

Appendix E-3: Invalidity of the '244 Patent in view of Kleve

US20140129053A1 (“Kleve”), alone or in combination with other prior art identified in the cover pleading, anticipates and/or renders obvious all of the claims at issue. Nothing in this chart should be construed as an admission of infringement.

As described herein, claims of the '244 Patent are expressly or inherently anticipated by Kleve. In addition, to the extent that Kleve is found not to anticipate one or more of the asserted claims of the '244 Patent, those claims are invalid as obvious in view of Kleve alone, in combination with the knowledge of one of ordinary skill in the art, and/or other prior art, including but not limited to the prior art identified in the Exhibits E claim charts. With respect to the proposed modifications to Kleve, such modification would have been obvious to try, an obvious combination of prior art elements according to known methods to yield predictable results, a simple substitution of one known element for another to obtain predictable results, a use of known techniques to improve a similar devices or method in the same way, an application of a known technique to a known device or method ready for improvement to yield predictable results, a variation of a known work in one field of endeavor for use in either the same field or a different one based on design incentives or other market forces with variations that are predictable to one of ordinary skill in the art, and/or obvious in view of teachings, suggestions, and motivations in the prior art that would have led one of ordinary skill to modify or combine the prior art references.

The charts below demonstrate how, at least under EA’s apparent infringement theory, each of the asserted claims is anticipated by Kleve or is obvious over Kleve in further of the knowledge of a POSITA and/or one or more prior art references.

The claim chart below is meant to illustrate how the materials identified above invalidates the asserted claims. By not discussing other portions of the materials below, Defendants do not waive their right to rely on other portions of the materials; instead, Defendants expressly reserve their right to rely on other portions of the materials. These contentions are not an admission by Defendants that any accused products, including any past or current version of these products, are covered by or infringe Plaintiffs’ asserted claims, particularly once the claims are construed by the Court, and do not constitute an admission by Defendants as to the proper construction of any asserted claim and citations may be based on Plaintiffs’ apparent construction of the claims. Defendants does not agree with EA’s application of the claims, or that the claims satisfy 35 U.S.C. § 112. These contentions are not an admission by Defendants as to the proper scope of any asserted claim or the proper construction of any asserted claim. Defendant’s initial patent disclosures are made in a variety of alternatives and do not represent Defendant’s agreement or view as tranto the meaning, definiteness, written description support for, or enablement of any claim contained therein. Defendants reserve the right to modify, amend, or supplement these contentions as additional information becomes available during the course of this action and in view of any applicable claim construction order that the Court is anticipated to issue.

Claims	Prior Art
[1pre] 1. A method executed by a server of a cloud services system that is configured to interface with vehicles, comprising:	To the extent the preamble is limiting, Kleve expressly or inherently discloses “[a] method executed by a server of a cloud services system that is configured to interface with vehicles.” For example: Kleve at [0002] The embodiments described herein generally relate to a method and system for authorizing a vehicle rental micro-business.

Claims	Prior Art
	Kleve at [0035] In addition to having exemplary processes executed by a vehicle computing system located in a vehicle, in certain embodiments, the exemplary processes may be executed by a computing system in communication with a vehicle computing system. Such a system may include, but is not limited to, a wireless device (e.g., and without limitation, a cellular telephone) or a remote computing system (e.g., and without limitation, a server) connected through the wireless device. Collectively, such systems may be referred to as vehicle associated computing systems (VACS). In certain embodiments particular components of the VACS may perform particular portions of a process depending on the particular implementation of the system. By way of example and not limitation, if a process has a step of sending or receiving information with a paired wireless device, then it is likely that the wireless device is not performing the process, since the wireless device would not “send and receive” information with itself. One of ordinary skill in the art will understand when it is inappropriate to apply a particular VACS to a given solution. In all solutions, it is contemplated that at least the vehicle computing system (VCS) located within the vehicle itself is capable of performing the exemplary processes. Kleve at [0057]–[0058] In this illustrative embodiment, the centralized system is a server system that includes processing capability for incoming nomadic device signals designated to interact with a remote vehicle 421. For example, the server(s) 401 may include an automated call server and/or web host. Further, the server(s) 401 may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to enable a Temporary User keyless access and drive away capabilities of the Owner's vehicle. Data sent in this fashion may be sent using data-over-voice, a data-plan, or in any other suitable format. Data can also be sent to the vehicle 421 through the server(s) 401 using a personal computer 405. In this case, the data is likely, although not necessarily, sent over the internet 409. Once the server(s) 401 receive the incoming data request from the remote source 403, 405, the message is processed and/or relayed to a vehicle 421 and the Temporary User's nomadic device 402. The vehicle may be identified by a header associated with one or more incoming data packets, or may be identifiable based on a database lookup, for example. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.

Claims	Prior Art
[1a] receiving, by the server, a request from electronics of a vehicle to access a profile for a user account, the request identifies user information for a user to use the vehicle;	Kleve expressly or inherently discloses “receiving, by the server, a request from electronics of a vehicle to access a profile for a user account, the request identifies user information for a user to use the vehicle.” For example: Kleve at [0050] At 324, the Temporary User may have vehicle preset settings applied when renting a vehicle. These enhancements may include, but not limited to providing the Temporary User with stored frequent destinations sent to the VCS, radio presets, seat and mirror position, and ambient lighting preferences. The personalization of returning user's may also include a “bread crumb” feature allowing users to mark their usage to leave future users recommendations including which restaurant to eat at, or which routes to avoid. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[1b] processing, by the server, at least part of the user information to verify the user for accessing the profile associated with the user account, the profile having a plurality of settings of the user for the vehicle [and at least one of said plurality of settings being restricted for use on the vehicle, wherein] at least part of the plurality of settings for the profile being stored on storage accessible to the cloud services system; and	Kleve expressly or inherently discloses “processing, by the server, at least part of the user information to verify the user for accessing the profile associated with the user account, the profile having a plurality of settings of the user for the vehicle, wherein at least part of the plurality of settings for the profile being stored on storage accessible to the cloud services system” or, to the extent the claim is amended, Kleve expressly or inherently discloses “processing, by the server, at least part of the user information to verify the user for accessing the profile associated with the user account, the profile having a plurality of settings of the user for the vehicle and at least one of said plurality of settings being restricted for use on the vehicle, wherein at least part of the plurality of settings for the profile being stored on storage accessible to the cloud services system.” For example: Kleve at [0044] Another exemplary example of the vehicle rental micro-business system may include other enhancements including, but not limited to, matrix barcode (ex. two-dimensional code) used as the virtual key being recognized by the VCS. The smart phone may be used to communicate the matrix barcode information to the vehicle rental micro-business system directly. The system may be able to communicate information from the smart phone to the vehicle notifying the VCS of a virtual key. Once the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive away event.

Kleve at [0050]

At 324, the Temporary User may have vehicle preset settings applied when renting a vehicle. These enhancements may include, but not limited to providing the Temporary User with stored frequent destinations sent to the VCS, radio presets, seat and mirror position, and ambient lighting preferences. The personalization of returning user's may also include a "bread crumb" feature allowing users to mark their usage to leave future users recommendations including which restaurant to eat at, or which routes to avoid.

Kleve at [0059]

In one embodiment, a message is relayed to the remote source 403, 405 as well. For example, as will be described in further detail below, when an authorized temporary user remotely transmits a request from a Temporary User's nomadic device 402 (e.g., via a button or key press) to receive authorization to operate and drive away the vehicle 421, the server(s) 401 may respond by transmitting an authorization code to both the Temporary User's nomadic device 402 and to the vehicle control system for input by the authorized Temporary User at the vehicle 421. An authorized temporary user may be any individual recognized by the vehicle 421 as an authorized user based on a matrix barcode, a fingerprint scan, an authorized code typed in a touchscreen, voice recognition, and the like. It should be understood that these examples are non-limiting and other means of authorization for the vehicle rental micro-business may be used.

Kleve at [0063]

Additional Temporary User identification 504 may be sent to the vehicle Owner allowing for this information to be entered into the server and used as a virtual key, or in addition to the virtual key, allowing the Temporary User access to the Owner's vehicle while enabling a keyless drive-away. The Temporary User identification and virtual key may be sent in an encrypted message to the VCS, Temporary User's nomadic device, and/or vehicle Owners nomadic device. The Temporary User's information for vehicle authorization credential verification 516 may include, but not limited to fingerprint recognition of user, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode (ex. two-dimensional code), code word or code phrase for speech recognition, temporary mobile web login IDs and password, or other types of unique Temporary User identification.

Kleve at [0069]

FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a

Claims	Prior Art
	vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of generating a virtual key may be done by using Temporary User's credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614. At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606. Kleve at [0072] At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings. Another exemplary example of setting personal preferences may include, but not limited to, facial recognition to recognize the driver using a camera mounted in the vehicle cabin on the dash. Once the camera recognizes the Temporary User, the VCS may request additional user settings and preferences including seat adjustment, and climate control temperatures. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[1c] transferring, by the server, upon verifying the user information, one or more settings of the plurality of settings to [storage of] the vehicle,	Kleve expressly or inherently discloses “transferring, by the server, upon verifying the user information, one or more settings of the plurality of settings to the vehicle” or, to the extent the claim is amended, Kleve expressly or inherently discloses “transferring, by the server, upon verifying the user information, one or more settings of the plurality of settings to storage of the vehicle.” For example: Kleve at [0057]–[0058] In this illustrative embodiment, the centralized system is a server system that includes processing capability for incoming nomadic device signals designated to interact with a remote vehicle 421. For example, the server(s) 401 may include an automated call server and/or web host. Further, the server(s) 401 may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to

Claims	Prior Art
	enable a Temporary User keyless access and drive away capabilities of the Owner's vehicle. Data sent in this fashion may be sent using data-over-voice, a data-plan, or in any other suitable format. Data can also be sent to the vehicle 421 through the server(s) 401 using a personal computer 405. In this case, the data is likely, although not necessarily, sent over the internet 409. Once the server(s) 401 receive the incoming data request from the remote source 403, 405, the message is processed and/or relayed to a vehicle 421 and the Temporary User's nomadic device 402. The vehicle may be identified by a header associated with one or more incoming data packets, or may be identifiable based on a database lookup, for example. Kleve at [0060] The relay to the vehicle 421 is sent out from the server(s) 401 through a network (e.g., without limitation, a cellular network 113, the internet, etc.) and passed through a cellular network 415 to the vehicle 421. In another embodiment, the relay may be passed through network 414 (e.g., WiFi or WiMax) and to the vehicle 421. A remote communication module in the vehicle 421 receives the signal sent from the server(s) 401 and processes it or relays it to an appropriate processing system within the vehicle 421. Kleve at [0061] In at least one illustrative embodiment, the vehicle 421 is also outfitted with a communication transceiver, such as, but not limited to, a BLUETOOTH transceiver. This transceiver may allow communication with the nomadic device 403 using a direct signal 419. This transceiver may also allow communication with the Temporary User's nomadic device 402 to the vehicle 421 using a wireless connection 420 including, but not limited to, a smart phone that may connect to the vehicle through SYNC or other Bluetooth pairing device. It should be understood that the communication between nomadic device 403, temporary user nomadic device 402, server 401, and vehicle 421 may be performed in a number of ways and FIG. 4 is presented for illustrative purposes. FIG. 4 illustrates various alternatives for communicating data. For example, and without limitation, data communication may be partially or entirely cellular or WiFi, or a combination of cellular and WiFi. Kleve at [0072] At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings. Another exemplary example of setting personal preferences may include, but not limited to, facial recognition to recognize the driver using a camera mounted in the vehicle cabin on the dash. Once the camera recognizes the Temporary User, the VCS may request additional user settings and preferences including seat adjustment, and climate control temperatures.

Claims	Prior Art
	To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[1d] the transferring is configured to instruct software and/or hardware associated with said electronics of the vehicle to apply said one or more settings to the vehicle for customizing said vehicle to use said one or more settings associated with the profile,	Kleve expressly or inherently discloses “the transferring is configured to instruct software and/or hardware associated with said electronics of the vehicle to apply said one or more settings to the vehicle for customizing said vehicle to use said one or more settings associated with the profile.” For example: Kleve at [0056] FIG. 4 shows an illustrative example of a communication system through which a wireless communication device can communicate with a vehicle 421 to enable a vehicle rental micro-business. In this illustrative embodiment, a nomadic device (e.g., without limitation, a cellular phone, a personal cellular telephone) 403 is used to send a communication through a cellular network 407. This communication is relayed through a network 411 (e.g., without limitation, the cellular network, the internet, etc.) to a centralized system 401. In another embodiment, the nomadic device 403 may send a communication through network 412 which may include, but is not limited to, WiFi or WiMax. This communication is relayed through a network 406 (e.g., without limitation, cloud computing, the internet,) to a centralized system 401. Kleve at [0060] The relay to the vehicle 421 is sent out from the server(s) 401 through a network (e.g., without limitation, a cellular network 113, the internet, etc.) and passed through a cellular network 415 to the vehicle 421. In another embodiment, the relay may be passed through network 414 (e.g., WiFi or WiMax) and to the vehicle 421. A remote communication module in the vehicle 421 receives the signal sent from the server(s) 401 and processes it or relays it to an appropriate processing system within the vehicle 421. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[1e] wherein the vehicle uses wireless communication for exchanging data with the cloud services system and for receiving said one or more settings for the profile.	Kleve expressly or inherently discloses “wherein the vehicle uses wireless communication for exchanging data with the cloud services system and for receiving said one or more settings for the profile.” For example: Kleve at [0056] FIG. 4 shows an illustrative example of a communication system through which a wireless communication device can communicate with a vehicle 421 to enable a vehicle rental micro-business. In

Claims	Prior Art
	this illustrative embodiment, a nomadic device (e.g., without limitation, a cellular phone, a personal cellular telephone) 403 is used to send a communication through a cellular network 407. This communication is relayed through a network 411 (e.g., without limitation, the cellular network, the internet, etc.) to a centralized system 401. In another embodiment, the nomadic device 403 may send a communication through network 412 which may include, but is not limited to, WiFi or WiMax. This communication is relayed through a network 406 (e.g., without limitation, cloud computing, the internet,) to a centralized system 401. Kleve at [0060] The relay to the vehicle 421 is sent out from the server(s) 401 through a network (e.g., without limitation, a cellular network 113, the internet, etc.) and passed through a cellular network 415 to the vehicle 421. In another embodiment, the relay may be passed through network 414 (e.g., WiFi or WiMax) and to the vehicle 421. A remote communication module in the vehicle 421 receives the signal sent from the server(s) 401 and processes it or relays it to an appropriate processing system within the vehicle 421. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[2] 2. The method of claim 1, wherein the profile of the user is transferrable to one or more other vehicles from the cloud services system.	Kleve expressly or inherently discloses “[t]he method of claim 1, wherein the profile of the user is transferrable to one or more other vehicles from the cloud services system.” For example: Kleve at [0057]–[0058] In this illustrative embodiment, the centralized system is a server system that includes processing capability for incoming nomadic device signals designated to interact with a remote vehicle 421. For example, the server(s) 401 may include an automated call server and/or web host. Further, the server(s) 401 may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to enable a Temporary User keyless access and drive away capabilities of the Owner's vehicle. Data sent in this fashion may be sent using data-over-voice, a data-plan, or in any other suitable format. Data can also be sent to the vehicle 421 through the server(s) 401 using a personal computer 405. In this case, the data is likely, although not necessarily, sent over the internet 409. Once the server(s) 401 receive the incoming data request from the remote source 403, 405, the message is processed and/or relayed to a vehicle 421 and the Temporary User's nomadic device 402. The vehicle may be identified by a header associated with one or more incoming data packets, or may be identifiable based on a database lookup, for example.

Kleve at [0060]

The relay to the vehicle 421 is sent out from the server(s) 401 through a network (e.g., without limitation, a cellular network 113, the internet, etc.) and passed through a cellular network 415 to the vehicle 421. In another embodiment, the relay may be passed through network 414 (e.g., WiFi or WiMax) and to the vehicle 421. A remote communication module in the vehicle 421 receives the signal sent from the server(s) 401 and processes it or relays it to an appropriate processing system within the vehicle 421.

Kleve at [0061]

In at least one illustrative embodiment, the vehicle 421 is also outfitted with a communication transceiver, such as, but not limited to, a BLUETOOTH transceiver. This transceiver may allow communication with the nomadic device 403 using a direct signal 419. This transceiver may also allow communication with the Temporary User's nomadic device 402 to the vehicle 421 using a wireless connection 420 including, but not limited to, a smart phone that may connect to the vehicle through SYNC or other Bluetooth pairing device. It should be understood that the communication between nomadic device 403, temporary user nomadic device 402, server 401, and vehicle 421 may be performed in a number of ways and FIG. 4 is presented for illustrative purposes. FIG. 4 illustrates various alternatives for communicating data. For example, and without limitation, data communication may be partially or entirely cellular or WiFi, or a combination of cellular and WiFi.

Kleve at [0072]

At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings. Another exemplary example of setting personal preferences may include, but not limited to, facial recognition to recognize the driver using a camera mounted in the vehicle cabin on the dash. Once the camera recognizes the Temporary User, the VCS may request additional user settings and preferences including seat adjustment, and climate control temperatures.

Kleve at [0081]

In the illustrative embodiment shown in FIG. 8 is a flow-chart illustrating an example method of a vehicle owner interface with a vehicle rental authorization system. The owner may begin by setting up a user profile within the vehicle rental authorization system at step 802. The owner may interact with the vehicle rental authorization system through a website. The website may be formatted to allow the owner to input profile information using a personal computer, smart phone or other nomadic device. The user profile may include owner's personal information including details about the vehicle he intends to list as a rental within the vehicle rental authorization system. Information may include, but not limited to, owners name, home address, email address, and vehicle specifications including pictures. The vehicle

Claims	Prior Art
	rental authorization system may have one or more databases with a list of vehicle owners and rental vehicles available. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[4] 4. The method of claim 1, further comprising, receiving, by the server, communication from the vehicle regarding inputs made to systems of the vehicle during use of the vehicle while the vehicle is associated with the profile of the user account; determining, by the server, based on the inputs made to systems of the vehicle that at least one of the plurality of settings of the profile is to be updated.	Kleve expressly or inherently discloses “[t]he method of claim 1, further comprising, receiving, by the server, communication from the vehicle regarding inputs made to systems of the vehicle during use of the vehicle while the vehicle is associated with the profile of the user account; determining, by the server, based on the inputs made to systems of the vehicle that at least one of the plurality of settings of the profile is to be updated.” For example: Kleve at [0023] The processor is also provided with a number of different inputs allowing the user to interface with the processor. In this illustrative embodiment, a microphone 29, an auxiliary input 25 (for input 33), a USB input 23, a GPS input 24, touchscreen visual display 4 and a BLUETOOTH input 15 are all provided. An input selector 51 is also provided, to allow a user to swap between various inputs. Input to both the microphone and the auxiliary connector is converted from analog to digital by a converter 27 before being passed to the processor. Although not shown, numerous of the vehicle components and auxiliary components in communication with the VCS may use a vehicle network (such as, but not limited to, a CAN bus) to pass data to and from the VCS (or components thereof). Kleve at [0043]-[0044] At step 224, the system may notify the Temporary User that the agreed upon rental period may expire soon, and if the rental period has ended the system may prompt the Temporary User with a message asking if he would like to purchase additional rental time. The system may allow the Temporary User to purchase additional rental time or decline the offer with the use of the vehicle touchscreen display or a nomadic device at step 226. If the rental term has ended, and no additional time is purchased, the system may begin the vehicle rental exit process within the VCS at step 228. If the rental period is still within the agreed upon rental period, the system may carry on to monitor the vehicle allowing the Owner continued control of the vehicle with the use of vehicle restriction limits initially set by the Owner at the beginning of the rental term. At step 226, if the Temporary User decides that he may need to purchase additional rental time, the system may update the new rental period end time restriction and continue to monitor usage of the vehicle.

Claims	Prior Art
	Another exemplary example of the vehicle rental micro-business system may include other enhancements including, but not limited to, matrix barcode (ex. two-dimensional code) used as the virtual key being recognized by the VCS. The smart phone may be used to communicate the matrix barcode information to the vehicle rental micro-business system directly. The system may be able to communicate information from the smart phone to the vehicle notifying the VCS of a virtual key. Once the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive away event. Kleve at [0054] At 330, the VCS may continue to monitor the vehicle for the entire rental period. If the rental period is soon to expire the system may notify Temporary User at step 338. If the Temporary User has not returned the vehicle at the time the rental period has expired, the system may notify the user if a rental term extension is desired at step 342. If the extension term is desired, the Temporary User may be prompted to accept additional rental charges at step 344. The Temporary User may be charged for the additional rental time at step 346. If the extension of time is not desired, and/or not allowed by the Owner, the system may transmit controlling action to warn and induce remedial actions at step 350. If the extension of time is not desired, and the Temporary User is within the allocated time and distance to return the vehicle to the required parking location at step 348. If the Temporary User has returned to the required parking spot, the system may begin to prepare for return to the vehicle Owner. During the preparation to return vehicle to Owner and end the rental period, the system may save any enhancements information based on the Temporary User's settings at step 352. Kleve at [0059] In one embodiment, a message is relayed to the remote source 403, 405 as well. For example, as will be described in further detail below, when an authorized temporary user remotely transmits a request from a Temporary User's nomadic device 402 (e.g., via a button or key press) to receive authorization to operate and drive away the vehicle 421, the server(s) 401 may respond by transmitting an authorization code to both the Temporary User's nomadic device 402 and to the vehicle control system for input by the authorized Temporary User at the vehicle 421. An authorized temporary user may be any individual recognized by the vehicle 421 as an authorized user based on a matrix barcode, a fingerprint scan, an authorized code typed in a touchscreen, voice recognition, and the like. It should be understood that these examples are non-limiting and other means of authorization for the vehicle rental micro-business may be used.

Claims	Prior Art
	Kleve at [0071] At step 618, the Temporary User may send the virtual key to the server requesting access to the vehicle, or use a vehicle input device, like camera, microphone, fingerprint scanner or retinal scanner integrated with the VCS to capture his identity and/or payment credentials to enable a keyless drive-away. If it is the scheduled time for the rental, the vehicle may compare the identity credentials just inputted at the vehicle and the one previously sent virtual key to the vehicle from the vehicle Owner to determine authorization. If the comparison is successful, the vehicle may enable drive-away access to that Temporary User for the scheduled time period of the rental agreement. For the duration of the rental term, the Temporary User may again input the same identifying credentials to unlock and drive. Kleve at [0081] In the illustrative embodiment shown in FIG. 8 is a flow-chart illustrating an example method of a vehicle owner interface with a vehicle rental authorization system. The owner may begin by setting up a user profile within the vehicle rental authorization system at step 802. The owner may interact with the vehicle rental authorization system through a website. The website may be formatted to allow the owner to input profile information using a personal computer, smart phone or other nomadic device. The user profile may include owner's personal information including details about the vehicle he intends to list as a rental within the vehicle rental authorization system. Information may include, but not limited to, owners name, home address, email address, and vehicle specifications including pictures. The vehicle rental authorization system may have one or more databases with a list of vehicle owners and rental vehicles available. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[5] 5. The method of claim 4, further comprising, processing by a learning engine that uses the inputs made to the systems of the vehicle to find patterns in use of the systems of the vehicle while the profile was used with the vehicle.	Kleve expressly or inherently discloses “[t]he method of claim 4, further comprising, processing by a learning engine that uses the inputs made to the systems of the vehicle to find patterns in use of the systems of the vehicle while the profile was used with the vehicle.” For example: Kleve at [0050] At 324, the Temporary User may have vehicle preset settings applied when renting a vehicle. These enhancements may include, but not limited to providing the Temporary User with stored frequent destinations sent to the VCS, radio presets, seat and mirror position, and ambient lighting preferences. The personalization of returning user's may also include a “bread crumb” feature allowing users to mark

Claims	Prior Art
	their usage to leave future users recommendations including which restaurant to eat at, or which routes to avoid. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[6] 6. The method of claim 5, further comprising, sending, by the server, a recommended setting to the user account, the recommended setting is based on processing by the learning engine and said recommended setting is applied to the vehicle when the vehicle is used with the profile or is applied to the vehicle upon receiving acceptance of the recommended setting via the user account.	Kleve expressly or inherently discloses “[t]he method of claim 5, further comprising, sending, by the server, a recommended setting to the user account, the recommended setting is based on processing by the learning engine and said recommended setting is applied to the vehicle when the vehicle is used with the profile or is applied to the vehicle upon receiving acceptance of the recommended setting via the user account.” For example: Kleve at [0053] At 330, the VCS may monitor that a restriction threshold has been violated indicating that the Temporary User may be abusing the vehicle. At step 332, the Temporary User operating the vehicle under excessive conditions may cause the system to send an issue warning to the vehicle display information center. At step 334, the system may send a message to issue a warning to the Temporary User notifying of unauthorized usage of the vehicle at the display information center, instrument cluster, and/or other driver display device. If the system detects that the usage of the vehicle is extreme by exceeding a predetermined threshold, the VCS may command controlling actions to put the vehicle in a remedial action at step 336. The remedial actions may include, but not limited to, reduce engine power, engine shut down, and immobilization. The VCS may monitor and detect the Temporary User exceeding a restriction limit and may notify the Owner while implementing remedial actions that may include preventing the vehicle from being started. The display message to alert the Temporary User of a restriction violation may be sent to the vehicle display information console and/or to the temporary user's nomadic device. Kleve at [0079]–[0080] At step 718, the vehicle owner may also be notified if the system has a detected driver behavior event. The vehicle owner may be sent information that the Temporary User has been in an accident or near miss based on airbag deployment, accelerometer data, and/or anti-lock brake information. If the Temporary User is involved in an accident, the system may store and save previous recorded data leading up to the accident at step 720. For example, if the airbag is deployed the VCS may save three minutes of all monitored data leading up to the airbag deployment including, but not limited to, a dashboard camera, accelerator pedal position, speed, and brake pedal position at step 722. The monitoring system may

Claims	Prior Art
	continue to check to see if continued usage of the vehicle is acceptable based on the accident data/near miss data to determine if the vehicle is safe for continued operation at step 724. At 726, if the vehicle is in an acceptable condition for continued usage and rental time has not expired, the system may continue to monitor the vehicle rental usage. If the vehicle cannot be used, the VCS may begin the vehicle rental exit mode process at step 728. At step 718, if the VCS monitoring detects no accident, and the rental period has not expired, the system may continue to monitor the vehicle rental usage. If the rental period has ended, the monitoring and control system of the vehicle rental micro-business may begin to start its Temporary User vehicle rental exit mode process at step 728. The exit mode process may include the monitoring system to store additional variables and data to report to the vehicle Owner including, but not limited to, vehicle location, fuel level, and additional vehicle diagnostic information. The exit mode process may also include, but not limited to, terminating the virtual key while allowing the system to reset any private information stored on the vehicle-based computing system. The system may include a standardized report form that requires certain information the Temporary User must fill out when returning the vehicle. Kleve at [0084] At step 812, if the owner decides he has no interest in accepting the Temporary User's offer, he may decline and wait for the vehicle rental authorization system to notify of any other offers. If the owner has decided to accept the offer he may begin the process of developing terms and conditions of the rental period. At step 814, the owner may negotiate additional terms and conditions based on the specific use and needs the Temporary User may use the vehicle for. These additional terms and conditions may include, but not limited to, cargo load weight restrictions, tow load restrictions, or the amount of miles that can be driven during the rental period. The negotiation of the terms and conditions may be done using the vehicle authorization rental system. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[7] 7. The method of claim 5, wherein the patterns are correlated to one or more conditions, the one or more conditions include type of input, or time of day inputs, or temperature, or security, or number of occupants in the	Kleve expressly or inherently discloses “[t]he method of claim 5, wherein the patterns are correlated to one or more conditions, the one or more conditions include type of input, or time of day inputs, or temperature, or security, or number of occupants in the vehicle, or weather, or age of the vehicle, or service requirements of the vehicle.” For example: Kleve at [0053]

Claims	Prior Art
vehicle, or weather, or age of the vehicle, or service requirements of the vehicle.	At 330, the VCS may monitor that a restriction threshold has been violated indicating that the Temporary User may be abusing the vehicle. At step 332, the Temporary User operating the vehicle under excessive conditions may cause the system to send an issue warning to the vehicle display information center. At step 334, the system may send a message to issue a warning to the Temporary User notifying of unauthorized usage of the vehicle at the display information center, instrument cluster, and/or other driver display device. If the system detects that the usage of the vehicle is extreme by exceeding a predetermined threshold, the VCS may command controlling actions to put the vehicle in a remedial action at step 336. The remedial actions may include, but not limited to, reduce engine power, engine shut down, and immobilization. The VCS may monitor and detect the Temporary User exceeding a restriction limit and may notify the Owner while implementing remedial actions that may include preventing the vehicle from being started. The display message to alert the Temporary User of a restriction violation may be sent to the vehicle display information console and/or to the temporary user's nomadic device. Kleve at [0079]–[0080] At step 718, the vehicle owner may also be notified if the system has a detected driver behavior event. The vehicle owner may be sent information that the Temporary User has been in an accident or near miss based on airbag deployment, accelerometer data, and/or anti-lock brake information. If the Temporary User is involved in an accident, the system may store and save previous recorded data leading up to the accident at step 720. For example, if the airbag is deployed the VCS may save three minutes of all monitored data leading up to the airbag deployment including, but not limited to, a dashboard camera, accelerator pedal position, speed, and brake pedal position at step 722. The monitoring system may continue to check to see if continued usage of the vehicle is acceptable based on the accident data/near miss data to determine if the vehicle is safe for continued operation at step 724. At 726, if the vehicle is in an acceptable condition for continued usage and rental time has not expired, the system may continue to monitor the vehicle rental usage. If the vehicle cannot be used, the VCS may begin the vehicle rental exit mode process at step 728. At step 718, if the VCS monitoring detects no accident, and the rental period has not expired, the system may continue to monitor the vehicle rental usage. If the rental period has ended, the monitoring and control system of the vehicle rental micro-business may begin to start its Temporary User vehicle rental exit mode process at step 728. The exit mode process may include the monitoring system to store additional variables and data to report to the vehicle Owner including, but not limited to, vehicle location, fuel level, and additional vehicle diagnostic information. The exit mode process may also include, but not limited to, terminating the virtual key while allowing the system to reset any private information stored

Claims	Prior Art
	on the vehicle-based computing system. The system may include a standardized report form that requires certain information the Temporary User must fill out when returning the vehicle. Kleve at [0084] At step 812, if the owner decides he has no interest in accepting the Temporary User's offer, he may decline and wait for the vehicle rental authorization system to notify of any other offers. If the owner has decided to accept the offer he may begin the process of developing terms and conditions of the rental period. At step 814, the owner may negotiate additional terms and conditions based on the specific use and needs the Temporary User may use the vehicle for. These additional terms and conditions may include, but not limited to, cargo load weight restrictions, tow load restrictions, or the amount of miles that can be driven during the rental period. The negotiation of the terms and conditions may be done using the vehicle authorization rental system. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[8] 8. The method of claim 1, further comprising, accessing, by the server, a plurality of profiles of different users stored in the storage accessible to the cloud services system; detecting, by the server, similarities in patterns for inputs made to systems of vehicles associated with the profiles of different users; using, by the server, a learning engine to produce a recommended setting that is sent to the user account.	Kleve expressly or inherently discloses “[t]he method of claim 1, further comprising, accessing, by the server, a plurality of profiles of different users stored in the storage accessible to the cloud services system; detecting, by the server, similarities in patterns for inputs made to systems of vehicles associated with the profiles of different users; using, by the server, a learning engine to produce a recommended setting that is sent to the user account.” For example: Kleve at [0050] At 324, the Temporary User may have vehicle preset settings applied when renting a vehicle. These enhancements may include, but not limited to providing the Temporary User with stored frequent destinations sent to the VCS, radio presets, seat and mirror position, and ambient lighting preferences. The personalization of returning user's may also include a “bread crumb” feature allowing users to mark their usage to leave future users recommendations including which restaurant to eat at, or which routes to avoid. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.

Claims	Prior Art
[9] 9. The method of claim 1, wherein the request is automatically generated by the electronics of the vehicle upon detecting a pairing with a user device of the user, or input of credentials of the user for the user account.	Kleve expressly or inherently discloses “[t]he method of claim 1, wherein the request is automatically generated by the electronics of the vehicle upon detecting a pairing with a user device of the user, or input of credentials of the user for the user account.” For example: Kleve at [0025]–[0027] In one illustrative embodiment, the system 1 uses the BLUETOOTH transceiver 15 to communicate 17 with a user's nomadic device 53 (e.g., cell phone, smart phone, PDA, or any other device having wireless remote network connectivity). The nomadic device can then be used to communicate 59 with a network 61 outside the vehicle 31 through, for example, communication 55 with a cellular tower 57. In some embodiments, tower 57 may be a WiFi access point. Exemplary communication between the nomadic device and the BLUETOOTH transceiver is represented by signal 14. Pairing a nomadic device 53 and the BLUETOOTH transceiver 15 can be instructed through a button 52 or similar input. Accordingly, the CPU is instructed that the onboard BLUETOOTH transceiver will be paired with a BLUETOOTH transceiver in a nomadic device. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[10] 10. The method of claim 1, wherein the profile is configured for application in other vehicles.	Kleve expressly or inherently discloses “[t]he method of claim 1, wherein the profile is configured for application in other vehicles.” For example: Kleve at [0056] FIG. 4 shows an illustrative example of a communication system through which a wireless communication device can communicate with a vehicle 421 to enable a vehicle rental micro-business. In this illustrative embodiment, a nomadic device (e.g., without limitation, a cellular phone, a personal cellular telephone) 403 is used to send a communication through a cellular network 407. This communication is relayed through a network 411 (e.g., without limitation, the cellular network, the internet, etc.) to a centralized system 401. In another embodiment, the nomadic device 403 may send a communication through network 412 which may include, but is not limited to, WiFi or WiMax. This communication is relayed through a network 406 (e.g., without limitation, cloud computing, the internet,) to a centralized system 401.

Claims	Prior Art
	Kleve at [0060] The relay to the vehicle 421 is sent out from the server(s) 401 through a network (e.g., without limitation, a cellular network 113, the internet, etc.) and passed through a cellular network 415 to the vehicle 421. In another embodiment, the relay may be passed through network 414 (e.g., WiFi or WiMax) and to the vehicle 421. A remote communication module in the vehicle 421 receives the signal sent from the server(s) 401 and processes it or relays it to an appropriate processing system within the vehicle 421. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[11] 11. The method of claim 1, wherein the profile is activated on the vehicle when the user information, including biometrics data, is activated [verified].	Kleve expressly or inherently discloses “[t]he method of claim 1, wherein the profile is activated on the vehicle when the user information, including biometrics data, is activated” or, to the extent the claim is amended, Kleve expressly or inherently discloses “[t]he method of claim 1, wherein the profile is activated on the vehicle when the user information, including biometrics data, is verified.” For example: Kleve at [0049] The system may be further extended to facilitate the virtual key with additional security by requiring remote credential verification at the vehicle. The remote credential verification at the vehicle may be done with additional hardware assembled on the exterior of the vehicle or in the vehicle cabin. The remote credential verification may be done by the VCS, using a server, or allowing the Owner to verify the Temporary User's request. For example, but not limited to, the Temporary User entering a credential verification password at the vehicle's touchscreen visual display while having the VCS, server, or owner compare and verify authorization. Once the Temporary User has completed the rental period and returned the vehicle to the appropriate drop off, the virtual key may terminate allowing the system to reset any private information stored on the vehicle-based computing system. Kleve at [0063] Additional Temporary User identification 504 may be sent to the vehicle Owner allowing for this information to be entered into the server and used as a virtual key, or in addition to the virtual key, allowing the Temporary User access to the Owner's vehicle while enabling a keyless drive-away. The Temporary User identification and virtual key may be sent in an encrypted message to the VCS, Temporary User's nomadic device, and/or vehicle Owners nomadic device. The Temporary User's information for vehicle authorization credential verification 516 may include, but not limited to fingerprint recognition of user, photos of credit cards, photo of forms of ID, facial recognition, voice

Claims	Prior Art
	print recognition, matrix barcode (ex. two-dimensional code), code word or code phrase for speech recognition, temporary mobile web login IDs and password, or other types of unique Temporary User identification. Kleve at [0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of generating a virtual key may be done by using Temporary User's credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614. At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[14] 14. The method of claim 1, wherein the plurality of settings include one or more of tracking settings, or use metrics settings, or comfort settings, or entertainment settings, or driving mode settings, or refuel routing settings, or purchase settings, or combinations of two or more thereof.	Kleve expressly or inherently discloses “[t]he method of claim 1, wherein the plurality of settings include one or more of tracking settings, or use metrics settings, or comfort settings, or entertainment settings, or driving mode settings, or refuel routing settings, or purchase settings, or combinations of two or more thereof.” For example: Kleve at [0050] At 324, the Temporary User may have vehicle preset settings applied when renting a vehicle. These enhancements may include, but not limited to providing the Temporary User with stored frequent destinations sent to the VCS, radio presets, seat and mirror position, and ambient lighting preferences. The personalization of returning user's may also include a “bread crumb” feature allowing users to mark

Claims	Prior Art
	their usage to leave future users recommendations including which restaurant to eat at, or which routes to avoid. Kleve at [0072] At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings. Another exemplary example of setting personal preferences may include, but not limited to, facial recognition to recognize the driver using a camera mounted in the vehicle cabin on the dash. Once the camera recognizes the Temporary User, the VCS may request additional user settings and preferences including seat adjustment, and climate control temperatures. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[15] 15. The method of claim 1, wherein the profile stored in the storage is accessible via a device using a connection to the Internet and/or a vehicle interface of the vehicle, and the device is one of a portable device, or a computer.	Kleve expressly or inherently discloses “[t]he method of claim 1, wherein the profile stored in the storage is accessible via a device using a connection to the Internet and/or a vehicle interface of the vehicle, and the device is one of a portable device, or a computer.” For example: Kleve at [0030] In another embodiment, nomadic device 53 includes a modem for voice band or broadband data communication. In the data-over-voice embodiment, a technique known as frequency division multiplexing may be implemented when the owner of the nomadic device can talk over the device while data is being transferred. At other times, when the owner is not using the device, the data transfer can use the whole bandwidth (300 Hz to 3.4 kHz in one example). While frequency division multiplexing may be common for analog cellular communication between the vehicle and the internet, and is still used, it has been largely replaced by hybrids of Code Domain Multiple Access (CDMA), Time Domain Multiple Access (TDMA), Space-Domain Multiple Access (SDMA) for digital cellular communication. These are all ITU IMT-2000 (3G) compliant standards and offer data rates up to 2 mbs for stationary or walking users and 385 kbs for users in a moving vehicle. 3G standards are now being replaced by IMT-Advanced (4G) which offers 100 mbs for users in a vehicle and 1 gbs for stationary users. If the user has a data-plan associated with the nomadic device, it is possible that the data-plan allows for broad-band transmission and the system could use a much wider bandwidth (speeding up data transfer). In still another embodiment, nomadic device 53 is replaced with a cellular communication device (not shown) that is installed to vehicle 31. In yet another embodiment, the ND 53 may be a wireless local area network

Claims	Prior Art
	(LAN) device capable of communication over, for example (and without limitation), an 802.11g network (i.e., WiFi) or a WiMax network. Kleve at [0056] FIG. 4 shows an illustrative example of a communication system through which a wireless communication device can communicate with a vehicle 421 to enable a vehicle rental micro-business. In this illustrative embodiment, a nomadic device (e.g., without limitation, a cellular phone, a personal cellular telephone) 403 is used to send a communication through a cellular network 407. This communication is relayed through a network 411 (e.g., without limitation, the cellular network, the internet, etc.) to a centralized system 401. In another embodiment, the nomadic device 403 may send a communication through network 412 which may include, but is not limited to, WiFi or WiMax. This communication is relayed through a network 406 (e.g., without limitation, cloud computing, the internet,) to a centralized system 401. Kleve at [0082]-[0083] At step 804, the vehicle rental authorization system stores the owner's data. The data may be organized by the vehicle rental authorization system to allow potential Temporary Users to view vehicle information. Once a Temporary User has selected the owner's vehicle to rent, the vehicle rental authorization system may notify the owner of a rental request at step 806. At step 808, the vehicle owner may be able to review the temporary user's vehicle rental request. The owner may review the requested rental based on what the Temporary User is looking to use the vehicle for (e.g. without limitation, for towing, hauling, or errands), when the requested use will be taking place, and where. The owner may also review the Temporary Users profile and rental history, to see how they have ranked with past experiences using the vehicle rental authorization system at step 810. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[16] 16. The method of claim 1, wherein the user information includes one or more of sign-in credentials, or biometrics or face recognition data, or voice data, or fingerprint data, or eye-retina scan	Kleve expressly or inherently discloses “[t]he method of claim 1, wherein the user information includes one or more of sign-in credentials, or biometrics or face recognition data, or voice data, or fingerprint data, or eye-retina scan data, or a combination of two or more thereof.” For example: Kleve at [0049] The system may be further extended to facilitate the virtual key with additional security by requiring remote credential verification at the vehicle. The remote credential verification at the vehicle may be

Claims	Prior Art
data, or a combination of two or more thereof.	done with additional hardware assembled on the exterior of the vehicle or in the vehicle cabin. The remote credential verification may be done by the VCS, using a server, or allowing the Owner to verify the Temporary User's request. For example, but not limited to, the Temporary User entering a credential verification password at the vehicle's touchscreen visual display while having the VCS, server, or owner compare and verify authorization. Once the Temporary User has completed the rental period and returned the vehicle to the appropriate drop off, the virtual key may terminate allowing the system to reset any private information stored on the vehicle-based computing system. Kleve at [0063] Additional Temporary User identification 504 may be sent to the vehicle Owner allowing for this information to be entered into the server and used as a virtual key, or in addition to the virtual key, allowing the Temporary User access to the Owner's vehicle while enabling a keyless drive-away. The Temporary User identification and virtual key may be sent in an encrypted message to the VCS, Temporary User's nomadic device, and/or vehicle Owners nomadic device. The Temporary User's information for vehicle authorization credential verification 516 may include, but not limited to fingerprint recognition of user, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode (ex. two-dimensional code), code word or code phrase for speech recognition, temporary mobile web login IDs and password, or other types of unique Temporary User identification. Kleve at [0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of generating a virtual key may be done by using Temporary User's credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614. At step 616, the virtual key

Claims	Prior Art
	is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[17pre] 17. A cloud-based system including one or more data centers, and each data center of the cloud-based system includes one or more servers, wherein some of said one or more servers have program instructions for enabling connections with vehicles and providing services to vehicles, wherein one service includes enabling access to settings associated with profiles of user accounts of the cloud-based system, comprising:	To the extent the preamble is limiting, Kleve expressly or inherently discloses “[a] cloud-based system including one or more data centers, and each data center of the cloud-based system includes one or more servers, wherein some of said one or more servers have program instructions for enabling connections with vehicles and providing services to vehicles, wherein one service includes enabling access to settings associated with profiles of user accounts of the cloud-based system.” For example: Kleve at [0035] In addition to having exemplary processes executed by a vehicle computing system located in a vehicle, in certain embodiments, the exemplary processes may be executed by a computing system in communication with a vehicle computing system. Such a system may include, but is not limited to, a wireless device (e.g., and without limitation, a cellular telephone) or a remote computing system (e.g., and without limitation, a server) connected through the wireless device. Collectively, such systems may be referred to as vehicle associated computing systems (VACS). In certain embodiments particular components of the VACS may perform particular portions of a process depending on the particular implementation of the system. By way of example and not limitation, if a process has a step of sending or receiving information with a paired wireless device, then it is likely that the wireless device is not performing the process, since the wireless device would not “send and receive” information with itself. One of ordinary skill in the art will understand when it is inappropriate to apply a particular VACS to a given solution. In all solutions, it is contemplated that at least the vehicle computing system (VCS) located within the vehicle itself is capable of performing the exemplary processes. Kleve at [0057]–[0058] In this illustrative embodiment, the centralized system is a server system that includes processing capability for incoming nomadic device signals designated to interact with a remote vehicle 421. For example, the server(s) 401 may include an automated call server and/or web host. Further, the server(s) 401 may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to enable a Temporary User keyless access and drive away capabilities of the Owner's vehicle. Data sent in this fashion may be sent using data-over-voice, a data-plan, or in any other suitable format.

Claims	Prior Art
	Data can also be sent to the vehicle 421 through the server(s) 401 using a personal computer 405. In this case, the data is likely, although not necessarily, sent over the internet 409. Once the server(s) 401 receive the incoming data request from the remote source 403, 405, the message is processed and/or relayed to a vehicle 421 and the Temporary User's nomadic device 402. The vehicle may be identified by a header associated with one or more incoming data packets, or may be identifiable based on a database lookup, for example. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[17a] receiving, by one of the servers, a request from a vehicle to access a profile for a user account associated with a user, the request identifies user information related to a user;	Kleve expressly or inherently discloses “receiving, by one of the servers, a request from a vehicle to access a profile for a user account associated with a user, the request identifies user information related to a user.” For example: See above at row [1a]. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[17b] processing, by one of the servers, at least part of the user information to verify the access for the user, the profile having a plurality of settings of the user for the vehicle [and at least one of said plurality of settings being restricted for use on the vehicle, wherein] at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers; and	Kleve expressly or inherently discloses “processing, by one of the servers, at least part of the user information to verify the access for the user, the profile having a plurality of settings of the user for the vehicle at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers” or, to the extent the claim is amended, Kleve expressly or inherently discloses “processing, by one of the servers, at least part of the user information to verify the access for the user, the profile having a plurality of settings of the user for the vehicle and at least one of said plurality of settings being restricted for use on the vehicle, wherein at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers.” For example: Kleve at [0063] Additional Temporary User identification 504 may be sent to the vehicle Owner allowing for this information to be entered into the server and used as a virtual key, or in addition to the virtual key, allowing the Temporary User access to the Owner's vehicle while enabling a keyless drive-away. The Temporary User identification and virtual key may be sent in an encrypted message to the VCS, Temporary User's nomadic device, and/or vehicle Owners nomadic device. The Temporary User's information for vehicle authorization credential verification 516 may include, but not limited to

Claims	Prior Art
	fingerprint recognition of user, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode (ex. two-dimensional code), code word or code phrase for speech recognition, temporary mobile web login IDs and password, or other types of unique Temporary User identification. Kleve at [0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of generating a virtual key may be done by using Temporary User's credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614. At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[17c] transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to [storage of] the vehicle, the transferring is configured to instruct software and hardware associated the vehicle to enable said one or more settings for use	Kleve expressly or inherently discloses “transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to the vehicle, the transferring is configured to instruct software and hardware associated the vehicle to enable said one or more settings for use on the vehicle to customize said vehicle for the user, the request and the transferring being via wireless communication of said vehicle” or, to the extent the claim is amended, Kleve expressly or inherently discloses “transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to storage of the vehicle, the transferring is configured to instruct software and hardware associated the vehicle to enable said one or more settings for use on the vehicle to customize said

Claims	Prior Art
on the vehicle to customize said vehicle for the user, the request and the transferring being via wireless communication of said vehicle.	vehicle for the user, the request and the transferring being via wireless communication of said vehicle.” For example: Kleve at [0056] FIG. 4 shows an illustrative example of a communication system through which a wireless communication device can communicate with a vehicle 421 to enable a vehicle rental micro-business. In this illustrative embodiment, a nomadic device (e.g., without limitation, a cellular phone, a personal cellular telephone) 403 is used to send a communication through a cellular network 407. This communication is relayed through a network 411 (e.g., without limitation, the cellular network, the internet, etc.) to a centralized system 401. In another embodiment, the nomadic device 403 may send a communication through network 412 which may include, but is not limited to, WiFi or WiMax. This communication is relayed through a network 406 (e.g., without limitation, cloud computing, the internet,) to a centralized system 401. Kleve at [0057]–[0058] In this illustrative embodiment, the centralized system is a server system that includes processing capability for incoming nomadic device signals designated to interact with a remote vehicle 421. For example, the server(s) 401 may include an automated call server and/or web host. Further, the server(s) 401 may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to enable a Temporary User keyless access and drive away capabilities of the Owner's vehicle. Data sent in this fashion may be sent using data-over-voice, a data-plan, or in any other suitable format. Data can also be sent to the vehicle 421 through the server(s) 401 using a personal computer 405. In this case, the data is likely, although not necessarily, sent over the internet 409. Once the server(s) 401 receive the incoming data request from the remote source 403, 405, the message is processed and/or relayed to a vehicle 421 and the Temporary User's nomadic device 402. The vehicle may be identified by a header associated with one or more incoming data packets, or may be identifiable based on a database lookup, for example. Kleve at [0060] The relay to the vehicle 421 is sent out from the server(s) 401 through a network (e.g., without limitation, a cellular network 113, the internet, etc.) and passed through a cellular network 415 to the vehicle 421. In another embodiment, the relay may be passed through network 414 (e.g., WiFi or WiMax) and to the vehicle 421. A remote communication module in the vehicle 421 receives the signal sent from the server(s) 401 and processes it or relays it to an appropriate processing system within the vehicle 421.

Claims	Prior Art
	Kleve at [0061] In at least one illustrative embodiment, the vehicle 421 is also outfitted with a communication transceiver, such as, but not limited to, a BLUETOOTH transceiver. This transceiver may allow communication with the nomadic device 403 using a direct signal 419. This transceiver may also allow communication with the Temporary User's nomadic device 402 to the vehicle 421 using a wireless connection 420 including, but not limited to, a smart phone that may connect to the vehicle through SYNC or other Bluetooth pairing device. It should be understood that the communication between nomadic device 403, temporary user nomadic device 402, server 401, and vehicle 421 may be performed in a number of ways and FIG. 4 is presented for illustrative purposes. FIG. 4 illustrates various alternatives for communicating data. For example, and without limitation, data communication may be partially or entirely cellular or WiFi, or a combination of cellular and WiFi. Kleve at [0072] At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings. Another exemplary example of setting personal preferences may include, but not limited to, facial recognition to recognize the driver using a camera mounted in the vehicle cabin on the dash. Once the camera recognizes the Temporary User, the VCS may request additional user settings and preferences including seat adjustment, and climate control temperatures. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[18] 18. The cloud-based system of claim 17, wherein the profile is transferrable to one or more other vehicles.	Kleve expressly or inherently discloses “[t]he cloud-based system of claim 17, wherein the profile is transferrable to one or more other vehicles.” For example: Kleve at [0057]–[0058] In this illustrative embodiment, the centralized system is a server system that includes processing capability for incoming nomadic device signals designated to interact with a remote vehicle 421. For example, the server(s) 401 may include an automated call server and/or web host. Further, the server(s) 401 may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to enable a Temporary User keyless access and drive away capabilities of the Owner's vehicle. Data sent in this fashion may be sent using data-over-voice, a data-plan, or in any other suitable format.

Claims	Prior Art
	Data can also be sent to the vehicle 421 through the server(s) 401 using a personal computer 405. In this case, the data is likely, although not necessarily, sent over the internet 409. Once the server(s) 401 receive the incoming data request from the remote source 403, 405, the message is processed and/or relayed to a vehicle 421 and the Temporary User's nomadic device 402. The vehicle may be identified by a header associated with one or more incoming data packets, or may be identifiable based on a database lookup, for example. Kleve at [0060] The relay to the vehicle 421 is sent out from the server(s) 401 through a network (e.g., without limitation, a cellular network 113, the internet, etc.) and passed through a cellular network 415 to the vehicle 421. In another embodiment, the relay may be passed through network 414 (e.g., WiFi or WiMax) and to the vehicle 421. A remote communication module in the vehicle 421 receives the signal sent from the server(s) 401 and processes it or relays it to an appropriate processing system within the vehicle 421. Kleve at [0061] In at least one illustrative embodiment, the vehicle 421 is also outfitted with a communication transceiver, such as, but not limited to, a BLUETOOTH transceiver. This transceiver may allow communication with the nomadic device 403 using a direct signal 419. This transceiver may also allow communication with the Temporary User's nomadic device 402 to the vehicle 421 using a wireless connection 420 including, but not limited to, a smart phone that may connect to the vehicle through SYNC or other Bluetooth pairing device. It should be understood that the communication between nomadic device 403, temporary user nomadic device 402, server 401, and vehicle 421 may be performed in a number of ways and FIG. 4 is presented for illustrative purposes. FIG. 4 illustrates various alternatives for communicating data. For example, and without limitation, data communication may be partially or entirely cellular or WiFi, or a combination of cellular and WiFi. Kleve at [0072] At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings. Another exemplary example of setting personal preferences may include, but not limited to, facial recognition to recognize the driver using a camera mounted in the vehicle cabin on the dash. Once the camera recognizes the Temporary User, the VCS may request additional user settings and preferences including seat adjustment, and climate control temperatures.

Claims	Prior Art
	To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[19] 19. The cloud-based system of claim 17, wherein the vehicle is configured to use the one or more settings for the vehicle while the profile is active in the vehicle, and said one or more settings are removed when the profile is no longer active in the vehicle, and wherein the request is processed automatically by the vehicle upon a pairing of a user device or input by the user of credentials.	Kleve expressly or inherently discloses “[t]he cloud-based system of claim 17, wherein the vehicle is configured to use the one or more settings for the vehicle while the profile is active in the vehicle, and said one or more settings are removed when the profile is no longer active in the vehicle, and wherein the request is processed automatically by the vehicle upon a pairing of a user device or input by the user of credentials.” For example: Kleve at [0039] At step 210, once the Temporary User selects the vehicle, pays the appropriate amount and signs a consent agreement, than the system may generate a virtual key to distribute to the Temporary User and VCS. The virtual key may be sent to, but not limited to, the website for the Temporary User to view, sent through an email, or to the Temporary User's nomadic device at step 212. The virtual key may also be sent to the vehicle configuring the VCS to enable the keyless drive system for the appropriate Temporary User during a given rental period. Kleve at [0044] Another exemplary example of the vehicle rental micro-business system may include other enhancements including, but not limited to, matrix barcode (ex. two-dimensional code) used as the virtual key being recognized by the VCS. The smart phone may be used to communicate the matrix barcode information to the vehicle rental micro-business system directly. The system may be able to communicate information from the smart phone to the vehicle notifying the VCS of a virtual key. Once the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive away event. Kleve at [0054]-[0055] At 330, the VCS may continue to monitor the vehicle for the entire rental period. If the rental period is soon to expire the system may notify Temporary User at step 338. If the Temporary User has not returned the vehicle at the time the rental period has expired, the system may notify the user if a rental term extension is desired at step 342. If the extension term is desired, the Temporary User may be prompted to accept additional rental charges at step 344. The Temporary User may be charged for the additional rental time at step 346. If the extension of time is not desired, and/or not allowed by the Owner, the system may transmit controlling action to warn and induce remedial actions at step 350. If the

Claims	Prior Art
	extension of time is not desired, and the Temporary User is within the allocated time and distance to return the vehicle to the required parking location at step 348. If the Temporary User has returned to the required parking spot, the system may begin to prepare for return to the vehicle Owner. During the preparation to return vehicle to Owner and end the rental period, the system may save any enhancements information based on the Temporary User's settings at step 352. At step 354, once the Temporary User has completed the rental period and returned the vehicle to the appropriate drop off, the virtual key may terminate. Once the virtual key has terminated, the system may reset any private information stored on the vehicle-based computing system by the Temporary User at step 356. The Temporary User may collect pictures to report status of the vehicle to the Owner after the rental period has ended at step 358. The system may include a standardized report form that requires certain information the Temporary User must fill out when returning the vehicle, including pictures. After the rental experience, the Owner and Temporary User may rate their experience on the website to notify others of their satisfaction each person had during the transaction at step 360. Kleve at [0068] At step 510, the vehicle may verify the Temporary User's virtual key by communicating with the server to compare the credential and verify Temporary User's access. The vehicle using the wireless device to transmit confirmation back to the vehicle Owner 512 through a telecommunications network notifying that the Temporary User entered the vehicle and has commenced the vehicle rental agreement. Once the rental period has expired the virtual key may be reset and cleared from the VCS. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[20pre] 20. The cloud-based system of claim 17,	Kleve expressly or inherently discloses “[t]he cloud-based system of claim 17.” See above.
[20a] wherein one or more of the settings are associated with systems of the vehicle, and the systems of the vehicle are configured to receive input or cause one or more actions or functions,	To the extent the preamble is limiting, Kleve expressly or inherently discloses “wherein one or more of the settings are associated with systems of the vehicle, and the systems of the vehicle are configured to receive input or cause one or more actions or functions.” For example: Kleve at [0050] At 324, the Temporary User may have vehicle preset settings applied when renting a vehicle. These enhancements may include, but not limited to providing the Temporary User with stored frequent destinations sent to the VCS, radio presets, seat and mirror position, and ambient lighting preferences.

Claims	Prior Art
	The personalization of returning user's may also include a “bread crumb” feature allowing users to mark their usage to leave future users recommendations including which restaurant to eat at, or which routes to avoid. Kleve at [0072] At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings. Another exemplary example of setting personal preferences may include, but not limited to, facial recognition to recognize the driver using a camera mounted in the vehicle cabin on the dash. Once the camera recognizes the Temporary User, the VCS may request additional user settings and preferences including seat adjustment, and climate control temperatures. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[20b] wherein the systems include one or more of a door lock, a heating and cooling system, a speaker, an engine start/shut switch, a user interface, a button, a lever, a key, a graphical user interface (GUI), an electronic component of the vehicle, a telecommunications system, a remote face-to-face conferencing system, a mapping function system, a GPS system, a fingerprint scanner, a touch screen, a navigation system, a wireless communication system, a data encryption system, WiFi logic, Bluetooth logic, NFC logic, a microprocessor, a memory system, a camera, application programming interfaces (APIs) for	To the extent the preamble is limiting, Kleve expressly or inherently discloses “wherein the systems include one or more of a door lock, a heating and cooling system, a speaker, an engine start/shut switch, a user interface, a button, a lever, a key, a graphical user interface (GUI), an electronic component of the vehicle, a telecommunications system, a remote face-to-face conferencing system, a mapping function system, a GPS system, a fingerprint scanner, a touch screen, a navigation system, a wireless communication system, a data encryption system, WiFi logic, Bluetooth logic, NFC logic, a microprocessor, a memory system, a camera, application programming interfaces (APIs) for vehicle systems, kernel level systems, function invoking systems, temperature detection systems, HVAC APIs, display screens, data network logic, mechanical systems, electrical systems, physical mechanical and electrical systems, seat mechanical systems, mirror systems, alarm systems, battery systems, battery, lighting systems, an application shared by mobile a device present and paired with the vehicle for providing at least one interface in a display screen of the vehicle, or vehicle electronics system.” For example: Kleve at [0050] At 324, the Temporary User may have vehicle preset settings applied when renting a vehicle. These enhancements may include, but not limited to providing the Temporary User with stored frequent destinations sent to the VCS, radio presets, seat and mirror position, and ambient lighting preferences. The personalization of returning user's may also include a “bread crumb” feature allowing users to mark their usage to leave future users recommendations including which restaurant to eat at, or which routes to avoid.

Claims	Prior Art
vehicle systems, kernel level systems, function invoking systems, temperature detection systems, HVAC APIs, display screens, data network logic, mechanical systems, electrical systems, physical mechanical and electrical systems, seat mechanical systems, mirror systems, alarm systems, battery systems, battery, lighting systems, an application shared by mobile a device present and paired with the vehicle for providing at least one interface in a display screen of the vehicle, or vehicle electronics system.	Kleve at [0072] At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings. Another exemplary example of setting personal preferences may include, but not limited to, facial recognition to recognize the driver using a camera mounted in the vehicle cabin on the dash. Once the camera recognizes the Temporary User, the VCS may request additional user settings and preferences including seat adjustment, and climate control temperatures. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[21pre] 21. A cloud-based system including one or more data centers, and each data center of the cloud-based system includes one or more servers, wherein some of said one or more servers have program instructions for enabling connections with vehicles and providing services to vehicles, wherein one service includes enabling access to settings associated with profiles of user accounts of the cloud-based system, comprising:	To the extent the patent is amended to include claim 21, Kleve discloses it. To the extent the preamble is limiting, Kleve expressly or inherently discloses “[a] cloud-based system including one or more data centers, and each data center of the cloud-based system includes one or more servers, wherein some of said one or more servers have program instructions for enabling connections with vehicles and providing services to vehicles, wherein one service includes enabling access to settings associated with profiles of user accounts of the cloud-based system.” For example: See above at row [17pre]. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[21a] receiving, by one of the servers, a request from a vehicle to access a profile for a user account associated with a user, the request	Kleve expressly or inherently discloses “receiving, by one of the servers, a request from a vehicle to access a profile for a user account associated with a user, the request identifies user information related to a user.” For example:

Claims	Prior Art
identifies user information related to a user;	See above at row [1a]. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[21b] processing, by one of the servers, at least part of the user information to verify the access for the user, the profile having a plurality of settings of the user for the vehicle, wherein at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers; and	Kleve expressly or inherently discloses “processing, by one of the servers, at least part of the user information to verify the access for the user, the profile having a plurality of settings of the user for the vehicle, wherein at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers.” For example: Kleve at [0059] In one embodiment, a message is relayed to the remote source 403, 405 as well. For example, as will be described in further detail below, when an authorized temporary user remotely transmits a request from a Temporary User's nomadic device 402 (e.g., via a button or key press) to receive authorization to operate and drive away the vehicle 421, the server(s) 401 may respond by transmitting an authorization code to both the Temporary User's nomadic device 402 and to the vehicle control system for input by the authorized Temporary User at the vehicle 421. An authorized temporary user may be any individual recognized by the vehicle 421 as an authorized user based on a matrix barcode, a fingerprint scan, an authorized code typed in a touchscreen, voice recognition, and the like. It should be understood that these examples are non-limiting and other means of authorization for the vehicle rental micro-business may be used. Kleve at [0063] Additional Temporary User identification 504 may be sent to the vehicle Owner allowing for this information to be entered into the server and used as a virtual key, or in addition to the virtual key, allowing the Temporary User access to the Owner's vehicle while enabling a keyless drive-away. The Temporary User identification and virtual key may be sent in an encrypted message to the VCS, Temporary User's nomadic device, and/or vehicle Owners nomadic device. The Temporary User's information for vehicle authorization credential verification 516 may include, but not limited to fingerprint recognition of user, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode (ex. two-dimensional code), code word or code phrase for speech recognition, temporary mobile web login IDs and password, or other types of unique Temporary User identification.

Claims	Prior Art
	Kleve at [0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of generating a virtual key may be done by using Temporary User's credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614. At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[21c] transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to storage of the vehicle, the transferring is configured to instruct software and hardware associated the vehicle to enable said one or more settings for use on the vehicle to customize said vehicle for the user, the request and the transferring being via	Kleve expressly or inherently discloses “transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to storage of the vehicle, the transferring is configured to instruct software and hardware associated the vehicle to enable said one or more settings for use on the vehicle to customize said vehicle for the user, the request and the transferring being via wireless communication of said vehicle.” For example: See above at row [17c]. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.

Claims	Prior Art
wireless communication of said vehicle;	
[21d] wherein a learning engine executed by a server of at least one data center is configured to process inputs made to one or more settings of the vehicle by the user to generate a recommended setting to add to the plurality of settings of the profile;	Kleve expressly or inherently discloses “wherein a learning engine executed by a server of at least one data center is configured to process inputs made to one or more settings of the vehicle by the user to generate a recommended setting to add to the plurality of settings of the profile.” For example: Kleve at [0050] At 324, the Temporary User may have vehicle preset settings applied when renting a vehicle. These enhancements may include, but not limited to providing the Temporary User with stored frequent destinations sent to the VCS, radio presets, seat and mirror position, and ambient lighting preferences. The personalization of returning user's may also include a “bread crumb” feature allowing users to mark their usage to leave future users recommendations including which restaurant to eat at, or which routes to avoid. To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[21e] wherein accepted recommendations are saved to the profile and added to the cloud storage that is accessible to said one or more servers.	Kleve expressly or inherently discloses “wherein accepted recommendations are saved to the profile and added to the cloud storage that is accessible to said one or more servers.” For example: To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[22] 22. The cloud-based system of claim 21, wherein the profile is transferrable to one or more other vehicles, and wherein being transferrable enables syncing of said profile by uploading and downloading the profile from the server and saving it to storage of the one or more other vehicles for use of said plurality of settings.	To the extent the patent is amended to include claim 22, Kleve discloses it. Kleve expressly or inherently discloses “[t]he cloud-based system of claim 21, wherein the profile is transferrable to one or more other vehicles, and wherein being transferrable enables syncing of said profile by uploading and downloading the profile from the server and saving it to storage of the one or more other vehicles for use of said plurality of settings.” For example: Kleve at [0057]–[0058] In this illustrative embodiment, the centralized system is a server system that includes processing capability for incoming nomadic device signals designated to interact with a remote vehicle 421. For example, the server(s) 401 may include an automated call server and/or web host. Further, the server(s) 401 may route an incoming signal from a nomadic device (ND) 403 to the appropriate remote vehicle to

Claims	Prior Art
	enable a Temporary User keyless access and drive away capabilities of the Owner's vehicle. Data sent in this fashion may be sent using data-over-voice, a data-plan, or in any other suitable format. Data can also be sent to the vehicle 421 through the server(s) 401 using a personal computer 405. In this case, the data is likely, although not necessarily, sent over the internet 409. Once the server(s) 401 receive the incoming data request from the remote source 403, 405, the message is processed and/or relayed to a vehicle 421 and the Temporary User's nomadic device 402. The vehicle may be identified by a header associated with one or more incoming data packets, or may be identifiable based on a database lookup, for example. Kleve at [0060] The relay to the vehicle 421 is sent out from the server(s) 401 through a network (e.g., without limitation, a cellular network 113, the internet, etc.) and passed through a cellular network 415 to the vehicle 421. In another embodiment, the relay may be passed through network 414 (e.g., WiFi or WiMax) and to the vehicle 421. A remote communication module in the vehicle 421 receives the signal sent from the server(s) 401 and processes it or relays it to an appropriate processing system within the vehicle 421. Kleve at [0061] In at least one illustrative embodiment, the vehicle 421 is also outfitted with a communication transceiver, such as, but not limited to, a BLUETOOTH transceiver. This transceiver may allow communication with the nomadic device 403 using a direct signal 419. This transceiver may also allow communication with the Temporary User's nomadic device 402 to the vehicle 421 using a wireless connection 420 including, but not limited to, a smart phone that may connect to the vehicle through SYNC or other Bluetooth pairing device. It should be understood that the communication between nomadic device 403, temporary user nomadic device 402, server 401, and vehicle 421 may be performed in a number of ways and FIG. 4 is presented for illustrative purposes. FIG. 4 illustrates various alternatives for communicating data. For example, and without limitation, data communication may be partially or entirely cellular or WiFi, or a combination of cellular and WiFi. Kleve at [0072] At step 624, the Temporary User's nomadic device may be paired with the VCS and may send personal settings to the vehicle including, but not limited to, radio station presets, navigation routes, and/or preferred climate control settings. Another exemplary example of setting personal preferences may include, but not limited to, facial recognition to recognize the driver using a camera mounted in the vehicle cabin on the dash. Once the camera recognizes the Temporary User, the VCS may request additional user settings and preferences including seat adjustment, and climate control temperatures.

Claims	Prior Art
	To the extent that Kleve was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Kleve with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.

Appendix E-6: Invalidity of the '244 Patent in view of Rector

US20110137520A1 (“Rector”), alone or in combination with other prior art identified in the cover pleading, anticipates and/or renders obvious all of the claims at issue. Nothing in this chart should be construed as an admission of infringement.

As described herein, claims of the '244 Patent are expressly or inherently anticipated by Rector. In addition, to the extent that Rector is found not to anticipate one or more of the asserted claims of the '244 Patent, those claims are invalid as obvious in view of Rector alone, in combination with the knowledge of one of ordinary skill in the art, and/or other prior art, including but not limited to the prior art identified in the Exhibits E claim charts. With respect to the proposed modifications to Rector, such modification would have been obvious to try, an obvious combination of prior art elements according to known methods to yield predictable results, a simple substitution of one known element for another to obtain predictable results, a use of known techniques to improve a similar devices or method in the same way, an application of a known technique to a known device or method ready for improvement to yield predictable results, a variation of a known work in one field of endeavor for use in either the same field or a different one based on design incentives or other market forces with variations that are predictable to one of ordinary skill in the art, and/or obvious in view of teachings, suggestions, and motivations in the prior art that would have led one of ordinary skill to modify or combine the prior art references.

The charts below demonstrate how, at least under EA’s apparent infringement theory, each of the asserted claims is anticipated by Rector or is obvious over Rector in further of the knowledge of a POSITA and/or one or more prior art references.

The claim chart below is meant to illustrate how the materials identified above invalidates the asserted claims. By not discussing other portions of the materials below, Defendants do not waive their right to rely on other portions of the materials; instead, Defendants expressly reserve their right to rely on other portions of the materials. These contentions are not an admission by Defendants that any accused products, including any past or current version of these products, are covered by or infringe Plaintiffs’ asserted claims, particularly once the claims are construed by the Court, and do not constitute an admission by Defendants as to the proper construction of any asserted claim and citations may be based on Plaintiffs’ apparent construction of the claims. Defendants does not agree with EA’s application of the claims, or that the claims satisfy 35 U.S.C. § 112. These contentions are not an admission by Defendants as to the proper scope of any asserted claim or the proper construction of any asserted claim. Defendant’s initial patent disclosures are made in a variety of alternatives and do not represent Defendant’s agreement or view as to the meaning, definiteness, written description support for, or enablement of any claim contained therein. Defendants reserve the right to modify, amend, or supplement these contentions as additional information becomes available during the course of this action and in view of any applicable claim construction order that the Court is anticipated to issue.

Claims	Prior Art
[1pre] 1. A method executed by a server of a cloud services system that is configured to interface with vehicles, comprising:	To the extent the preamble is limiting, Rector expressly or inherently discloses “[a] method executed by a server of a cloud services system that is configured to interface with vehicles.” For example: Rector at 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

Claims	Prior Art
	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. Reflector at Fig. 1 Figure 1

Rector at Fig. 3

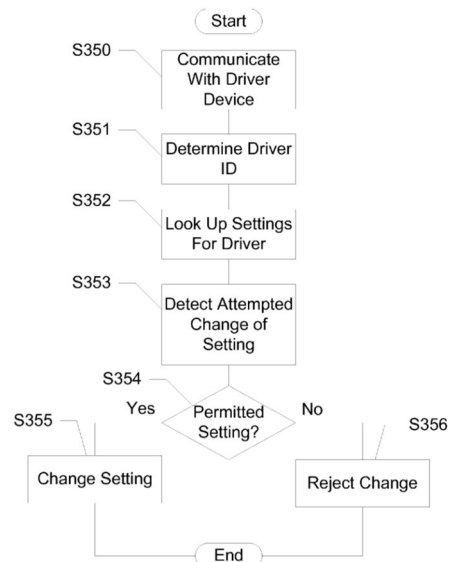


Figure 3

Rector at Title

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

Rector at [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.

Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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.

Rector at [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.

Rector at [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.

Rector at [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 S350. 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

Claims	Prior Art
	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 S351. 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 S352. 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 S353. 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 S354. 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 S355. 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 S356. 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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[1a] receiving, by the server, a request from electronics of a vehicle to access a profile for a user account, the request identifies user information for a user to use the vehicle;	Rector expressly or inherently discloses “receiving, by the server, a request from electronics of a vehicle to access a profile for a user account, the request identifies user information for a user to use the vehicle.” For example: Rector at 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

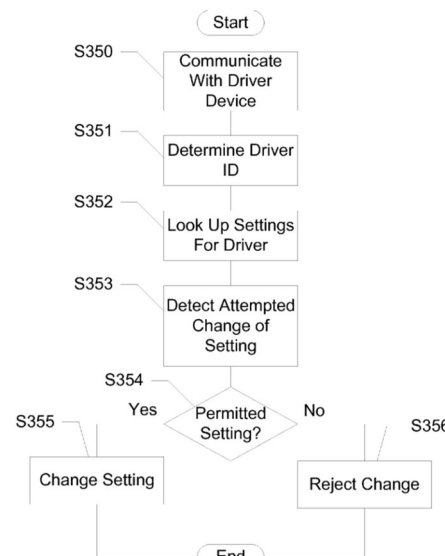
Claims	Prior Art
	reference a database to determine the identity of the driver as well as settings for the driver created by a controlling authority. The controlling authority may be, for instance, a parent or employer of the driver. The settings may limit certain devices within the vehicle and/or the 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. Rector at [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. Rector at [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. Rector at [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

Claims	Prior Art
	more of permitted speed settings, permitted radio settings, and permitted use of the wireless communication device. Rector at [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. Rector at [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. Rector at [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

Claims	Prior Art
	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. 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. Rector at [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 S350. 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 S351. 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 S352. 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 S353. 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 S354. 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 S355. For

Claims	Prior Art
	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 S356. 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. Rector at [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. Rector at [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. Rector at [0056] FIGS. 8A and 8B 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.

Claims	Prior Art
	Rector at [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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[1b] processing, by the server, at least part of the user information to verify the user for accessing the profile associated with the user account, the profile having a plurality of settings of the user for the vehicle [and at least one of said plurality of settings being restricted for use on the vehicle, wherein] at least part of the plurality of settings for the profile being stored on storage accessible to the cloud services system; and	Rector expressly or inherently discloses “processing, by the server, at least part of the user information to verify the user for accessing the profile associated with the user account, the profile having a plurality of settings of the user for the vehicle, wherein at least part of the plurality of settings for the profile being stored on storage accessible to the cloud services system” or, to the extent the claim is amended, Rector expressly or inherently discloses “processing, by the server, at least part of the user information to verify the user for accessing the profile associated with the user account, the profile having a plurality of settings of the user for the vehicle and at least one of said plurality of settings being restricted for use on the vehicle, wherein at least part of the plurality of settings for the profile being stored on storage accessible to the cloud services system.” For example: Rector at 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

Claims	Prior Art
	distractions to the driver. Further, the settings may be influenced by the number or identities of passengers within the vehicle. Reactor at Fig. 3  <pre> graph TD Start([Start]) --> S350[S350: Communicate With Driver Device] S350 --> S351[S351: Determine Driver ID] S351 --> S352[S352: Look Up Settings For Driver] S352 --> S353[S353: Detect Attempted Change of Setting] S353 --> S354{S354: Permitted Setting?} S354 -- Yes --> S355[S355: Change Setting] S354 -- No --> S356[S356: Reject Change] S355 --> End([End]) S356 --> End </pre> Figure 3

Rector at Fig. 11

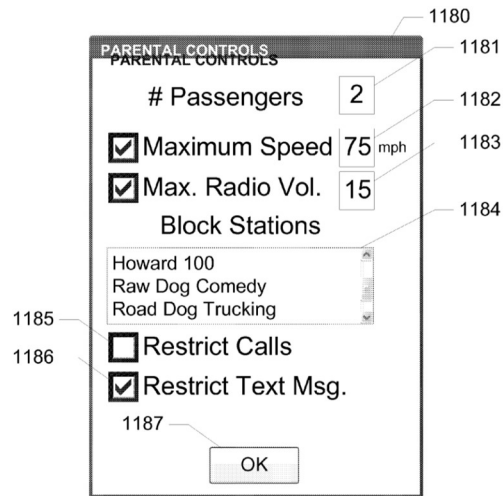


Figure 11

Rector at Title

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

Rector at [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.

Rector at [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.

Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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

Claims	Prior Art
	distractions to the driver. Further, the settings may be influenced by the number or identities of passengers within the vehicle. Rector at [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. Rector at [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. Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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.

Rector at [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.

Rector at [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.

Rector at [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.

Rector at [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 S350. 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

Claims	Prior Art
	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 S351. 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 S352. 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 S353. 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 S354. 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 S355. 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 S356. 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. Rector at [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.

Rector at [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.

Rector at [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.

Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[1c] transferring, by the server, upon verifying the user information, one or more settings of the plurality of settings to [storage of] the vehicle,	Rector expressly or inherently discloses “transferring, by the server, upon verifying the user information, one or more settings of the plurality of settings to the vehicle” or, to the extent the claim is amended, Rector expressly or inherently discloses “transferring, by the server, upon verifying the user information, one or more settings of the plurality of settings to storage of the vehicle.” For example: Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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 S350. 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 S351. 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 S352. 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 S353. 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 S354. 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 S355. 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 S356. 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.

Rector at [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.

Rector at [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.

Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[1d] the transferring is configured to instruct software and/or hardware associated with said electronics of the vehicle to apply said one or more settings to the vehicle for customizing said vehicle to use said one or more	Rector expressly or inherently discloses “the transferring is configured to instruct software and/or hardware associated with said electronics of the vehicle to apply said one or more settings to the vehicle for customizing said vehicle to use said one or more settings associated with the profile.” For example: Rector at [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,

Claims	Prior Art
settings associated with the profile,	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. Rector at [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. Rector at [0010]–[0011] 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. 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.

Rector at [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.

Rector at [0031]–[0034]

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.

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.

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

Claims	Prior Art
	employer may set a maximum volume level for employees in the settings for each employee, for the smart vehicle, for certain times, etc. 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. Rector at [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. Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[1e] wherein the vehicle uses wireless communication for exchanging data with the cloud services system and for receiving said one or more settings for the profile.	Rector expressly or inherently discloses “wherein the vehicle uses wireless communication for exchanging data with the cloud services system and for receiving said one or more settings for the profile.” For example: Rector at [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.

Rector at [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.

Rector at [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.

Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at claim 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.

Claims	Prior Art
	To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[2] 2. The method of claim 1, wherein the profile of the user is transferrable to one or more other vehicles from the cloud services system.	Rector expressly or inherently discloses “[t]he method of claim 1, wherein the profile of the user is transferrable to one or more other vehicles from the cloud services system.” For example: Rector at [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. Rector at [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. Rector at [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

Claims	Prior Art
	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. Rector at [0028] A “vehicle,” as used herein and throughout this disclosure, includes cars, trucks, and buses, as well as aircrafts and watercrafts. Rector at [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. Rector at [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 S350. 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 S351. 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 S352. 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

Claims	Prior Art
	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 S353. 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 S354. 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 S355. 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 S356. 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. Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[4] 4. The method of claim 1, further comprising, receiving, by the server, communication from the vehicle regarding inputs made to systems of the vehicle during use of the vehicle while the vehicle is associated with the profile of the user account; determining, by the server, based on the inputs made to systems of the vehicle that at least one of the plurality of settings of the profile is to be updated.	Rector expressly or inherently discloses “[t]he method of claim 1, further comprising, receiving, by the server, communication from the vehicle regarding inputs made to systems of the vehicle during use of the vehicle while the vehicle is associated with the profile of the user account; determining, by the server, based on the inputs made to systems of the vehicle that at least one of the plurality of settings of the profile is to be updated.” For example: To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[5] 5. The method of claim 4, further comprising, processing by a learning engine that uses the inputs made to the systems of the vehicle to find patterns in use of the systems of the vehicle while the profile was used with the vehicle.	Rector expressly or inherently discloses “[t]he method of claim 4, further comprising, processing by a learning engine that uses the inputs made to the systems of the vehicle to find patterns in use of the systems of the vehicle while the profile was used with the vehicle.” For example: Rector at [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.

Claims	Prior Art
	To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[6] 6. The method of claim 5, further comprising, sending, by the server, a recommended setting to the user account, the recommended setting is based on processing by the learning engine and said recommended setting is applied to the vehicle when the vehicle is used with the profile or is applied to the vehicle upon receiving acceptance of the recommended setting via the user account.	Rector expressly or inherently discloses “[t]he method of claim 5, further comprising, sending, by the server, a recommended setting to the user account, the recommended setting is based on processing by the learning engine and said recommended setting is applied to the vehicle when the vehicle is used with the profile or is applied to the vehicle upon receiving acceptance of the recommended setting via the user account.” For example: Rector at [0036]-[0038] 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. 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. 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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.

Claims	Prior Art
[7] 7. The method of claim 5, wherein the patterns are correlated to one or more conditions, the one or more conditions include type of input, or time of day inputs, or temperature, or security, or number of occupants in the vehicle, or weather, or age of the vehicle, or service requirements of the vehicle.	Rector expressly or inherently discloses “[t]he method of claim 5, wherein the patterns are correlated to one or more conditions, the one or more conditions include type of input, or time of day inputs, or temperature, or security, or number of occupants in the vehicle, or weather, or age of the vehicle, or service requirements of the vehicle.” For example: Rector at 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. Rector at [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. Rector at [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.

Claims	Prior Art
	Rector at [0051] 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. Rector at [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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[8] 8. The method of claim 1, further comprising, accessing, by the server, a plurality of profiles of different users stored in the storage accessible to the cloud services system; detecting, by the server, similarities in patterns for inputs made to systems of vehicles associated with the profiles of different users; using, by the server, a learning engine to produce a recommended setting that is sent to the user account.	Rector expressly or inherently discloses “[t]he method of claim 1, further comprising, accessing, by the server, a plurality of profiles of different users stored in the storage accessible to the cloud services system; detecting, by the server, similarities in patterns for inputs made to systems of vehicles associated with the profiles of different users; using, by the server, a learning engine to produce a recommended setting that is sent to the user account.” For example: Rector at [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.

Claims	Prior Art
	To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[9] 9. The method of claim 1, wherein the request is automatically generated by the electronics of the vehicle upon detecting a pairing with a user device of the user, or input of credentials of the user for the user account.	Rector expressly or inherently discloses “[t]he method of claim 1, wherein the request is automatically generated by the electronics of the vehicle upon detecting a pairing with a user device of the user, or input of credentials of the user for the user account.” For example: Rector at [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. Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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 S350. 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

Claims	Prior Art
	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 S351. 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 S352. 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 S353. 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 S354. 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 S355. 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 S356. 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. Rector at [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. Rector at [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

Claims	Prior Art
	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. Rector at [0056] FIGS. 8A and 8B 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. Rector at [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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.

Claims	Prior Art
[10] 10. The method of claim 1, wherein the profile is configured for application in other vehicles.	Rector expressly or inherently discloses “[t]he method of claim 1, wherein the profile is configured for application in other vehicles.” For example: Rector at [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. Rector at [0010]–[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. Rector at [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. Rector at [0028] A “vehicle,” as used herein and throughout this disclosure, includes cars, trucks, and buses, as well as aircrafts and watercrafts.

Rector at [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 S350. 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 S351. 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 S352. 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 S353. 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 S354. 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 S355. 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 S356. 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.

Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[11] 11. The method of claim 1, wherein the profile is activated on the vehicle when the user information, including biometrics data, is activated [verified].	Rector expressly or inherently discloses “[t]he method of claim 1, wherein the profile is activated on the vehicle when the user information, including biometrics data, is activated” or, to the extent the claim is amended, Rector expressly or inherently discloses “[t]he method of claim 1, wherein the profile is activated on the vehicle when the user information, including biometrics data, is verified.” For example: Rector at [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

Claims	Prior Art
	communicating with a driver's device S350. 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 S351. 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 S352. 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 S353. 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 S354. 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 S355. 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 S356. 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. Rector at [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.

Rector at [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.

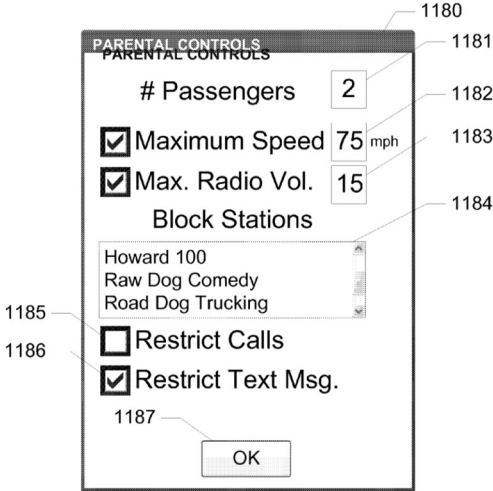
Rector at [0051]

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.

Rector at [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.

To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.

Claims	Prior Art
[14] 14. The method of claim 1, wherein the plurality of settings include one or more of tracking settings, or use metrics settings, or comfort settings, or entertainment settings, or driving mode settings, or refuel routing settings, or purchase settings, or combinations of two or more thereof.	Rector expressly or inherently discloses “[t]he method of claim 1, wherein the plurality of settings include one or more of tracking settings, or use metrics settings, or comfort settings, or entertainment settings, or driving mode settings, or refuel routing settings, or purchase settings, or combinations of two or more thereof.” For example: Rector at 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. Rector at Fig. 11  Figure 11

Rector at [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.

Rector at [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.

Rector at [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.

Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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 S350. 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

Claims	Prior Art
	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 S351. 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 S352. 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 S353. 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 S354. 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 S355. 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 S356. 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. Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[15] 15. The method of claim 1, wherein the profile stored in the storage is accessible via a device using a connection to the Internet and/or a vehicle interface of the vehicle, and the device is one of a portable device, or a computer.	Rector expressly or inherently discloses “[t]he method of claim 1, wherein the profile stored in the storage is accessible via a device using a connection to the Internet and/or a vehicle interface of the vehicle, and the device is one of a portable device, or a computer.” For example: Rector at [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

Claims	Prior Art
	(read-only memories), EPROMS (erasable programmable read-only memories), and EEPROMS (electrically erasable programmable read-only memories). To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[16] 16. The method of claim 1, wherein the user information includes one or more of sign-in credentials, or biometrics or face recognition data, or voice data, or fingerprint data, or eye-retina scan data, or a combination of two or more thereof.	Rector expressly or inherently discloses “[t]he method of claim 1, wherein the user information includes one or more of sign-in credentials, or biometrics or face recognition data, or voice data, or fingerprint data, or eye-retina scan data, or a combination of two or more thereof.” For example: Rector at [0047] 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. Rector at [0049] 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. Rector at [0051] 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.

Claims	Prior Art
	To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[17pre] 17. A cloud-based system including one or more data centers, and each data center of the cloud-based system includes one or more servers, wherein some of said one or more servers have program instructions for enabling connections with vehicles and providing services to vehicles, wherein one service includes enabling access to settings associated with profiles of user accounts of the cloud-based system, comprising:	To the extent the preamble is limiting, Rector expressly or inherently discloses “[a] cloud-based system including one or more data centers, and each data center of the cloud-based system includes one or more servers, wherein some of said one or more servers have program instructions for enabling connections with vehicles and providing services to vehicles, wherein one service includes enabling access to settings associated with profiles of user accounts of the cloud-based system.” For example: Rector at 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.

Rector at Fig. 1

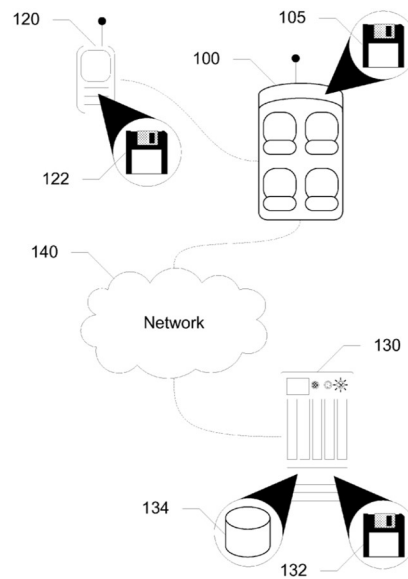


Figure 1

Rector at Title

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

Rector at [0006]

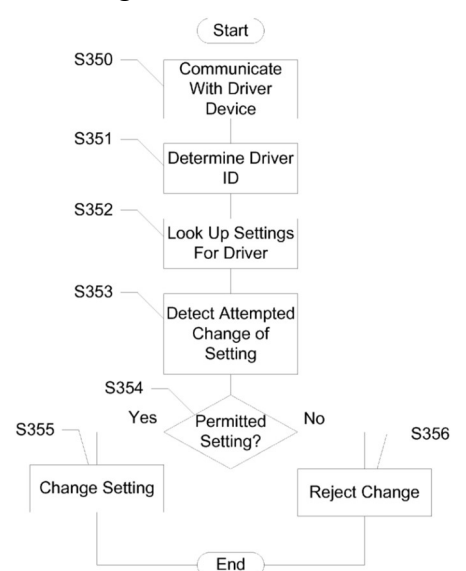
Present-day technology can alleviate some of these distractions. Notably, microelectronic devices are becoming more and more ubiquitous. By coupling processors, memories, and transceivers to these devices, almost any handheld object can become a wireless communication device capable of transmitting and 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.

Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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

Claims	Prior Art
	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. Rector at [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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[17a] receiving, by one of the servers, a request from a vehicle to access a profile for a user account associated with a user, the request identifies user information related to a user;	Rector expressly or inherently discloses “receiving, by one of the servers, a request from a vehicle to access a profile for a user account associated with a user, the request identifies user information related to a user.” For example: See above at row [1a]. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[17b] processing, by one of the servers, at least part of the user	Rector expressly or inherently discloses “processing, by one of the servers, at least part of the user information to verify the access for the user, the profile having a plurality of settings of the user for the

Claims	Prior Art
information to verify the access for the user, the profile having a plurality of settings of the user for the vehicle [and at least one of said plurality of settings being restricted for use on the vehicle, wherein] at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers; and	vehicle at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers” or, to the extent the claim is amended, Rector expressly or inherently discloses “processing, by one of the servers, at least part of the user information to verify the access for the user, the profile having a plurality of settings of the user for the vehicle and at least one of said plurality of settings being restricted for use on the vehicle, wherein at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers.” For example: Rector at 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. Rector at Fig. 3  <pre> graph TD Start([Start]) --> S350[Communicate With Driver Device] S350 --> S351[Determine Driver ID] S351 --> S352[Look Up Settings For Driver] S352 --> S353[Detect Attempted Change of Setting] S353 --> S354{Permitted Setting?} S354 -- Yes --> S355[Change Setting] S354 -- No --> S356[Reject Change] S355 --> End([End]) S356 --> End </pre> Figure 3

Rector at Fig. 11

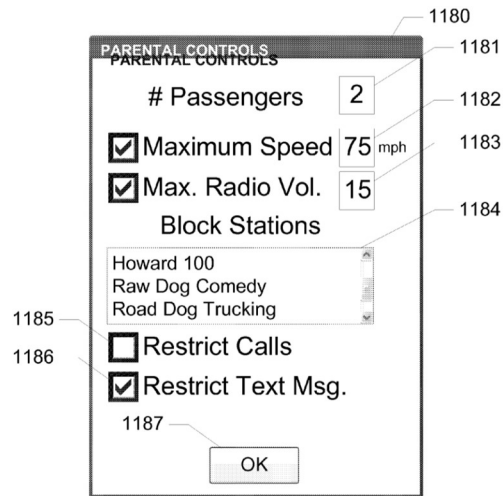


Figure 11

Rector at Title

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

Rector at [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.

Rector at [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.

Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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.

Rector at [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.

Rector at [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.

Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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. Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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 S350. 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 S351. 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 S352. 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

Claims	Prior Art
	S353. 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 S354. 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 S355. 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 S356. 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. Rector at [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. Rector at [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.

Rector at [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.

Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[17c] transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to [storage of] the vehicle, the transferring is configured to instruct software and hardware associated the vehicle to enable said one or more settings for use on the vehicle to customize said vehicle for the user, the request and the transferring being via wireless communication of said vehicle.	Rector expressly or inherently discloses “transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to the vehicle, the transferring is configured to instruct software and hardware associated the vehicle to enable said one or more settings for use on the vehicle to customize said vehicle for the user, the request and the transferring being via wireless communication of said vehicle” or, to the extent the claim is amended, Rector expressly or inherently discloses “transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to storage of the vehicle, the transferring is configured to instruct software and hardware associated the vehicle to enable said one or more settings for use on the vehicle to customize said vehicle for the user, the request and the transferring being via wireless communication of said vehicle.” For example: Rector at [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.

Rector at [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.

Rector at [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.

Rector at [0010]–[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.

Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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 S350. 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 S351. A client logic and processor on the smart vehicle

Claims	Prior Art
	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 S352. 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 S353. 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 S354. 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 S355. 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 S356. 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. Rector at [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. Rector at [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.

Rector at [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.

Rector at [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,

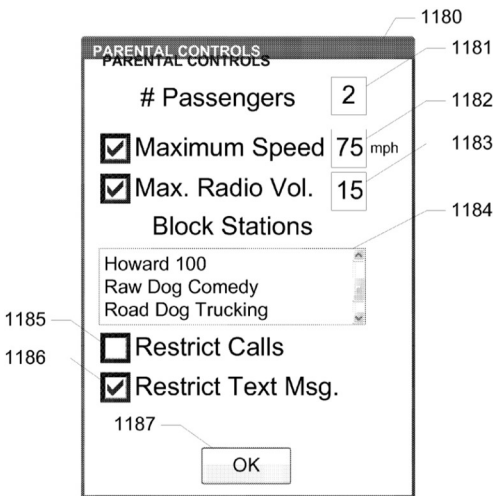
Claims	Prior Art
	etc. With these settings in place when two passengers are present, the smart vehicle will not allow the radio to be changed to these stations. Call restriction option 1185 prevents the driver from receiving calls on the driver's wireless communication device while driving. Text message 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. Rector at claim 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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[18] 18. The cloud-based system of claim 17, wherein the profile is transferrable to one or more other vehicles.	Rector expressly or inherently discloses “[t]he cloud-based system of claim 17, wherein the profile is transferrable to one or more other vehicles.” For example: Rector at [0028] A “vehicle,” as used herein and throughout this disclosure, includes cars, trucks, and buses, as well as aircrafts and watercrafts. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.

Claims	Prior Art
[19] 19. The cloud-based system of claim 17, wherein the vehicle is configured to use the one or more settings for the vehicle while the profile is active in the vehicle, and said one or more settings are removed when the profile is no longer active in the vehicle, and wherein the request is processed automatically by the vehicle upon a pairing of a user device or input by the user of credentials.	Rector expressly or inherently discloses “[t]he cloud-based system of claim 17, wherein the vehicle is configured to use the one or more settings for the vehicle while the profile is active in the vehicle, and said one or more settings are removed when the profile is no longer active in the vehicle, and wherein the request is processed automatically by the vehicle upon a pairing of a user device or input by the user of credentials.” For example: Rector at [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. Rector at [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 S350. 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 S351. 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 S352. 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

Claims	Prior Art
	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 S353. 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 S354. 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 S355. 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 S356. 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. Rector at [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. Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[20pre] 20. The cloud-based system of claim 17,	Rector expressly or inherently discloses “[t]he cloud-based system of claim 17.” See above.
[20a] wherein one or more of the settings are associated with systems of the vehicle, and the systems of the vehicle are configured to receive input or cause one or more actions or functions,	To the extent the preamble is limiting, Rector expressly or inherently discloses “wherein one or more of the settings are associated with systems of the vehicle, and the systems of the vehicle are configured to receive input or cause one or more actions or functions.” For example: Rector at 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

Claims	Prior Art
	distractions to the driver. Further, the settings may be influenced by the number or identities of passengers within the vehicle. Rector at [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. Rector at [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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[20b] wherein the systems include one or more of a door lock, a heating and cooling system, a speaker, an engine start/shut switch, a user interface, a button, a lever, a key, a graphical user interface (GUI), an electronic component of the vehicle, a telecommunications system, a	To the extent the preamble is limiting, Rector expressly or inherently discloses “wherein the systems include one or more of a door lock, a heating and cooling system, a speaker, an engine start/shut switch, a user interface, a button, a lever, a key, a graphical user interface (GUI), an electronic component of the vehicle, a telecommunications system, a remote face-to-face conferencing system, a mapping function system, a GPS system, a fingerprint scanner, a touch screen, a navigation system, a wireless communication system, a data encryption system, WiFi logic, Bluetooth logic, NFC logic, a microprocessor, a memory system, a camera, application programming interfaces (APIs) for vehicle systems, kernel level systems, function invoking systems, temperature detection systems, HVAC APIs, display screens, data network logic, mechanical systems, electrical systems, physical mechanical and electrical systems, seat mechanical systems, mirror

Claims	Prior Art
remote face-to-face conferencing system, a mapping function system, a GPS system, a fingerprint scanner, a touch screen, a navigation system, a wireless communication system, a data encryption system, WiFi logic, Bluetooth logic, NFC logic, a microprocessor, a memory system, a camera, application programming interfaces (APIs) for vehicle systems, kernel level systems, function invoking systems, temperature detection systems, HVAC APIs, display screens, data network logic, mechanical systems, electrical systems, physical mechanical and electrical systems, seat mechanical systems, mirror systems, alarm systems, battery systems, battery, lighting systems, an application shared by mobile a device present and paired with the vehicle for providing at least one interface in a display screen of the vehicle, or vehicle electronics system.	systems, alarm systems, battery systems, battery, lighting systems, an application shared by mobile a device present and paired with the vehicle for providing at least one interface in a display screen of the vehicle, or vehicle electronics system.” For example: Rector at 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. Rector at Fig. 11  Figure 11

Rector at [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.

Rector at [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.

Rector at [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.

Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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. Rector at [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 S350. 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

Claims	Prior Art
	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 S351. 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 S352. 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 S353. 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 S354. 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 S355. 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 S356. 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. Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[21pre] 21. A cloud-based system including one or more data centers, and each data center of the cloud-based system includes one or more servers, wherein some of said one or more servers have program instructions for enabling connections with vehicles and providing services to vehicles, wherein one service includes enabling access to settings associated with profiles of user accounts of the cloud-based system, comprising:	To the extent the patent is amended to include claim 21, Rector discloses it. To the extent the preamble is limiting, Rector expressly or inherently discloses “[a] cloud-based system including one or more data centers, and each data center of the cloud-based system includes one or more servers, wherein some of said one or more servers have program instructions for enabling connections with vehicles and providing services to vehicles, wherein one service includes enabling access to settings associated with profiles of user accounts of the cloud-based system.” For example: See above at row [17pre]. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.

Claims	Prior Art
[21a] receiving, by one of the servers, a request from a vehicle to access a profile for a user account associated with a user, the request identifies user information related to a user;	Rector expressly or inherently discloses “receiving, by one of the servers, a request from a vehicle to access a profile for a user account associated with a user, the request identifies user information related to a user.” For example: See above at row [1a]. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[21b] processing, by one of the servers, at least part of the user information to verify the access for the user, the profile having a plurality of settings of the user for the vehicle, wherein at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers; and	Rector expressly or inherently discloses “processing, by one of the servers, at least part of the user information to verify the access for the user, the profile having a plurality of settings of the user for the vehicle, wherein at least part of the plurality of settings of the profile being stored on storage accessible to said one or more servers.” For example: Rector at [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. Rector at [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. Rector at [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

Claims	Prior Art
	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. Rector at [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. Rector at [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 S350. 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

Claims	Prior Art
	unique identifier is associated with a user of the smart vehicle. With the unique identifier, the smart vehicle determines the identity of the driver S351. 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 S352. 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 S353. 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 S354. 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 S355. 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 S356. 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. Rector at [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. Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[21c] transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to storage of the vehicle, the transferring is configured to	Rector expressly or inherently discloses “transferring, by one of the servers, upon verification of the user information, one or more settings of the plurality of settings to storage of the vehicle, the transferring is configured to instruct software and hardware associated the vehicle to enable said one or more settings for use on the vehicle to customize said vehicle for the user, the request and the transferring being via wireless communication of said vehicle.” For example:

Claims	Prior Art
instruct software and hardware associated the vehicle to enable said one or more settings for use on the vehicle to customize said vehicle for the user, the request and the transferring being via wireless communication of said vehicle;	See above at row [17c]. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[21d] wherein a learning engine executed by a server of at least one data center is configured to process inputs made to one or more settings of the vehicle by the user to generate a recommended setting to add to the plurality of settings of the profile;	Rector expressly or inherently discloses “wherein a learning engine executed by a server of at least one data center is configured to process inputs made to one or more settings of the vehicle by the user to generate a recommended setting to add to the plurality of settings of the profile.” For example: Rector at [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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.
[21e] wherein accepted recommendations are saved to the profile and added to the cloud storage that is accessible to said one or more servers.	Rector expressly or inherently discloses “wherein accepted recommendations are saved to the profile and added to the cloud storage that is accessible to said one or more servers.” For example: Rector at [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.

Rector at [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.

Rector at [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.

Rector at [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.

Claims	Prior Art
	Rector at [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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.

Claims	Prior Art
[22] 22. The cloud-based system of claim 21, wherein the profile is transferrable to one or more other vehicles, and wherein being transferrable enables syncing of said profile by uploading and downloading the profile from the server and saving it to storage of the one or more other vehicles for use of said plurality of settings.	To the extent the patent is amended to include claim 21, Rector discloses it. Rector expressly or inherently discloses “[t]he cloud-based system of claim 21, wherein the profile is transferrable to one or more other vehicles, and wherein being transferrable enables syncing of said profile by uploading and downloading the profile from the server and saving it to storage of the one or more other vehicles for use of said plurality of settings.” For example: Rector at [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. Rector at [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. Rector at [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.

Rector at [0028]

A “vehicle,” as used herein and throughout this disclosure, includes cars, trucks, and buses, as well as aircrafts and watercrafts.

Rector at [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.

Rector at [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 S350. 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 S351. 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 S352. 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 S353. This may be the driver speeding up, the radio volume changing, the radio station changing, the

Claims	Prior Art
	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 S354. 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 S355. 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 S356. 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. Rector at [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

Claims	Prior Art
	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. To the extent that Rector was found not to disclose this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine Rector with the teachings identified in the Exhibit E claim charts for other prior art for this claim limitation as described in the cover pleading.