PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: TADD F. WILSON
SHERIDAN ROSS P.C.
1560 BROADWAY
SUITE 1200
DENVER, CO 80202

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	14 SEP 2017
Applicant's or agent's file reference 8322-30-PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2017/041061	07 July 2017	07 July 2016

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - B60R 99/00; G06F 19/00; G07C 9/00; H04L 29/08 (2017.01)
CPC - B60R 99/00; G06F 19/36; G06F 3/017; H04W 4/046 (2017.08)

Applicant NEXTEV USA, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	17 August 2017	Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2017/041061

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a)).

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2017/041061

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	None	YES
	Claims	1-20	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-20	NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-20 lack novelty under PCT Article 33(2) as being anticipated by Hoyos Labs Corporation (hereinafter Hoyos).

Regarding Claim 1, Hoyos discloses a vehicle, comprising:
a sensor to (See Hoyos: Para 21, "In addition, using optical sensors and other sensors placed throughout the vehicle..."):
detect a first presence of a driver in a vehicle (See Hoyos: Para 127, "...the on-board computer can detect when Joe sits down in the driver's seat.");
detect a second presence of a passenger in the vehicle (See Hoyos: Para 120, "Other cameras might be place in the passenger locations so that passengers can be detected as well")
a memory to: store first sensitive information (See Hoyos: Para 51, "In some implementations, sensitive user information can be stored on an encrypted datastore...")for the driver of the vehicle
store second sensitive information for a passenger in the vehicle (See Hoyos: Para 30, "...the client app can configure the user devices to provide users with secure access to systems and services that typically require physical keys, a password and or a username, and the like") [username and password are sensitive information] See also Para 72);
a processor in communication with the sensor and the memory (See Hoyos: Para 44, "components of the on-board computer include one or more processors 110, a memory 120, a microphone 125, a display 140, one or more cameras 145, and audio output 155, a storage 190 and a communication interface 150."), the processor to: receive the first presence and second presence (See Hoyos: Para 45, "Processor 110 servers to execute the client application including software instructions in the form of executable code that can be loaded into memory 120."; See also Para 141, "The imagery can be analyzed by the on-board computer to detect the presence of occupants (driver and/or passengers) in the vehicle.");
provide a user interface for the passenger to enter the sensitive information (See Hoyos: Fig. 2A User Interface 110; Para 53, "A User interface 115 is also operatively connected to the processor...For example, interface servers to facilitate the capture of certain information form the user such as person information...");
receive the second sensitive information for the passenger (See Hoyos: Para 134, "The disclosed embodiments also provide an infrastructure with which vehicle owners can share access to a vehicle.");
associate the second sensitive information with the vehicle (See Hoyos: Para 51, "For example, using key derivation function one or more secret keys can be generated from unique user information such as biometric information such that the key is uniquely associated with the user.." See also Para 84, "...a particular vehicle can be shared by any number of approved users..."); and
send the second sensitive information to the memory for storage (See Hoyos: Para 134, "...The owner can define setting that identify the friend and the vehicle, which prompts the system server 105 to generate an encrypted key and send the encrypted key to the friends mobile device that can.").

Regarding Claim 2, Hoyos discloses the vehicle of claim 1, wherein the sensor receives biometric information associated with the passenger (See Hoyos: Para 23, "During authentication by the on-board computer, for example, biometric information can be captured using one or more sensors that are located in or around the vehicle and that are operatively connected to the on-board computer.").

Regarding Claim 3, Hoyos discloses the vehicle of claim 2, wherein the biometric information is also stored with the second sensitive information (See Hoyos: Para 34, "The user devices can also be configured to receive user inputs, as well as facilitate biometric authentication of users by capturing and processing user biometric information." See also Para 95).

Regarding Claim 4, Hoyos discloses the vehicle of claim 3, wherein, when the passenger enters the vehicle a second time (See Hoyos: Para 20, "...the term "access" encompasses one or more user's physical access to a vehicle..."), the biometric information identifies the passenger (See Hoyos: Para 132, "Access rules/permissions relating to each enrolled user can also be defined by the owner." [upon each entry to the vehicle, authorized users are identified]).

Regarding Claim 5, Hoyos discloses the vehicle of claim 1, wherein the second sensitive information is encrypted in the memory (See Hoyos: Para 51, In some implementations, sensitive user information can be stored on an encrypted datastore that is specifically allocated so as to securely store information collected or generated by the processor...").

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2017/041061

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding Claim 6, Hoyos discloses the vehicle of claim 5, wherein the second sensitive information comprises one or more of a biometric (See Hoyos: Para 07, "...biometrically authenticated by the mobile device..."), a username. a password (See Hoyos: Para 93, "...the device can receive form the user additional user identification information, passwords..."), mobile device information, payment information, a personal identification number, identifiers, an address, limits, preferences, and/or rules (See Hoyos: Para 91, "...the user can specify default payment methods/accounts thereby configuring the on-board-computer 101b and/or system server 105 to process transactions..." See also Para 22 user based on rules and permissions) .

Regarding Claim 7, Hoyos discloses the vehicle of claim 6, wherein the second sensitive information comprises one or more of a desired product, a desired service (See Hoyos: para 20, " The user access also includes using features, functions and services provided by a computing device that is integrated into the vehicle..." See also Para 145), and/or a triggering event.

Regarding Claim 8, Hoyos discloses the vehicle of claim 1, wherein the processor presents a user interface to a head unit display (See Hoys: Fig. 2A Display 140; to receive the second sensitive information (See Hoyos: Para 53, "User Interface serves to facilitate the capture of commands from the users..." See also Para 55).

Regarding Claim 9, Hoyos discloses the vehicle of claim 8, wherein the user interface receives input from the passenger in the user interface (See Hoyos: Para 55, "...the interface and display can be integrated into a touch screen display. Accordingly, the display is also used a show a graphical user interface, which can display various data and provide "forms" that include fields that allow for the entry of information by the user.").

Regarding Claim 10, Hoyos discloses the vehicle of claim 9, wherein the input includes financial information (See Hoyos: Para 75, "...the methods are used to authenticate a financial transaction may require stringent identity validation"; See also Para 122, "...user is trying to complete a financial transaction...").

Regarding Claim 11, Hoyos discloses a method for associated passenger information with a vehicle, comprising:
detecting a first presence of a driver in a vehicle (See Hoyos: Para 127, "...the on-board computer can detect when Joe sits down in the driver's seat.");
detecting a second presence of a passenger in the vehicle(See Hoyos: Para 120, "Other cameras might be place in the passenger locations so that passengers can be detected as well")
receiving the first presence and second presence (See Hoyos: Para 45, "Processor 110 servers to execute the client application including software instructions in the form of executable code that can be loaded into memory 120."; See also Para 141, "The imagery can be analyzed by the on-board computer to detect the presence of occupants (driver and/or passengers) in the vehicle.")
providing a user interface for the passenger to enter the sensitive information (See Hoyos: Para 53, "User Interface serves to facilitate the commands form the user such as an on-off commands or user information and settings related to operation of the disclosed embodiments. For example, interface serves to facilitate the capture of certain information...");
receiving the second sensitive information for the passenger (See Hoyos: Para 134, "The disclosed embodiments also provide an infrastructure with which vehicle owners can share access to a vehicle.");
associating the second sensitive information with the vehicle (See Hoyos: Para 51, "For example, using key derivation function one or more secret keys can be generated from unique user information such as biometric information such that the key is uniquely associated with the user.." See also Para 84, "...a particular vehicle can be shared by any number of approved users..."); and
storing second sensitive information for a passenger in the vehicle (See Hoyos: Para 134, "...The owner can define setting that identify the friend and the vehicle, which prompts the system server 105 to generate an encrypted key and send the encrypted key to the friends mobile device that can.").

Regarding Claim 12, Hoyos discloses the method of claim 11, wherein the sensor receives biometric information associated with the passenger (See Hoyos, "Para 135, The conditions relating to the parameters can be automatically enforced based on, biometric authentication and authorization...received from on-board sensors..."), wherein the biometric information is also stored (See Hoyos: Para 137, "The information collectd by the on-board computer during use of the vehicle can be stored locally and/or on a remote device such as the system server.") with the second sensitive information, and wherein, when the passenger enters the vehicle a second time, the biometric information identifies the passenger (See Hoyos: Para 117, "Authorization can also include determining, by the system server 105, whether the user has permission to "access" the vehicle as requested..." and Para 57, "...the imagery is captured for the purpose of biometrically identifying/authenticating the user from the images.").

Regarding Claim 13, Hoyos discloses the method of claim 12, wherein the second sensitive information is encrypted in the memory (See Hoyo: Para 29, "In particular, the
BOPS protocol can enable a two-way secure socket layer (SSL)/transport layer security (TLS)
connection over an encryption mechanism between user devices and the system
server."), wherein the second sensitive information comprises one or more of a biometric (See Hoyos: Para 07, "...biometrically authenticated by the mobile device..."), a username. a password (See Hoyos: Para 93, "...the device can receive form the user additional user identification information, passwords..."), mobile device information (See Hoyos: Para 152, "...mobile device 101a..."), payment information, a personal identification number (See Hoyos: Para 112, "...information identifying the user (e.g., user identification information or a user's identifier..."), identifiers, an address, limits, preferences, and/or rules (See Hoyos: Para 91, "...the user can specify default payment methods/accounts thereby configuring the on-board-computer 101b and/or system server 105 to process transactions...").

Regarding Claim 14, Hoyos discloses the method of claim 13, wherein the second sensitive information comprises one or more of a desired product , a desired service (See Hoyos: para 20, " The user access also includes using features, functions and services provided by a computing device that is integrated into the vehicle..." See also Para 145), and/or a triggering event.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2017/041061

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:

Regarding Claim 15, Hoyos discloses the method of claim 14, wherein the processor presents a user interface to receive the second sensitive information, wherein the user interface receives input from the passenger, and wherein the input includes financial information (See Hoyos: Para 75, "...the methods are used to authenticate a financial transaction may require stringent identity validation"; See also Para 122, "...user is trying to complete a financial transaction...").

Regarding Claim 16, Hoyos discloses a non-transitory information storage media having stored thereon one or more instructions, that when executed by one or more processors (See Hoyos: Para 160, "...portion of coed, which comprises one or more executable instructions, for implementing the specified logical function(s)."), cause a vehicle to perform a method, the method comprising:
detecting a first presence of a driver in a vehicle (See Hoyos: Para 127, "...the on-board computer can detect when Joe sits down in the driver's seat.");
detecting a second presence of a passenger in the vehicle receiving the first presence and second presence (See Hoyos: Para 120, "Other cameras might be place in the passenger locations so that passengers can be detected as well");
providing a user interface for the passenger to enter the sensitive information (See Hoyos: Fig. 2A User Interface 110; Para 53, "A User interface 115 is also operatively connected to the processor...For example, interface servers to facilitate the capture of certain information form the user such as person information...");
receiving the second sensitive information for the passenger; associating the second sensitive information with the vehicle (See Hoyos: Para 134, "The disclosed embodiments also provide an infrastructure with which vehicle owners can share access to a vehicle."); and storing second sensitive information for a passenger in the vehicle (See Hoyos: Para 134, "...The owner can define setting that identify the friend and the vehicle, which prompts the system server 105 to generate an encrypted key and send the encrypted key to the friends mobile device that can.").

Regarding Claim 17, Hoyos discloses the media of claim 16, wherein the sensor receives biometric information associated with the passenger (See Hoyos, "Para 135, The conditions relating to the parameters can be automatically enforced based on, biometric authentication and authorization...received from on-board sensors..."), wherein the biometric information is also stored (See Hoyos: Para 137, "The information collectd by the on-board computer during use of the vehicle can be stored locally and/or on a remote device such as the system server.") with the second sensitive information, and wherein, when the passenger enters the vehicle a second time, the biometric information identifies the passenger (See Hoyos: Para 117, "Authorization can also include determining, by the system server 105, whether the user has permission to "access" the vehicle as requested..." and Para 57, "...the imagery is captured for the purpose of biometrically identifying/authenticating the user from the images.").

Regarding Claim 18, Hoyos discloses the media of claim 17, wherein the second sensitive information is encrypted in the memory, wherein the second sensitive information comprises one or more of a biometric biometric (See Hoyos: Para 07, "...biometrically authenticated by the mobile device..."), a username. a password (See Hoyos: Para 93, "...the device can receive form the user additional user identification information, passwords..."),, mobile device information, payment information, a personal identification number, identifiers, an address, limits, preferences, and/or rules (See Hoyos: Para 91, "...the user can specify default payment methods/accounts thereby configuring the on-board-computer 101b and/or system server 105 to process transactions...").

Regarding Claim 19, Hoyos discloses the media of claim 18, wherein the second sensitive information comprises one or more of a desired product, a desired service (See Hoyos: para 20, " The user access also includes using features, functions and services provided by a computing device that is integrated into the vehicle..." See also Para 145), and/or a triggering event.

Regarding Claim 20, Hoyos discloses the media of claim 19, wherein the processor presents a user interface to receive the second sensitive information, wherein the user interface receives input from the passenger, and wherein the input includes financial information (See Hoyos: Para 75, "...the methods are used to authenticate a financial transaction may require stringent identity validation"; See also Para 122, "...user is trying to complete a financial transaction...").

Claims 1-20 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.