, using a personal computer in communication with the settings server **130** over network **140**, etc. When smart vehicle **100** determines that the child is driving, smart vehicle **100** limits the maximum speed that smart vehicle **100** will travel. This may be accomplished, for example, by using a speed governor on smart vehicle **100**. Even if the child attempts to exceed the maximum allowed speed, the speed governor will prevent this action.

[0033] Radio controls may also be set by the controlling authority. The controlling authority may set a maximum radio volume, allowed radio stations, prohibited radio stations, prohibited compact discs, etc. For example, certain satellite radio stations use language or play songs which a parent may not wish their child to listen to, especially while driving. The parent may prohibit these stations in the settings for the child. An employer may not want an employee to play loud music while driving the company car. The employer may set a maximum volume level for employees in the settings for each employee, for the smart vehicle, for certain times, etc.

[0034] Wireless communication device controls restrict the actions allowed by the driver's wireless communication device **120**. For example, the driver's wireless communication device **120** may be prohibited from accepting calls or creating text messages while the key is in the ignition. Other features of the driver's wireless communication device **120** may also be limited. The restrictions may be executed via a "crippling" application installed on the driver's wireless communication device, by editing registry entries of an operating system of the driver's wireless communication device, by limiting services offered by the network during the course of driving the smart vehicle (such as disabling text messages), or by any equivalent means known in the art.

[0035] In embodiments of the present invention, the settings may further include the number of passengers in the smart vehicle or the identities of passengers. For instance, the radio control settings or speed control settings may be dependent upon the number of passengers or their identities. For example, when a young driver has a passenger, the settings may prevent the radio from being played and may set a maximum speed of the smart vehicle. When, however, the passenger is the young driver's parent, the smart vehicle can identify the parent, much like the identification of the driver, and remove or alter the settings.

[0036] Further settings may be based upon the time of day. The controlling authority may set a lower maximum permitted speed for certain hours, for instance, at night. The controlling authority may disable functions of the smart vehicle when the smart vehicle should not be in use. For example, a parent may limit the function of the smart vehicle during school hours so that his or her child is not tempted to skip class and drive off of school grounds.

[0037] In embodiments of the present invention, a notification may be sent to the controlling authority should the driver attempt to bypass or override the settings. This notification may be in the form of a text message, e-mail, etc. and may be automatically sent by the smart vehicle or settings server. For example, a text message may be sent to a wireless communication device of the controlling authority from the smart vehicle if the driver attempts to exceed the maximum permitted speed.

[0038] In further embodiments of the present invention, the settings may be stored on the driver's wireless communication device or on the memory of the smart vehicle. In these embodiments, the settings may be uploaded from the settings server to the driver's wireless communication device or the smart vehicle's memory. Alternatively, the settings may be directly set or uploaded by a second wireless communication device, such as that of a parent of the driver. In this alternative embodiment, the settings server may not be necessary to the system. The driver's wireless communications device would communicate with client logic of the smart vehicle and create settings which are stored on the memory of the wireless communications device or the smart vehicle. Various other settings are possible and would be apparent to one of ordinary skill in the art in light of this disclosure.

[0039] FIG. **2** shows a smart vehicle **200**, according to an exemplary embodiment of the present invention. In this embodiment, smart vehicle **200** is a vehicle which includes a central processing unit (CPU) **202**, a memory **204** storing client logic **205**, a transceiver **206**, an antenna **208**, a driver seat **210**, and passenger seats **212**. The vehicle can be any car, truck, boat, or aircraft. CPU **202** commands components of smart vehicle **200** according to client logic **205** on memory **204**. Transceiver **206** allows smart vehicle **200** to wirelessly communicate with other devices on a network, for instance a personal area network within smart vehicle **200**, a server on a network, other wireless devices, and so on. This communication may be through cellular radio frequency (RF) signals, WiFi, BLUETOOTH, infrared (IR), ZIGBEE™, etc. Antenna **208** is a transducer designed to transmit or receive electromagnetic waves.

[0040] The determination of a driver's identification and the subsequent initiation of the corresponding settings for the driver are performed by smart vehicle **200**, in this exemplary embodiment, as follows. Transceiver **206**, via antenna **208**, detects the presence of wireless communication devices located within smart vehicle **200**. At least the driver of smart vehicle **200** carries with them a wireless communication device such as a cellular telephone or a contactless smart card. The driver's wireless communication device is able to transmit a unique identifier corresponding to a user account for the driver. In the case of a cellular telephone, the unique identifier may be an MSISDN, IMSI, MAC address, etc. In the case of a contactless smart card, the unique identifier can be any alphanumeric, hexadecimal, or other unique string of charac-

ters. Using short range wireless communications, such as near-field communication or BLUETOOTH, antenna **208** transmits a request for the unique identifier from the driver's wireless communication devices within range of antenna **208**. The driver's wireless communication device responds with the unique identifier. Client logic **205** retrieves the unique identifier from the driver's wireless communication device and associates the identifier with a plurality of driver settings. These driver settings may be contained on memory **204**, may be contained on an external server, may be contained on the driver's wireless communication device, etc.

[0041] In many instances, more than one wireless communication device may be located within smart vehicle **200**. The determination of a driver versus a passenger may be determined via a proximity measurement derived from signal strength, delay, or other measurements from antenna **208**. For instance, antenna **208** may be located closer to driver seat **210** than passenger seats **212** such that the driver's wireless communication device has the strongest communication link to antenna **208**, along with the shortest delay. Therefore, a driver is easily determined by placing antenna **208** significantly closer to the driver than any passenger. This ensures that antenna **208** perceives a measurable difference between signals from the driver and signals from a passenger.

[0042] As previously stated, the settings may further include the number of passengers in the smart vehicle or the identities of passengers. For instance, the radio control settings or speed control settings may be dependent upon the number of passengers or their identities. Thus, if antenna **208** detects wireless communication devices of the passengers, client logic **205** references the settings for the determined number of passengers.

[0043] FIG. **3** shows a method of controlling a driver's settings on a smart vehicle, according to an exemplary embodiment of the present invention. In this embodiment, the method begins with the smart vehicle communicating with a driver's device S**350**. This device may be a wireless communications device, such as a cellular telephone, a contactless smart card, etc. The communication may occur as the driver enters the smart vehicle, as the driver starts the smart vehicle, etc. The smart vehicle communicates with the wireless communication device using short range wireless communication to request a unique identifier for the driver's wireless communication device. This short range wireless communication may be a personal area network, WiFi, BLUETOOTH, NFC, ZIGBEE, etc. In the case of a cellular telephone, the unique identifier may be an MSISDN, IMSI, MAC address, etc. In the case of a contactless smart card, the unique identifier can be any alphanumeric, hexadecimal, or other unique string of characters. The unique identifier is associated with a user of the smart vehicle. With the unique identifier, the smart vehicle determines the identity of the driver S**351**. A client logic and processor on the smart vehicle compares the unique identifier with a set of unique identifiers stored on a memory of the smart vehicle. Alternatively, the unique identifier may be compared with a set of unique identifiers on a server on a network. With the identity of the driver determined, the smart vehicle looks up settings for the driver S**352**. These settings may include driver created settings, controlling authority settings, etc. The settings are determined by comparing the driver's identity with a database of identities with corresponding settings. This database may be on the network, on the driver's device, on the smart vehicle's memory, etc. With the settings determined for the driver, the smart vehicle detects an attempted change of a setting S**353**. This may be the driver speeding up, the radio volume changing, the radio station changing, the driver's wireless communication device receiving an incoming call or text, etc. The smart vehicle determines whether the attempted change of the setting is permitted S**354**. This is accomplished by the client logic of the smart vehicle comparing the detected attempted change with the database of permitted or prohibited settings for the driver. If the change in setting is permitted, the change is allowed S**355**. For instance, the radio volume increases, the radio station changes, the call is received, the smart vehicle accelerates, etc. If the attempted setting is not permitted, the setting is rejected S**356**. For instance, the radio volume cannot be raised above the permitted setting, the radio station does not change, the call is not received, the smart vehicle does not accelerate above the maximum permitted speed, etc.

[0044] FIG. **4** shows a smart vehicle **400** with multiple occupants, each with a wireless communications device, according to an exemplary embodiment of the present invention. In this embodiment, smart vehicle **400** is carrying three occupants: a driver, and two passengers. The driver is a user of driver's wireless communication device **420**, a front seat passenger is a user of wireless communication device **424**, and a backseat passenger is a user of wireless communication device **426**.

[0045] An antenna and transceiver in smart vehicle **400** are used by client logic to determine the number of passengers, based upon the number of wireless communication devices located within smart vehicle **400**. For instance, wireless communication devices **420**, **424**, and **426** are detected and smart vehicle **400** determines there is a driver and two passengers. Smart vehicle **400** identifies the driver using the methods described herein, i.e. by capturing a unique identifier from driver's wireless communication device **420**. With multiple devices, smart vehicle **400** determines wireless communication device **420** belongs to the driver, as wireless communications device **420** is closest to the antenna located near the driver's seat. Smart vehicle **400** references the settings for the driver from a memory on smart vehicle **400**, a database on a network, a memory of wireless communication device **420**, etc. For instance, a parent may place restrictions on his or her child based upon the number of passengers in the vehicle, as higher numbers of passengers tend to distract the driver. With the two passengers in the car, the child may not be able to listen to the radio, or only listen at a low volume, as the radio may add another distraction. The speed of smart vehicle **400** may be limited in order to prevent the child from trying to drive fast, such as to "impress friends", etc.

[0046] Other restrictions may be placed upon the driver based upon the identity of a passenger. The identity of a passenger may be determined similarly to that of the driver, by requesting and receiving a device identifier. The identity of the passenger may place further restrictions on the driver. For instance, if the passenger is the driver's younger sibling, restrictions may be put in place to protect the younger sibling. This may include limiting the maximum speed, blocking certain radio stations, etc. If the passenger is a friend, different restrictions may be placed on the driver. These restrictions may be in place to limit distractions. If the passenger is a parent of the driver, restrictions may be taken away. For instance, restrictions that may usually occur with two passengers may not take effect if the parent is in the car, as determined by the device identifier of the parent's device. As

families often share devices, such as cellular phones, biometrics may also be utilized to determine the driver, passenger, etc.

[0047] The present invention also allows for several secondary means of driver identification. One can conceive of situations where an occupant of a smart vehicle is not instantly detectable. For instance, a wireless communication device may be switched off or a battery dies. The wireless communication device may be placed in a purse or bag and put in the back seat, or another part of the smart vehicle, or held by a passenger. The device may be shared by multiple users. This can result in mistaken driver identification. Therefore, embodiments of the smart vehicle include a plurality of secondary identification means, including biometrics and weight sensors. These backup means for driver and passenger identification introduce a redundancy to the present invention, allowing the settings control system to verify that the correct party is determined to be the driver and appropriate settings are enforced.

[0048] FIG. **5** shows secondary means for verifying a driver's identity, according to an exemplary embodiment of the present invention. Smart vehicle **500** comes equipped with a CPU **502**, a memory **504**, a transceiver **506**, an antenna **508**, and a driver seat **510**. As described above, CPU **502**, based on logic stored on memory **504**, controls transceiver **506** to detect the presence of and unique identifiers from any wireless communication devices located within smart vehicle **500**. A driver's wireless communication device is identified by its relative proximity to antenna **508**, which is positioned significantly closer to driver seat **510** than any other seat in smart vehicle **500**.

[0049] However, in the case that an identity of a driver cannot be ascertained, smart vehicle **500** includes a plurality of secondary sensors. These include a biometric identifier **514**, for instance, a fingerprint scanner placed on the steering wheel. A database of drivers' fingerprints is stored on memory **504** or externally on a network, and the detected fingerprint is associated with a driver's identity. Although this can be used for security purposes (such as starting the smart vehicle, reporting a stolen vehicle, etc.) or for convenience purposes (such as adjusting the seat back/position/mirrors based on the identified driver), the present invention uses this biometric identifier to associate the driver with a user account associated with the driver. Thus, if the driver's wireless communication device is switched off or undetectable, the driver can still be determined and the appropriate settings put in place.

[0050] Smart vehicle **500** further includes a weight scale **516** coupled to driver seat **510**. Weight scale **516** determines a weight of a driver. Weight scale **516** can include a strain gauge, piezoelectric sensor, etc. The measured weight serves several purposes including identifying whether or not a driver is present in smart vehicle **500**. Using this, a false driver identification is avoided even if a passenger's wireless communication device is detected to be in proximity of antenna **508**. Further, a particular weight or range of weights can be programmed to correspond to specified driver profiles, such that smart vehicle **500** is aware which driver is driving smart vehicle **500**, and thereby transmits the appropriate driver's identity to the settings server or the client logic on memory **504** for determining appropriate settings. Combinations of these secondary sensors are possible, and will be apparent to one skilled in the art in light of this disclosure.

[0051] The concept of backup identification can also be applied to the passengers in the smart vehicle. FIG. **6** shows a smart vehicle **600** including biometric sensors, according to an exemplary embodiment of the present invention. In this embodiment, smart vehicle **600** includes an antenna **608**, positioned near a driver's seat **610** of smart vehicle **600**. Each seat is equipped with a biometric sensor, such as fingerprint readers **614**, and weight scales **616**. Biometric sensors are in communication with a processor and memory (not shown) for determining the driver and implementing settings based upon the driver and passengers.

[0052] Secondary sensors **614** and **616** serve to verify an identity of a driver and passengers as described above. Furthermore, weight scales **616** can help smart vehicle **600** to determine a number of passengers regardless of whether or not the passengers have wireless communication devices. Therefore, the number of passengers can be counted even if no unique identifiers are received by antenna **608**. Furthermore, fingerprint readers **614** provide a verification of the identity of passengers, so as to avoid errors in case a wireless communication device belonging to a driver or a passenger is moved around smart vehicle **600**. In some exemplary embodiments weight scales **616** are used merely to determine passenger presence and not necessarily passenger identity.

[0053] The above embodiment disclosed a smart vehicle having an in-dash transceiver, processor, and memory to control settings of the smart vehicle. However, the present invention allows for the entire functionality of the smart vehicle to be incorporated into a single aftermarket unit that can be used to upgrade any basic vehicle into a smart vehicle. FIGS. **7**A and **7**B show such an aftermarket smart vehicle upgrade **709**, according to an exemplary embodiment of the present invention. Upgrade **709** mimics the form factor of traditional in-dash head units such as CD players or car audio receivers, and includes a display **791**, a control panel **719**, and can also include a disc-reader **790**. Display **791** is any LCD or equivalent display, control panel **719** includes buttons, sliders, etc., and disc reader **790** can play audio and data discs such as CDs, DVDs, etc. The inner components of upgrade **709** include a CPU **702**, a memory **704** having client logic **705** stored therein, a transceiver **706**, an antenna **708**, and a wire harness **792**. The functions of CPU **702**, memory **704**, transceiver **706**, and antenna **708** in the aftermarket unit are substantially similar to the functions of the equivalent components of the smart vehicle, which have been amply described above. Note that the placement of antenna **708** is flexible, thereby allowing a user to configure the upgrade to conform to a particular vehicle. Antenna **708** has a long wire connecting it to upgrade **709** allowing antenna **708** to be placed near the driver's seat inside vehicle.

[0054] Wire harness **792** provides an interface to other components of a vehicle. In traditional in-dash head units, wire harnesses **792** provide an interface to the speakers, amplifiers, fuse boxes, and other electrical systems of a vehicle. In this embodiment, wire harness **792** can further provide an interface to various sensors within the vehicle, such as speedometers, external transceivers, biometric/weight sensors embedded in the seats, etc. Therefore a controlling authority who installs upgrade **709** in their vehicle can program settings directly into upgrade **709** via display **791** and control panel **719**. Further, disc reader **790** can be used to program new settings, load databases of settings for different drivers, and other information.

[0055] A wireless communication device includes many devices having a processor, memory, and transceiver. A contactless smart card includes all of the above, and in some

embodiments, can be integrated into any object that a driver or passenger carries around all the time. Thus, no extra effort is needed to ensure that the wireless communication device is on the user's person at all times. For instance, a contactless smart card can be embedded in a user's driver's license. Since the driver is required by law to carry positive identification at all times while driving, a smart vehicle equipped with a contactless smart card reader will always be able to determine the driver's identity, and therefore implement settings for the driver based on his or her identity.

[0056] FIGS. **8**A and **8**B show a contactless smart card embedded in a driver's license **860**, according to an exemplary embodiment of the present invention. Driver's license **860** includes embedded within it a CPU **862**, a memory **864** having wireless logic **865** stored therein, a transceiver **866** and an antenna **868**. CPU **862** controls the sending and receiving of signals via transceiver **866** based on wireless logic **865** stored on memory **864**. Antenna **868** receives RF signals from the smart vehicle and transmits them to transceiver **866**. Antenna **868** further acts as an inductor to capture the RF signal from the smart vehicle, rectify it, and thereby power the other components. In an alternative embodiment, the contactless smart card includes a power supply, thereby allowing driver's license **860** to communicate across greater distances. Memory **864** additionally stores a unique identifier for the driver. Upon receiving an RF query from the smart vehicle, logic **865** retrieves the stored unique identifier and transmits it to the smart vehicle via transceiver **866**.

[0057] FIG. **9** shows a smart vehicle **900** detecting a driver's license **960**, according to an exemplary embodiment of the present invention. Driver's license **960**, including wireless logic **965**, is in communication with an antenna **908** of smart vehicle **900**. Client logic **905** onboard smart vehicle **900** enables antenna **908** to transmit an RF query within smart vehicle **900**. The RF query is sensed by an antenna of driver's license **960**. Wireless logic **965**, in response, transmits a unique identifier corresponding to the driver's identity back to client logic **905**. As described in the embodiments above, client logic **905** determines that the unique identifier corresponds to a driver's identity, depending on the placement of antennas **908**, and the strength and/or latency of the received signal. Upon a determination of the driver's identity, this information can be transmitted to a settings server to implement settings for the driver.

[0058] FIG. **10** shows a call block notification **1070** transmitted to a wireless communication device **1020**, according to an exemplary embodiment of the present invention. In this embodiment, wireless communication device **1020** belongs to the driver of a smart vehicle who has restrictions placed upon them while driving such that the driver cannot receive telephone calls. Call block notification **1070** notifies the driver that a call is incoming, but cannot be received. Wireless communication device **1020** includes a screen **1027** and a keypad **1025**. Screen **1027** displays call block notification **1070**, notifying the driver that the driver cannot receive calls while driving. The driver may, however, be given the option to automatically reply to the incoming call to notify the caller that the driver cannot take the call. To accomplish this, call block notification **1070** includes a 'Yes' button **1071** and a 'No' button **1072**. Selecting 'Yes' button **1071** confirms that the driver wishes to reply to the caller. Selecting 'No' button **1072** confirms that the driver does not wish to reply to the caller. Keypad **1025** allows the driver to input an acceptance or denial of the reply, but may be locked to prevent the driver from being otherwise distracted. A similar notification can be sent to wireless communication device **1020** in the event of an incoming text, etc.

[0059] FIG. **11** shows a screenshot of the creation of settings for a driver, according to an exemplary embodiment of the present invention. The settings may be created on a wireless communications device in communication with a network, on a personal computer in communication with the network through a web portal, on a screen in a vehicle, etc. In this embodiment, the settings are in the form of parental controls **1180**. Parental controls **1180** includes a number of passengers entry **1181**, a maximum speed entry **1182**, a maximum radio volume entry **1183**, a station block selection **1184**, a call restriction option **1185**, and a text message restriction option **1186**. A parent or other controlling authority may use parental controls **1180** in order to control settings of a smart vehicle for certain drivers. Number of passengers entry **1181** allows the parent to choose a number of passengers to create settings for. In this instance, the parent is creating settings that will occur when the specified driver has two passengers. The parent has checked the box of maximum speed entry **1182** and entered a maximum speed of seventy-five miles per hour for the driver. Thus, when the settings are in place and two passengers are present, if the driver attempts to exceed seventy-five miles per hour, a speed governor on the smart vehicle restricts these attempts. The parent has checked the box of maximum radio volume **1182** and has entered a maximum volume of fifteen. This maximum volume may be decibels, a volume unit on the radio, etc. With this setting in place, the driver is not able to play the radio at a volume in excess of the set limit when two passengers are present. The parent has the option of blocking certain radio stations with station block selection **1184**. Station block selection **1184** may present the parent with local radio stations available in the area, satellite radio stations, etc. The parent may select stations from a list, enter stations manually, etc. With these settings in place when two passengers are present, the smart vehicle will not allow the radio to be changed to these stations. Call restriction option **1185** prevents the driver from receiving calls on the driver's wireless communication device while driving. Text message restriction option **1186** prevents the driver from creating text messages on the driver's wireless communication device while driving. As previously stated, call restriction option **1185** and text message option **1186** may be executed via a "crippling" application installed on the driver's wireless communication device, by editing registry entries of an operating system of the driver's wireless communication device, by limiting services offered by the network during the course of driving the smart vehicle (such as disabling text messages), or by any equivalent means known in the art.

[0060] The foregoing disclosure of the exemplary embodiments of the present invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many variations and modifications of the embodiments described herein will be apparent to one of ordinary skill in the art in light of the above disclosure. The scope of the invention is to be defined only by the claims appended hereto, and by their equivalents.

[0061] Further, in describing representative embodiments of the present invention, the specification may have presented the method and/or process of the present invention as a particular sequence of steps. However, to the extent that the method or process does not rely on the particular order of

steps set forth herein, the method or process should not be limited to the particular sequence of steps described. As one of ordinary skill in the art would appreciate, other sequences of steps may be possible. Therefore, the particular order of the steps set forth in the specification should not be construed as limitations on the claims. In addition, the claims directed to the method and/or process of the present invention should not be limited to the performance of their steps in the order written, and one skilled in the art can readily appreciate that the sequences may be varied and still remain within the spirit and scope of the present invention.

What is claimed is:

1. A system for controlling a driver's settings, the system comprising:
- a network;
- a smart vehicle in communication with the network;
- a wireless communication device in communication with the smart vehicle;
- a settings server on the network, the settings server including a user account for a user of the wireless communication device, the user account including permitted settings for the user;
- a client logic on the smart vehicle to retrieve a unique identifier from the wireless communication device and transmit the unique identifier to the settings server; and
- a server logic on the settings server to associate the unique identifier with the user account, determine the permitted settings for the user, and transmit the permitted settings to the client logic,
- wherein the client logic limits functions of the smart vehicle based upon the permitted settings.

2. The system of claim **1**, wherein the permitted settings are created by a controlling authority.

3. The system of claim **2**, wherein the controlling authority is one or more of a parent of the driver and an employer of the driver.

4. The system of claim **1**, wherein the permitted settings include a maximum allowed speed of the smart vehicle.

5. The system of claim **1**, wherein the permitted settings include a radio setting.

6. The system of claim **5**, wherein the radio setting includes one or more of a maximum volume and a restricted station.

7. The system of claim **1**, wherein the permitted settings include a prohibition of the use of a function of the wireless communication device.

8. The system of claim **1**, further comprising:
- a driver seat in the smart vehicle;
- a passenger seat in the smart vehicle;
- a plurality of passenger wireless communication devices in communication with the smart vehicle; and
- an antenna coupled to the smart vehicle, the antenna being positioned significantly closer to the driver seat than the passenger seat;
- wherein the client logic:
  - retrieves a unique passenger identifier from each of the plurality of passenger wireless communication devices, and
  - changes the permitted settings based upon one or more of a number of passengers and an identity of a passenger.

9. The system of claim **1**, further comprising one of a biometric sensor and a weight scale coupled to a seat in the smart vehicle.

10. The system of claim **1**, wherein the wireless communication device is a contactless smart card.

11. A method for controlling a driver's settings, the method comprising:
- requesting a unique identifier from a wireless communication device in communication with a smart vehicle;
- receiving the unique identifier from the wireless communication device and determining an identity of a driver in possession of the wireless communication device based upon the unique identifier;
- referencing settings corresponding to the identity of the driver; and
- implementing the settings,
- wherein the settings are chosen by a controlling authority and include one or more of permitted speed settings, permitted radio settings, and permitted use of the wireless communication device.

12. The method of claim **11**, wherein the controlling authority is one or more of a parent of the driver and an employer of the driver.

13. The method of claim **11**, wherein the permitted speed settings include a maximum allowed speed of the smart vehicle.

14. The method of claim **11**, wherein the permitted radio settings includes one or more of a maximum volume and a restricted station.

15. The method of claim **11**, wherein the permitted use of the wireless communication device includes a prohibition of the use of a function of the wireless communication device.

16. The method of claim **11**, wherein the smart vehicle retrieves a unique passenger identifier from each of the plurality of passenger wireless communication devices located within the smart vehicle and changes the settings based upon one or more of a number of passengers and an identity of a passenger.

17. The method of claim **11**, further comprising sending a blocked call notification to the wireless communication device.

18. The method of claim **11**, wherein determining the identity of the driver further includes using one of a biometric sensor and a weight scale coupled to a seat in the smart vehicle.

19. A smart vehicle, comprising:
- a vehicle;
- a processor coupled to the vehicle;
- a memory in communication with the processor;
- a transceiver in communication with the processor;
- an antenna coupled to the transceiver; and
- a client logic on the memory to
  - retrieve a unique identifier from a wireless communication device,
  - determine an identity of a user of the wireless communication device based upon the unique identifier,
  - determine permitted settings for the user, the permitted settings created by a controlling authority, and
  - implement the permitted settings.

20. The smart vehicle of claim **19**, wherein the permitted settings include one or more of a maximum speed of the vehicle, a radio setting, and a prohibition of use of a function of the wireless communication device.

* * * * *