UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/992,805	01/11/2016	Sandeep CHENNAKESHU	P5230US00	8050

63617 7590 02/28/2020

PERRY + CURRIER INC. (BlackBerry)
1300 YONGE STREET
SUITE 500
TORONTO, ONTARIO M4T-1X3
CANADA

EXAMINER	
NGUYEN, NGA X	

ART UNIT	PAPER NUMBER
3662	

NOTIFICATION DATE	DELIVERY MODE
02/28/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@pckip.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte SANDEEP CHENNAKESHU

Appeal 2019-002690
Application 14/992,805
Technology Center 3600

Before JOHN C. KERINS, CHARLES N. GREENHUT, and LISA M. GUIJT, *Administrative Patent Judges*.

GUIJT, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellant[1] seeks our review under 35 U.S.C. § 134(a) of the rejection of claims 1–19. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies Blackberry Limited as the real party in interest. Br. 3.

THE INVENTION

Appellant's invention relates to "computing devices in vehicles . . . for collecting user-based insurance data in vehicles." Spec. ¶ 1. Claims 1, 10, and 19 are the independent claims on appeal. Claim 1, reproduced below, is illustrative of the subject matter on appeal.

1. A device comprising:

a processor;

a memory storing (i) a plurality of driver-associated encryption keys, and (ii) for each of the plurality of driver-associated encryption keys, a corresponding driver identifier; the plurality of driver identifiers corresponding to respective drivers; and

a communication interface configured to communicate with a vehicle diagnostic monitor and a remote server, the processor configured to:

determine a current driver of the vehicle by receiving data that identifies the current driver;

select, as a current encryption key, one of the plurality of the driver-associated encryption keys that corresponds to one of the driver identifiers matching the data that identifies the current driver;

collect, using the communication interface, vehicle data from the vehicle diagnostic monitor;

encrypt the vehicle data using the current encryption key to produce encrypted vehicle data; and,

transmit, using the communication interface, the encrypted vehicle data to the remote server.

THE REJECTIONS

The Examiner relies upon the following as evidence in support of the rejections:

NAME	REFERENCE	DATE
Davis	US 6,038,549	Mar. 14, 2000
McMillan	US 6,064,970	May 16, 2000
Phillips	US 2016/0086397 A1	Mar. 24, 2016

The following rejections are before us for review:

1. Claims 1–4, 6–8, 10–12, 14–17, and 19 are rejected under 35 U.S.C. § 103 as unpatentable over McMillan and Phillips.

2. Claims 5, 9, 13, and 18 are rejected under 35 U.S.C. § 103 as unpatentable over McMillan, Phillips, and Davis.

OPINION

Rejection I

Appellant argues claims 1–4, 6–8, 10–12, 14–17, and 19 as a group. We select claim 1 as representative, with claims 2–4, 6–8, 10–12, 14–17, and 19 standing or falling with claim 1. *See* 37 C.F.R. § 41.37(c)(1)(iv).

Regarding independent claims 1, 10, and 19, the Examiner finds that McMillan discloses a processor (i.e., on-board computer 300) and memory device (i.e., on-board data storage device 402), and also a communication interface (i.e., input/output subsystem 404) configured to communicate with a vehicle diagnostic monitor and a remote server (i.e., operation control center 416), wherein the processor is configured to (i) determine a current driver of the vehicle by receiving data that identifies the current driver (i.e., driver input console 410); and (ii) collect, using the communication

interface, vehicle data from the vehicle diagnostic monitor. Final Act. 2–3 (citing McMillan, 6:44–7:22, 10:50, Figs. 3, 4).

The Examiner determines that McMillan fails to teach the claim limitations involving encryption, and relies on Phillips for disclosing the claim limitations involving "driver-associated encryption keys." Final Act. 3–4 (citing, at least, Phillips ¶¶ 50, 115, 116, 118–140, 202–207, 230–232, 228–229). The Examiner reasons that it would have been obvious to modify McMillan to use driver-associated encryption keys, as taught by Phillips, "for security [of] the driver's information." *Id.* at 4–5 (emphasis omitted).

Appellant argues that "[t]he Examiner's assertion that Phillips discloses *driver-associated encryption keys* is unsupported by [paragraphs 50 and 118–140 of Phillips, as relied on by the Examiner]." Br. 8. Appellant submits that "Phillips merely mentions various mechanisms by which <u>any</u> driver profiles could be encrypted," but "does not relate any of the various mechanisms to encrypting driver profiles, and in particular does not suggest storing separate encryption keys corresponding to different driver profiles." *Id.* at 9 ("[Phillips is] <u>silent</u> on storing encryption keys <u>on a per-driver basis</u>"). Appellant submits that "Phillips merely discuss[es] wireless encryption in general terms, and provide[s] no guidance that would lead the skilled person to implement a wireless security scheme in which distinct encryption keys are stored for each driver profile 28." *Id.*

The Examiner responds by explaining that Phillips is relied on for enabling "driver-associated encryption keys," as follows:

> [a] computer readable medium 40 for storing a unique driver profile 28 for the drivers 42, wherein the profile 28 is stored in an encrypted format (see at least [Phillips ¶¶ 115–116]. . . . The security and encryptions techniques for secure communications and secure storage of data in the computer readable medium 40

> includes security and encryption application programs 41 such as Wireless Encryption Protocol (WEP) which accepts encryption keys (see at least [Phillips ¶¶ 120, 121]) . . . . Therefore, the computer readable medium 40 enables to have []"a memory storing (i) a plurality of driver-associated encryption keys, and (ii) for each of the plurality of driver-associated encryption keys, a corresponding driver identifier; the plurality of driver identifiers corresponding to respective drivers."

Ans. 4 (emphasis added).

Phillips discloses that

> [t]he electronic circuit 36 is configured for automatically creating the unique driver profile 28 for a driver 42 of the vehicle 24 from the electronic information 30 . . . received as a result of the driver 42 operating the vehicle 24 and stored in the non-transitory computer readable medium 40. The non-transitory computer readable medium 40 connected to the electronic circuit 36 is used for storing the created unique driver profile 28 and for storing the electronic information 30 received from the plural electronic signals . . . received as the result of the driver 42 operating the vehicle.

Phillips ¶ 50; *see also id.* at Abstract ("[t]he unique driver profile information is recorded on the apparatus and/or network device, downloaded at a later time or sent in real-time to check and verify an identity of a driver"); ¶ 116 ("unique driver profile 28 . . . is stored in an encrypted format in the non-transitory computer readable medium").

Phillips also discloses, as relied on by the Examiner *supra*, the use of "one or more of the . . . encryption[] techniques discussed herein for . . . [the] secure storage of data" (*id.* ¶ 118), for example, "Wireless Encryption Protocol (WEP)," which "is cryptographic privacy algorithm, based on the Rivest Cipher 4 (RC4) encryption engine" (*id.* ¶ 120), and "RC4," which "can accept encryption keys of arbitrary length, and is essentially a pseudo random number generator with an output of the generator being XORed with

a data stream to produce encrypted data" (*id.* ¶ 121) (wherein Phillips discloses that WEP uses static encryption keys (*id.* ¶ 122)).

Thus, a preponderance of the evidence supports the Examiner's finding that Phillips at least discloses the concept of separately storing (or downloading) *encrypted data* into a memory, wherein the separately stored encrypted data corresponds to *individual* driver identifiers corresponding to drivers (i.e., unique driver profiles), and further, Phillips at least suggests using encryption keys associated with stored data files. Thus, contrary to Appellant's argument, we determine that Phillips is not silent regarding the use of encryption keys for indexing (i.e., selecting and adding encrypted vehicle data to a data file, as claimed), as argued by Appellant, but rather, provides *some* guidance for storing encrypted data representative of separately stored, individual, unique driver profiles relative to encryption keys capable of use for indexing the profiles. The arguments presented do not apprise us of error in the Examiner's finding that Phillips discloses using encryption keys to store individual driver data files and, in combination with McMillan, enables indexing individual driver identifiers using corresponding encryption keys for the selection and matching of driver profiles with additional vehicle data.

Accordingly, we sustain the Examiner's rejection of independent claim 1, and claims 2–4, 6–8, 10–12, 14–17, and 19 fall therewith.

Rejection II

Appellant chose not to present separate arguments for the patentability of dependent claims 5, 9, 13, and 18. Br. 8–10. Therefore, for essentially

the same reasons as set forth *supra*, we also sustain the Examiner's rejection of claims 5, 9, 13, and 18.

CONCLUSION

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)	Affirmed	Reversed
1–4, 6–8, 10–12, 14–17, 19	103	McMillan, Phillips	1–4, 6–8, 10–12, 14–17, 19	
5, 9, 13, 18	103	McMillan, Phillips, Davis	5, 9, 13, 18	
Overall Outcome			1–19	

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED