

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MERCEDES-BENZ GROUP AG,
Petitioner,

v.

THE PHELAN GROUP, LLC
Patent Owner.

Case (to be assigned)
U.S. Patent No. 9,908,508

**PETITION FOR *INTER PARTES* REVIEW OF
CLAIMS 1-14 OF U.S. PATENT NO. 9,908,508
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. §§42.100 *et seq.***

Filed on behalf of Petitioner:

Celine Jimenez Crowson (Reg. No. 40,357)
Joseph Raffetto (Reg. No. 66,218)
Scott Hughes (Reg. No. 68,385)
HOGAN LOVELLS US LLP
555 13th Street N.W.
Washington, D.C. 20004
Telephone: 202.637.5600
Facsimile: 202.637.5710

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. MANDATORY NOTICES (37 C.F.R. §42.8(A)(1)).....	2
A. Real Parties-in-Interest.....	2
B. Related Matters.....	3
C. Counsel and Service Information.....	3
III. NOTICE OF FEES PAID.....	4
IV. CERTIFICATION OF GROUNDS FOR STANDING	4
V. PRECISE RELIEF REQUESTED	4
VI. '508 OVERVIEW.....	5
A. Background	5
B. Prosecution	6
C. Priority Date	7
VII. CLAIM CONSTRUCTION AND POSITA.....	7
A. Claim Construction.....	7
B. Definition of a Person of Ordinary Skill in the Art.....	7
VIII. ANALYSIS OF GROUNDS FOR UNPATENTABILITY	8
A. <u>Ground 1</u> – Murphy Anticipates and Renders Obvious Claims 1-6, 8-11, 13-14.....	8
1. Independent Claims.....	8
a) Claim 1	8
1[pre]: <i>A system comprising:</i>	8
1[A]: <i>a driver authentication system for authenticating at least one driver via a driver identification interface,</i>	9
1[B]: <i>wherein the driver authentication system receives a unique identification code to permit the at least one driver to operate the vehicle within an operating profile associated with the at least one driver; and</i>	12
1[C]: <i>[i] at least one computer associated with the driver authentication system, said driver authentication</i>	

system in communication with said computer and [ii] configured to monitor operation of the vehicle and generate a signal if the at least one driver violates the operating profile thereby providing feedback to the driver authentication system about usage of the vehicle, and [iii] wherein the driver authentication system cooperates with the at least one computer to control operation of the vehicle.

.....15

b) Claim 11 21

11[pre]: A system comprising: 21

11[A]: a driver authentication system in a motor vehicle for authenticating at least one driver via driver identification and associating an operating profile with the at least one driver; 21

11[B]: a GPS module providing at least location and speed information in association with movement of the motor vehicle; and 21

11[C]: a data logging device recording vehicle operation data associated with use of the motor vehicle by the at least one driver including location and speed information from the GPS module; 23

11[D]: wherein said driver authentication system is coupled to at least one computer associated with the motor vehicle, and is configured to monitor operation of the motor vehicle and generate a signal to the driver authentication system if the at least one driver violates the operating profile, and wherein the driver authentication system cooperates with the at least one computer to control operation of the vehicle; 23

11[E]: wherein the driver authentication system permits the at least one driver to operate the vehicle within an operating profile if the driver authentication system receives at least one of a unique identification code to permit the at least one driver

	<i>to operate the vehicle within an operating profile and the at least one driver has not violated the operating profile.....</i>	<i>24</i>
2.	Dependent Claims	24
a)	Claim 2: <i>The system of claim 1, further comprising a database comprising a program module including at least one operating parameter associated with a vehicle, the program module remotely accessible by an authorized user to program an operating profile with respect to at least one driver, the program module accessed by the authorized user via a network utilizing a remote computer.</i>	<i>24</i>
b)	Claim 3: <i>The system of claim 2, wherein the driver identification interface in conjunction with a remote computer loads the operating profile in the driver authentication system for the at least one driver.</i>	<i>26</i>
c)	Claim 4: <i>The system of claim 1, further comprising: a GPS module; a memory module; and a function indicator module.</i>	<i>28</i>
d)	Claim 5: <i>The system of claim 4, wherein the operating profile is loaded into the memory module for enabling controlled operation of the vehicle when the at least one driver is authenticated.....</i>	<i>32</i>
e)	Claim 6: <i>The system of claim 4, wherein the GPS module provides location information to the driver authentication system indicating a physical location of the vehicle.</i>	<i>33</i>
f)	Claims 8/13: <i>The system of claim [2/11], wherein [the/the operating profile comprises] at least one operating parameter [comprises/including] at least one of: a maximum allowable vehicle speed; an allowable vehicle location; allowable hours of operation; and seatbelt usage.....</i>	<i>33</i>
g)	Claims 9/14: <i>The system of claim [1/11], wherein the driver authentication system generates an alarm signal for [remotely] alerting [said/the] authorized user when the at least one driver violates [the/said] operating profile.</i>	<i>34</i>

h)	Claim 10: <i>The system of claim 1, wherein the driver identification interface comprises at least one of: a portable handheld device; a radio frequency identification device; and a USB compatible device.</i>	35
B.	<u>Ground 2</u> – Murphy-Adams Renders Obvious Claim 10	36
C.	<u>Ground 3</u> – Murphy-Wu Renders Obvious Claims 7/12	38
D.	<u>Ground 4</u> – Petrik Anticipates and Renders Obvious Claims 1-6, 8-11, 13-14.....	42
1.	Independent Claims.....	42
a)	Claim 1	42
	1[pre]: <i>A system comprising:</i>	43
	1[A]: <i>a driver authentication system for authenticating at least one driver via a driver identification interface,</i>	43
	1[B]: <i>wherein the driver authentication system receives a unique identification code to permit the at least one driver to operate the vehicle within an operating profile associated with the at least one driver; and</i>	45
	1[C]: [i] <i>at least one computer associated with the driver authentication system, said driver authentication system in communication with said computer and</i> [ii] <i>configured to monitor operation of the vehicle and generate a signal if the at least one driver violates the operating profile thereby providing feedback to the driver authentication system about usage of the vehicle, and</i> [iii] <i>wherein the driver authentication system cooperates with the at least one computer to control operation of the vehicle.</i>	47
b)	Claim 11	51
2.	Dependent Claims	54
a)	Claim 2: <i>The system of claim 1, further comprising a database comprising a program module including at least one operating parameter associated with a vehicle, the program module remotely accessible by an authorized</i>	

	<i>user to program an operating profile with respect to at least one driver, the program module accessed by the authorized user via a network utilizing a remote computer.</i>	54
b)	<i>Claim 3: The system of claim 2, wherein the driver identification interface in conjunction with a remote computer loads the operating profile in the driver authentication system for the at least one driver.</i>	56
c)	<i>Claim 4: The system of claim 1, further comprising: a GPS module; a memory module; and a function indicator module.</i>	57
d)	<i>Claim 5: The system of claim 4, wherein the operating profile is loaded into the memory module for enabling controlled operation of the vehicle when the at least one driver is authenticated.</i>	58
e)	<i>Claim 6: The system of claim 4, wherein the GPS module provides location information to the driver authentication system indicating a physical location of the vehicle.</i>	59
f)	<i>Claims 8/13: The system of claim [2/11], wherein [the/the operating profile comprises] at least one operating parameter [comprises/including] at least one of: a maximum allowable vehicle speed; an allowable vehicle location; allowable hours of operation; and seatbelt usage.</i>	59
g)	<i>Claims 9/14: The system of claim [1/11], wherein the driver authentication system generates an alarm signal for [remotely] alerting [said/the] authorized user when the at least one driver violates [the/said] operating profile.</i>	60
h)	<i>Claim 10: The system of claim 1, wherein the driver identification interface comprises at least one of: a portable handheld device; a radio frequency identification device; and a USB compatible device.</i>	61
E.	Ground 5 – Petrik-Schanz Render Obvious Claims 1-6, 8-11, 13-14	61
1.	Independent Claims	61
a)	Claim 1	61
b)	Claim 11	64

2.	Dependent Claims 2-6, 8-10, 13-14.....	65
F.	<u>Ground 6</u> – Petrik (Alone or as Modified by Schanz) in View of Adams Renders Obvious Claim 10	65
G.	<u>Ground 7</u> – Petrik (Alone or as Modified by Schanz) in View of Wu Renders Obvious Claims 7/12.....	66
IX.	DISCRETIONARY CONSIDERATIONS UNDER 314(A) AND 325(D) STRONGLY FAVOR INSTITUTION.	69
A.	The <i>Fintiv</i> Factors Strongly Favor Institution.....	69
B.	<i>Advanced Bionics</i> Strongly Favors Institution.....	69
X.	CONCLUSION.....	70

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Oticon Medical AB v. Cochlear Ltd.</i> , IPR2019-00975, Paper 15 (P.T.A.B. Oct. 16, 2019).....	70
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (Dec. 1, 2020)	69
<i>The Phelan Group, LLC v. Honda Motor Co.</i> , No. 2-23-cv-00606 (E.D. Tex.).....	3
<i>The Phelan Group, LLC v. Kia Corp.</i> , No. 2-23-cv-00094 (E.D. Tex.).....	3
<i>The Phelan Group, LLC v. Mercedes-Benz Group AG</i> , No. 1-25-cv-01399 (N.D. Ga.).....	3
<i>The Phelan Group, LLC v. Mercedes-Benz Group AG</i> , No. 2-23-cv-00607 (E.D. Tex.).....	3
<i>The Phelan Group, LLC v. State Farm Mutual Automobile Insurance Co.</i> , Case No. 2-23-cv-00611 (E.D. Tex.).....	3
<i>The Phelan Group, LLC v. Toyota Motor Corp.</i> , No. 2-23-cv-00093 (E.D. Tex.).....	3

Statutes

35 U.S.C. §102(b)	8
35 U.S.C. §103.....	7

Other Authorities

37 C.F.R. ¶ 42.100(b).....	7
37 C.F.R. §42.8(A)(1).....	2

I. INTRODUCTION

Mercedes-Benz Group AG (“**Petitioner**”) challenges Claims 1-14 of US9,908,508 (EX1001) (“’508”). The ’508 purports to invent a “driver authentication and safety system” for “monitoring and controlling vehicle usage by high-risk drivers,” such as “teen[s]...” (’508, Abstract, 2:27-31.) The claimed system allows a driver to use a “driver identification” interface to “authenticate” herself, after which she will be allowed to operate the vehicle using her “operating profile,” *e.g.*, allowable speed, location, hours of operation. (*Id.*, 7:1-6, 6:63-67, Cl. 8, 5:56-58.) If the driver violates her profile, the system provides feedback, including by generating alarm signals and controlling vehicle operation. (*Id.*, Abstract, 7:6-22.)

This was not new at the time of the ’508. For example, US6,225,890 (EX1006) (“**Murphy**”) predates the ’508 by ***over a decade*** and discloses a ***near-identical*** “system for restricting use of a vehicle by a selected vehicle operator,” including high-risk drivers like “teenager[s].” (Murphy, Abstract, 3:20-40, 11:60-63.) In Murphy, (1) the driver provides “ident indicium” (*e.g.*, biometric samples, unique token or smart card, unique keypad code); (2) the system “identifies the driver” and allows her to operate the vehicle using the pre-defined “vehicle operation restrictions” imposed on her; and (3) if the driver does not operate the vehicle within such profile, an “alarm signal is transmitted” or “other appropriate control actions

are taken,” such as “reduc[ing] the vehicle speed.” (*Id.*, Abstract, 5:12-60, Fig. 6, 13:28-15:8, Fig. 7, 15:9-54; *see also* 15:66-16:11, 16:50-17:63.)

As another example, US2007/0168125 (EX1009) (“**Petrik**”) discloses a system with an “in-vehicle monitoring unit” for controlling operation of a vehicle. (Petrik, Abstract, [0016]-[0026].) A driver is issued a “smart card” with his fingerprint template. (*Id.*, [0017], [0022], [0025], [0069].) The driver inserts the card into a “smart card reader/writer and places his finger on the fingerprint reader to confirm his identity,” which “automatically logs him in.” (*Id.*, [0025], [0069].) The system sets driver operating parameters, such as maximum speed, “intended route plan,” and “required rest times.” (*Id.*, [0024]-[0025], [0028], [0030].) If these are violated, the system may “beep” to warn the driver and can interact with an “engine management system” to slow down, speed up, or disable the vehicle. (*Id.* [0025]-[0026], [0028], [0030].)

These references, alone or in combination with additional prior art, invalidate all challenged claims.

II. MANDATORY NOTICES (37 C.F.R. §42.8(A)(1))

A. Real Parties-in-Interest

The real parties-in-interest are Mercedes-Benz Group AG; Mercedes-Benz AG; Mercedes-Benz USA, LLC; and Mercedes-Benz Intellectual Property GmbH & Co. KG.

B. Related Matters

Assignee-of-record The Phelan Group, LLC asserted the '508 in the following proceedings:

- *The Phelan Group, LLC v. Toyota Motor Corp.*, No. 2-23-cv-00093 (E.D. Tex.), filed March 7, 2023, voluntarily dismissed with prejudice;
- *The Phelan Group, LLC v. Kia Corp.*, No. 2-23-cv-00094 (E.D. Tex.), filed March 7, 2023, voluntarily dismissed with prejudice;
- *The Phelan Group, LLC v. Honda Motor Co.*, No. 2-23-cv-00606 (E.D. Tex.), filed December 15, 2023, voluntarily dismissed with prejudice;
- *The Phelan Group, LLC v. State Farm Mutual Automobile Insurance Co.*, Case No. 2-23-cv-00611 (E.D. Tex.), filed December 18, 2023;
- *The Phelan Group, LLC v. Mercedes-Benz Group AG*, No. 2-23-cv-00607 (E.D. Tex.), filed December 15, 2023, transferred to N.D. Ga.;
- *The Phelan Group, LLC v. Mercedes-Benz Group AG*, No. 1-25-cv-01399 (N.D. Ga.), filed Mar. 17, 2025.

C. Counsel and Service Information

Lead counsel is Celine Crowson (Reg. No. 40,357). Backup counsel are Joe Raffetto (Reg. No. 66,218) and Scott Hughes (Reg. No. 68,385). Service information is as follows:

Post and Hand Delivery	Hogan Lovells US LLP
------------------------	----------------------

	555 13th Street N.W. Washington, D.C. 20004
Email	celine.crowson@hoganlovells.com joseph.raffetto@hoganlovells.com scott.hughes@hoganlovells.com
Telephone / Facsimile	202.637.5600 / 202.637.5910

III. NOTICE OF FEES PAID

Fees are submitted herewith. If additional fees are due during the proceeding, the undersigned authorizes the Office to charge them to Deposit Account No. 50-1349.

IV. CERTIFICATION OF GROUNDS FOR STANDING

Petitioner certifies that the '508 is available for *inter partes* review, and that it is not barred or estopped from requesting this review.

V. PRECISE RELIEF REQUESTED

Ground	References	Claims	Basis
1	Murphy	1-6, 8-11, 13-14	102/103
2	Murphy in view of Adams ¹	10	103
3	Murphy in view of Wu ²	7, 12	103

¹ “**Adams**” is US2008/0046739 (EX1010).

² “**Wu**” is US2008/0114501 (EX1011).

Ground	References	Claims	Basis
4	Petrik	1-6, 8-11, 13-14	102/103
5	Petrik in view of Schanz ³	1-6, 8-11, 13-14	103
6	Petrik (alone or as modified by Schanz) in view of Adams	10	103
7	Petrik (alone or as modified by Schanz) in view of Wu	7, 12	103

VI. '508 OVERVIEW

A. Background

The '508 is directed to a “driver authentication and safety system” for “monitoring and controlling vehicle usage by high-risk drivers.” ('508, Abstract.) An “authorized vehicle owner,” such as a “parent,” can create an “operating profile” for “high-risk drivers,” such as their “teen driver[s].” (*Id.*, 6:32-67, 2:27-31.) The operating profile, which can include restrictions like “maximum allowable vehicle speed,” “allowable vehicle location,” or “allowable hours of operation,” is enforced by an in-vehicle “driver authentication system” and “computer” associated therewith. (*Id.* at 2:26-44, 5:61-64, Fig. 6, Cls. 1, 8, 11.)

³ “**Schanz**” is DE10,323,723 (EX1007-1008). Citations herein are to the certified English translation (EX1008).

Drivers authenticate or identify themselves via a “driver identification” interface in the system, such as by presenting an “iButton, radio frequency identification device (RFID), etc.” (*Id.*, 6:57-62, Cls. 1, 11; *see also* 2:57-64.) Once authenticated, the system monitors operation of the vehicle, *e.g.*, using GPS providing “time of day, speed and location data associated with the vehicle,” and compares this to restrictions in the driver’s operating profile. (*Id.* at 2:62-64, 7:9-22.) If the driver violates her profile, the claimed system can provide feedback by, for example, generating an “audible alarm” or “control[ing]/govern[ing] operational aspects of the vehicle” like “lower[ing]/limit[ing] speed.” (*Id.*, 7:9-22, 2:40-44, Abstract.)

B. Prosecution

The ’508 was filed May 14, 2015 as a continuation of US9,045,101 (“’**101**”), filed April 8, 2013, which is a continuation of US8,417,415 (“’**415**”), filed July 1, 2009, and claims priority to Provisional Application No. 61/077,568, filed July 2, 2008. The ’508 received two Office Actions.

In the first Office Action, claims 1-20 were rejected over claims 1-11 of the ’415 for double patenting. (EX1002, 121-125.) Applicant amended claims 1-15 and 17-20 to remove “driver authentication” from the preamble and replace the words “master control unit” and “slave control unit” with, respectively, “driver

authentication system” and “at least one computer associated with the driver authentication system.” (*Id.*, 107-113.)

In the second Office Action, claims 1-14 were rejected over claims 1-11 of the ’415 and claims 1-18 of US9,493,149 (“’**149**”), and claims 15-20 were rejected over claims 15-20 of the ’101 for double patenting. (*Id.*, 77-85.) Claims 15-20 were also rejected under § 112 and under §102(a)(1) as anticipated by US2007/0158128 (“**Gratz**”). (*Id.*, 82-83.) Claim 16 was further rejected under 35 U.S.C. §103 as being unpatentable over Gratz in view of US2008/0319602. (*Id.*, 84.) Applicant filed a terminal disclaimer and cancelled claims 15-20, and a Notice of Allowance was issued. (*Id.*, 42-49, 58-65.)

C. Priority Date

Petitioner assumes, but does not concede, a priority date of July 2, 2008.

VII. CLAIM CONSTRUCTION AND POSITA

A. Claim Construction

Unless indicated otherwise, all claim terms herein are given the ordinary and customary meaning of such term as understood by one of ordinary skill in the art and the prosecution history pertaining to the ’508. 37 C.F.R. ¶ 42.100(b).

B. Definition of a Person of Ordinary Skill in the Art

A POSITA would have at least a bachelor’s degree in electrical engineering, computer engineering, computer science, or similar disciplines, and at least two

years of professional experience in the automotive industry with research, design, and/or development of automotive electrical and control systems, or an equivalent level of skill, knowledge, and experience. (Declaration of Dr. Mark Ehsani (EX1004) (“**Ehsani**”), ¶23.)⁴ The more education one has, the less experience needed to attain an ordinary level of skill. *Id.* Similarly, more experience in the field may serve as a substitute for formal education. *Id.*

VIII. ANALYSIS OF GROUNDS FOR UNPATENTABILITY

A. Ground 1 – Murphy Anticipates and Renders Obvious Claims 1-6, 8-11, 13-14

Murphy anticipates and renders obvious Claims 1-6, 8-11, 13-14. (Ehsani, ¶¶39-121.) Murphy was filed March 20, 1998, and issued May 1, 2001. Murphy is prior art under at least pre-AIA 35 U.S.C. §102(b).

1. Independent Claims

a) Claim 1

Murphy anticipates and renders obvious Claim 1. (Ehsani, ¶¶39-66.)

1[pre]: A *system comprising*:

To the extent limiting, Murphy discloses Claim 1[pre]. (Ehsani, ¶40.)

Murphy discloses “[a] **system** for restricting use of a vehicle by a selected

⁴ Dr. Ehsani is an expert in automotive control systems, among other things.

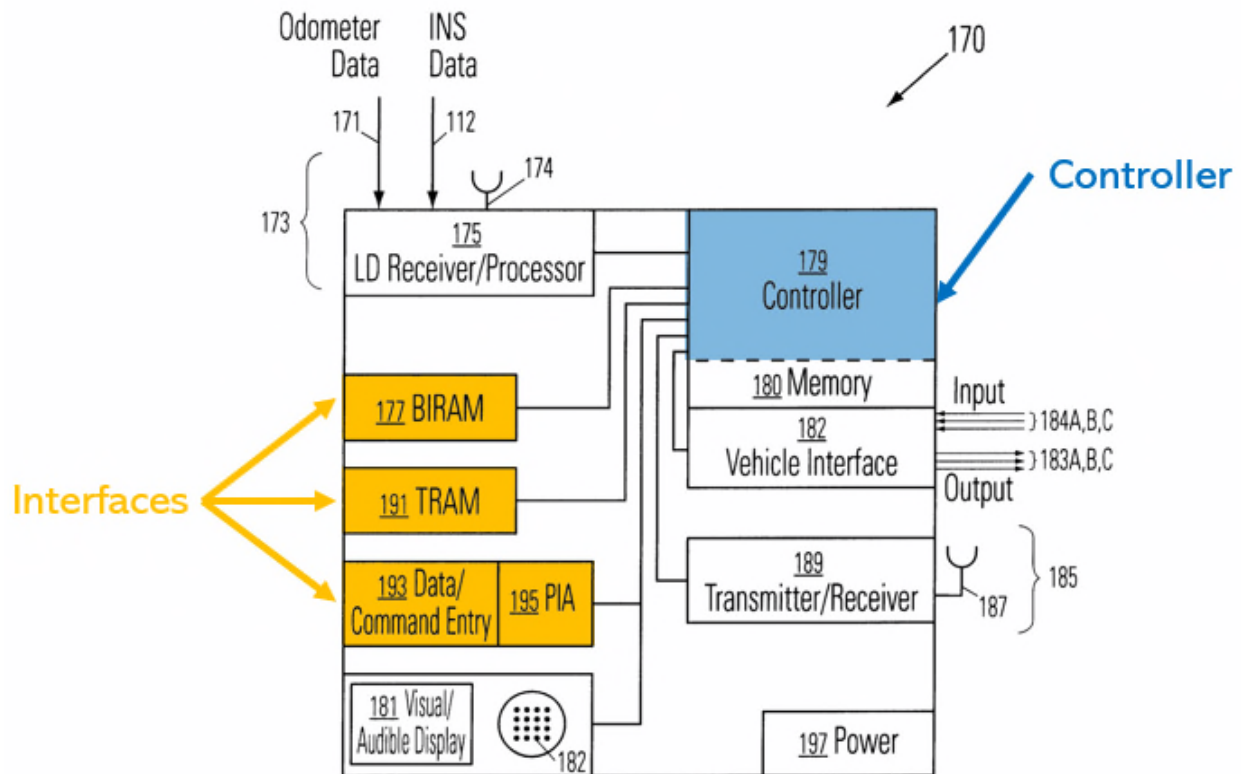
vehicle operator.” (Murphy, Abstract.)⁵ The system can be “installed in a vehicle dashboard or elsewhere” and “used to monitor operation of the vehicle by a teenager or other inexperienced driver, with restrictions imposed upon... vehicle maximum speed...,” among other things. (*Id.*, 15:1-8, 11:60-64; *see also* Fig. 1, Figs. 6-7.) *See also infra* Ground 1, Claim 1[A].

1[A]: a driver authentication system for authenticating at least one driver via a driver identification interface,

Murphy discloses Claim 1[A]—that is, a system for “authenticating” drivers via a “driver identification” interface. (Ehsani, ¶¶41-46.)

Murphy’s “driver authentication system” (such as shown in Figure 6 below) comprises a “controller” that can “authenticate” drivers via multiple interfaces, including: (1) “biometric indicium receiving and analysis mechanism” (BIRAM); (2) “token receiving analysis mechanism” (TRAM) and “token or smart card”; and (3) “data entry module” (*e.g.*, keypad) and “personal information analysis (PIA) module”:

⁵ All emphasis added unless otherwise indicated.



(Murphy, Fig. 6 (annotated), 13:28-42, 14:46-65, 6:55-7:14; *see also* Fig. 7, 15:8-31, 7:24-29.)

When a driver “turn[s] on the ignition,” Murphy’s system prompts the driver to “provide[] a sample of his/her ident indicium (a biometric indicium and/or token or keypad entries).” (*Id.*, 7:49-54, Fig. 2, Abstract.) The BIRAM can receive a driver’s “thumbprint, fingerprint, handprint, partial or full facial image, retina, iris, voice sample, cursive signature, blood vein pattern, blood sample or other suitable biometric indicium.” (*Id.*, 4:39-5:12; *see also* 2:20-34, 16:50-17:2, Cl. 37.) The TRAM can receive a “token or smart card” with “personal information on the (putative) token holder and/or information on limitations under which the token

holder can operate a vehicle.” (*Id.*, 6:55-7:14, 14:46-61, 2:32-34, Cl. 38.) *See also infra* Ground 1, Claim 10. And the “data entry module” (*e.g.*, keypad) and PIA can receive “entry of information that is specific to and known to only the individual who presents the information,” such as a “coded sequence of characters.” (*Id.*, 7:15-24, 14:55-65, Cl. 39.)⁶

Murphy’s system uses the “information” obtained via the BIRAM, TRAM and token, and data entry module and PIA for “**authenticating** the identity of the presenter [*i.e.*, driver].” (*Id.*, 7:22-24.) This information is “sent to the controller module 179 and associated memory module 180” to determine the “identity of a vehicle operator who has presented the indicium.” (*Id.*, 13:36-40, 14:51-54, 14:62-65, Fig. 6; *see also* 15:8-54 (discussing such information being sent to controller through identifier module 201), Fig. 7 (depicting same).) Murphy further teaches that its controller can authenticate the driver by “**compar[ing]** [this] indicium **with stored indicia**,” such as from a “**database** with identities and matching indicia for one or more authorized drivers of the vehicle.” (*Id.*, 5:12-24, 15:8-21; *see also* 2:26-38, Fig. 2, 7:49-63, Fig. 3, 10:45-11:27, Fig. 6, 14:46-65, 15:55-16:11, 16:50-17:62.)

⁶ The BIRAM, TRAM and token, and data entry device and PIA can be used alone or in combination. (Murphy, 6:55-61, 7:22-24, Fig. 7, 15:9-15, Fig. 6, 13:28-42, 14:45-65.)

See also *infra* Ground 1, Claim 1[B].

1[B]: wherein the driver authentication system receives a unique identification code to permit the at least one driver to operate the vehicle within an operating profile associated with the at least one driver; and

Murphy discloses Claim 1[B]. (Ehsani, ¶¶47-56.)

In Murphy, different vehicle drivers can have different “operating profiles.” For example, drivers can be divided into different categories, including “restricted operators” (or ROs)⁷ and drivers who are “identified and authorized[] but not an RO,” and “[d]ifferent driving restrictions are imposed[] depending upon the category to which the operator belongs,” including on “permitted time intervals and permitted travel corridor(s) and speeds for travel.” (Murphy, 7:64-8:2, 2:35-53; *see also* 1:66-2:16, Fig. 2, 7:49-9:44, 5:18-26.) Drivers can also be assigned their own “*individualized*” driving restrictions, such as individualized restrictions limiting “maximum speed,” “geographic region” and “routes,” “maximum accumulated” mileage and time, and “time intervals” when the vehicle can be driven. (*Id.*, 6:8-17, 17:14-29; *see also* 15:66-16:11, 17:14-29, 6:55-7:14, Fig. 2, 8:29-53, Fig. 3, 10:45-11, Abstract, Cls. 3, 10.) Murphy discloses that these “operating profiles” for drivers can be stored in a “database” or “memory” in its system. (*Id.*, Fig. 6, 13:35-41, 14:51-

⁷ “Restricted operators” can include, among others, “very young drivers” and “very old drivers.” (Murphy, 17:3-13; *see also* 3:20-47, 11:60-67.)

54, 14:62-65, 15:55-16:11; *see also* 15:8-31 (discussing schedule module storing “limitations on operation for each authorized vehicle operator”), Fig. 7.)

Further, Murphy’s system receives a “unique identification code” that allows drivers to operate the vehicle using their “operating profile.” For example, Murphy teaches its token (used with the TRAM) can be “*specific to the person* who presents” it; has “built into it a *circuit or pre-programmed information* in a storage medium that imposes selected restrictions on operation of the vehicle and/or *that identifies the token holder*”; and may rely upon “digitized data” that is “*encoded* or encrypted” and stored in its memory. (*Id.*, 6:55-7:14; *see also* 2:33-34, 14:46-54, Cl. 38.)

Similarly, when “identification indicium” is presented through the data entry device and PIA, “information *that is specific to* and known to only *the individual* who presents the information” is used, which can include a “*coded sequence* of characters...” (*Id.*, 7:15-24.) Finally, Murphy teaches that the BIRAM can receive “*samples* of an *ident indicium*” unique to the driver, such as, among other things, “a handprint,” “a full facial scan,” and “a voice sample analysis.” (*Id.*, Abstract, Cl. 37; *see also* 2:20-45, 4:39-5:28, 6:46-54, 15:55-16:28, 16:50-17:2, 17:63-18:19.)⁸

⁸ Murphy further teaches that after its identifier module receives “ident indicium” from the BIRAM, TRAM, or PIA, it will transmit the “ident information, *or a representation thereof*,” to the controller for comparison. (Murphy, 15:9-21.)

Murphy discloses that once a driver is authenticated using this information, *see supra* Ground 1, Claim 1[A], the system permits her to operate the vehicle in accordance with her corresponding profile. Specifically, when “[ident] indicum is satisfactorily presented and analyzed, the system allows operation of the vehicle” but will monitor “whether the vehicle location and/or speed are within ***permitted ranges for the driver*** and... whether the present time and/or accumulated time or mileage are within ***permitted ranges for the driver.***” (Murphy, Abstract, 8:28-49, Fig. 2; *see also* 2:46-53, 5:13-28, 6:55-7:14, 7:49-8:14, 8:54-61, Fig. 3, 10:45-11:19.) Murphy further teaches that its “controller” can receive the “***limitations*** on vehicle operation ***for each*** authorized vehicle ***operator***” and can use information it receives on the status of the vehicle (*e.g.*, location, speed, time) “for comparison... with any vehicle operation ***restrictions that may be imposed on an identified...***” driver. (*Id.*, 13:53-65, 14:46-65, 15:9-36; *see also* Figs. 6-7, 15:66-16:11, 17:14-29, 12:6-27.)

If Murphy’s controller determines the driver is not operating the vehicle within her “operating profile,” then “vehicle operation is temporarily disabled, or a coded alarm signal is transmitted, or other appropriate control actions are taken,” such as reducing vehicle speed. (*Id.*, Abstract, 5:29-60, Fig. 2, 13:53-14:17.) *See also infra* Ground 1, Claim 1[C].

1[C]: [i] at least one computer associated with the driver authentication system, said driver authentication system in communication with said computer and [ii] configured to monitor operation of the vehicle and generate a signal if the at least one driver violates the operating profile thereby providing feedback to the driver authentication system about usage of the vehicle, and [iii] wherein the driver authentication system cooperates with the at least one computer to control operation of the vehicle.

Murphy discloses Claim 1[C]. (Ehsani, ¶¶57-66.)

Murphy discloses multiple “computers” associated with its “driver authentication system.” For example, Murphy’s in-vehicle system has numerous “modules” (*e.g.*, computers) that are in communication with its controller, including (a) a “vehicle [or control action] interface module,” (b) a “visual and/or audible display [or feedback] module” and (c) a “telecommunication module”:

(1)...disabl[ing] the vehicle at a selected time so that the vehicle no longer operates... (2)...disabl[ing] use of selected vehicle accessories... (3)...reduc[ing] the vehicle speed to a selected speed range... (4)...forc[ing] the vehicle to operate only in selected lower gears... (5)...turn[ing] on at least one of the lights, exterior flashers and horn continuously or periodically... (6)...activat[ing] an on-board alarm the is visually or audibly perceptible to a person outside the vehicle... (7)...transmit[ting] an alarm (optionally silent) to a selected facility that is spaced apart from the vehicle... (8)...activat[ing] an air bag or other disabling device on the driver's side of the vehicle... (9)...allow[ing] the vehicle to operate for at most a selected cumulative time interval... (10)... allow[ing] the vehicle to operate only within one or more selected time intervals... (11)...allow[ing] the vehicle to operate for at most a selected cumulative vehicle mileage... and (12)...tak[ing] no action at that time but optionally log[ging] the activity and allow[ing] the driver to operate the vehicle without restriction for a selected time interval.

(Murphy, 5:13-54; *see also* 17:30-63, 6:1-18.)

Specifically, Murphy's controller will monitor "[i]nformation on the present vehicle location and/or vehicle speed and/or time and/or accumulated operating time

and/or accumulated mileage” and “**compar[e] this... with** any vehicle operation **restrictions that may be imposed on an** identified or unidentified vehicle **operator.**” (*Id.*, 13:53-61; *see also* 13:28-43, 14:18-22, Figs. 6-7, 15:9-16:11, 16:50-17:63, Cls. 1, 10, Abstract, 1:66-2:6, 2:20-53, Fig. 2 (depicting feedback loop used by system), 7:49-9:44 (discussing same), Fig. 3, 10:45-11:27.) Murphy’s vehicle (or control action) interface module, in turn, monitors vehicle operation, including for “information” from the controller as to whether the driver has violated any such operating restrictions (*e.g.*, her operating profile). (*Id.*, 13:66-14:17; *see also* Fig. 6, 15:9-54, Fig. 7.) If it receives such information, then it will “**control[] or restrict[] operation**” of the “vehicle component[s], such as vehicle engine, vehicle transmission system, vehicle fuel supply, vehicle power supply and accessories...,” that are connected to its “output terminals” and that are to be controlled (*e.g.*, based on the control action being taken). (*Id.*; *see also* 15:55-16:11, 16:50-17:63, Cls. 1, 10, Abstract, 2:20-53, Fig. 2, 7:49-9:44, Fig. 3, 10:45-11:27.)⁹

⁹ The vehicle (or control action) interface module is further configured to monitor vehicle operation by using its “input terminals” to monitor “components (doors, ignition, alarm system, vehicle cargo, accessories, etc.) whose activation may indicate that someone is preparing to drive the vehicle, which would activate a driver interrogation sequence.” (Murphy, 14:7-17, Fig. 6; *see also* Abstract, Fig. 3.)

Similarly, the “display [or **feedback**] **module**,” and “operations [vehicle activity] **log**” **module** (not shown above), monitor for signals from the controller as to whether the driver has violated (or will violate) her profile and can provide feedback to the system. For example, the vehicle activity log module is connected to the controller and used by it to record feedback on “vehicle location and speed,” including when a violation occurs, for “subsequent review and analysis if desired.” (Murphy, 5:53-54, 12:1-5, 15:42-54, Fig. 7.) *See also infra* Ground 1, Claim 11[C]. Similarly, the feedback module can “announc[e] or visually display[] an announcement that a violation has occurred...” (*Id.*, 5:29-60, 13:61-65, Fig. 6, 15:47-50, Fig. 7; *see also* 12:6-15 (discussing display providing feedback), 10:29-40 (same).) Moreover, the feedback module can further cooperate with the controller to control vehicle operation by making announcements **before** a violation occurs, such as that the “vehicle will become disabled within a selected time” if corrective action is not taken, and if the driver fails to take such corrective action, the controller will take appropriate control actions. (*Id.*; Ehsani, ¶63.)

Further, the controller can communicate with a “telecommunication module,” which includes “an antenna 187 and associated receiver/transmitter [] that exchanges information signals with an information processing facility,” when a driver violates her profile. (*Id.*, 14:23-45; *see also* Fig. 6, Abstract, 2:6-9, 12:16-27.) When the controller determines such a violation occurs, it can instruct the telecommunication

module to transmit a “selected **alarm signal**” (*e.g.*, feedback to the remote computer), which, in turn, can send signals and commands back to the telecommunication module and controller. (*Id.*, 5:13-60, Cl. 1, 14:23-45; *see also* Abstract, 17:30-63.) The controller will then cooperate with the telecommunication module and remote computer to control the vehicle, such as by implementing any new or modified driving restrictions that the telecommunication module receives from the remote computer. (*Id.*, 14:23-45; *see also* Cls. 7, 9, 12, 15, 18, Abstract, 12:16-27, 4:15-27.) *See also infra* Ground 1, Claim 3.¹⁰

In sum, Murphy’s controller, vehicle (or control action) interface module, display (or feedback) module, operations (or vehicle activity) log module, telecommunication module, and remote facility monitor vehicle operation and generate signals when the driver violates her operating profile (thereby providing feedback) *and* cooperate to control vehicle operation. (Ehsani, ¶¶58-66.)

¹⁰ For these same reasons, Murphy’s remote facility is also a “computer” associated and in communication with the in-vehicle system (*e.g.*, the controller); is configured to monitor vehicle operation and generate signals when a violation has occurred (thereby providing feedback to the system); and cooperates with the system to control vehicle operations. (Ehsani, ¶¶64-65.)

b) Claim 11

Murphy anticipates and renders obvious Claim 11. (Ehsani, ¶¶67-81.)

11[pre]: A system comprising:

To the extent limiting, Murphy discloses a system. (Ehsani, ¶68.) *See supra* Ground 1, Claim 1[pre].

11[A]: a driver authentication system in a motor vehicle for authenticating at least one driver via driver identification and associating an operating profile with the at least one driver;

Murphy discloses Claim 11[A]. (Ehsani, ¶¶69-72.)

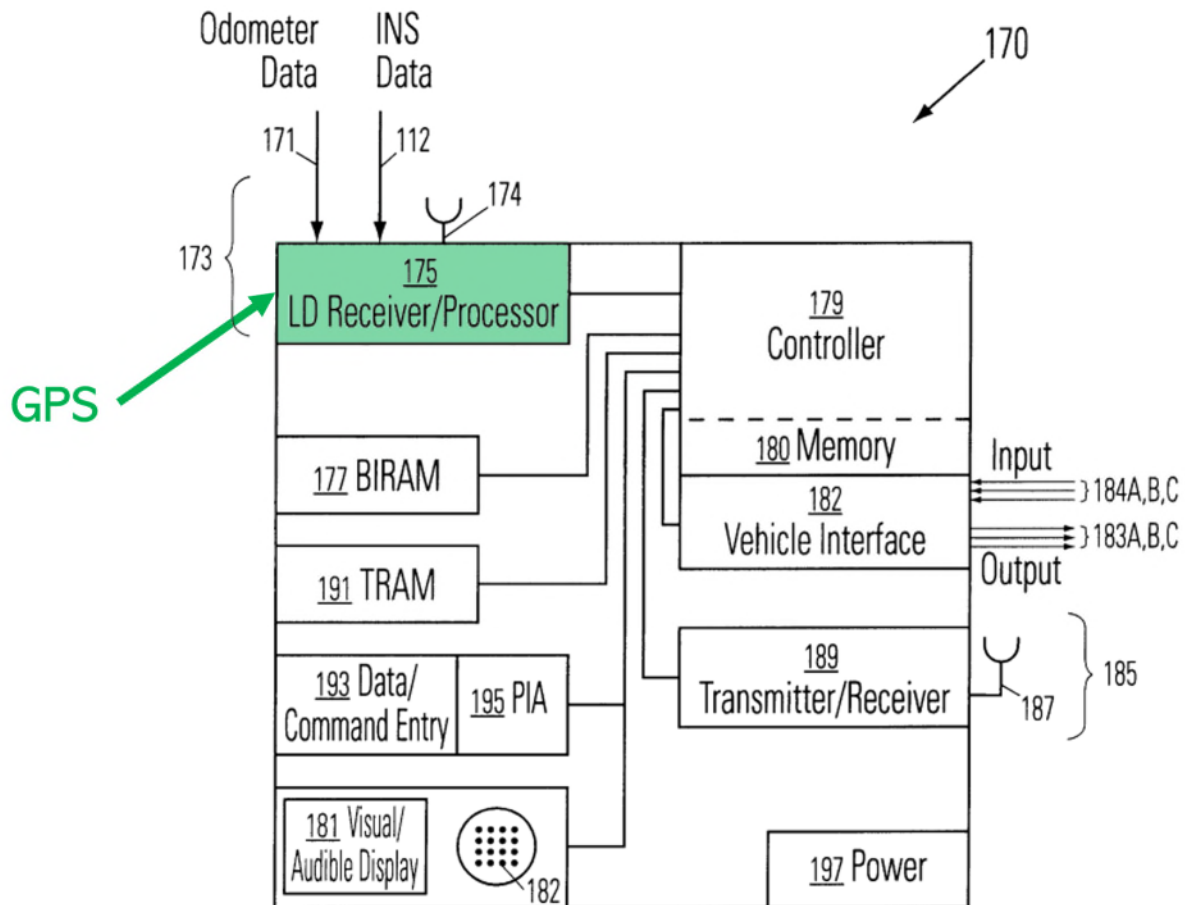
Murphy discloses a “driver authentication system” for “authenticating at least one driver via a driver identification interface.” *See supra* Ground 1, Claim 1[A]. This system is used in a “motor vehicle.” *Id.* (See also Murphy, Abstract, Fig. 1, 15:1-8, 19:3-12.) Moreover, the system “associate[s]” an “operating profile with the at least one driver.” *See supra* Ground 1, Claim 1[B].

11[B]: a GPS module providing at least location and speed information in association with movement of the motor vehicle; and

Murphy discloses Claim 11[B]. (Ehsani, ¶¶73-74.)

Murphy discloses a “location determination (LD) module” that is “part of an LD system, *such as GPS*, GLONASS, LEO, Iridium or LORAN, including an LD signal antenna [] and an LD signal receiver/processor connected to the antenna...” (Murphy, 3:48-64.) “When activated, the LD module [] *determines* the *present location, present speed...* and observation time... of the antenna [], and thus *of the*

vehicle...” (*Id.*) Murphy teaches the LD module can be integrated into its system and that “[i]nformation on... vehicle location and/or... speed and/or... time and/or accumulated operating time and/or... mileage is sent by the LD module 173 to the controller module 179” for use in determining whether to take control actions:



(Murphy, Fig. 6 (annotated), 13:28-65; *see also* Abstract, 14:23-45, Fig. 7, 15:32-54, 3:64-4:38, Fig. 5, 13:11-26, Cls. 1, 10, Fig. 2, 7:49-9:44.)

11[C]: a data logging device recording vehicle operation data associated with use of the motor vehicle by the at least one driver including location and speed information from the GPS module;

Murphy discloses Claim 11[C]. (Ehsani, ¶¶75-77.)

Murphy's system can include "an **operations log, including periodic recording of the present** observation time, **vehicle location and/or vehicle speed in a memory...**" (Murphy, 12:1:5; *see also* Fig. 6, 13:53-15:65, 14:18-22.) This operations (or vehicle activity) log allows the vehicle location and speed from the LD module to be stored for "subsequent review and analysis if desired" (including when the driver violates her profile), and, using a "data transfer module," to be "copied from or removed from the system for subsequent analysis or storage." (*Id.*, 15:42-54, Fig. 7, 5:52-54; *see also* 15:66-16:11.) As another example, GPS "vehicle location and selected status parameters" can be stored in a remote "base station" for use in determining whether to take actions remotely (such as modifying or adding new restrictions). (*Id.*, 4:15-27, 1:66-2:24, 16:30-49.)

11[D]: wherein said driver authentication system is coupled to at least one computer associated with the motor vehicle, and is configured to monitor operation of the motor vehicle and generate a signal to the driver authentication system if the at least one driver violates the operating profile, and wherein the driver authentication system cooperates with the at least one computer to control operation of the vehicle;

Murphy discloses Claim 11[D]. (Ehsani, ¶78.) *See supra* Ground 1, Claim 1[C].

11[E]: wherein the driver authentication system permits the at least one driver to operate the vehicle within an operating profile if the driver authentication system receives at least one of a unique identification code to permit the at least one driver to operate the vehicle within an operating profile and the at least one driver has not violated the operating profile.

Murphy discloses Claim 11[E]. (Ehsani, ¶¶79-81.)

Murphy's system "permits the at least one driver to operate the vehicle within an operating profile" after it receives a "unique identification code." *See supra* Ground 1, Claim 1[B]. Moreover, once a driver is authenticated, the system allows her to use the vehicle within her profile, so long as she does not violate the restrictions therein. *Id.* For example, if the driver violates her profile, or is "found to be unauthorized," the system can "(temporarily) disable[] the vehicle... so that the vehicle no longer operates, through fuel cutoff, brake disablement or some other similar measure." (Murphy, 5:17-67, 10:41-44; *see also* Abstract, 10:29-40.) *See also supra* Ground 1, Claim 1[C].

2. Dependent Claims

- a) **Claim 2: The system of claim 1, further comprising a database comprising a program module including at least one operating parameter associated with a vehicle, the program module remotely accessible by an authorized user to program an operating profile with respect to at least one driver, the program module accessed by the authorized user via a network utilizing a remote computer.**

Murphy anticipates and renders obvious Claim 2. (Ehsani, ¶¶82-87.)

Murphy's in-vehicle system includes a "database comprising a program

module,”¹¹ such as a “**database**” with “various limitations on vehicle operation” (*e.g.*, operating parameters), including on “geographic regions, corridors or routes where the vehicle may be driven, ...permitted time intervals during which the vehicle may be operated, ...permitted speed ranges for operation of the vehicle, and ...limitations on vehicle transmission ranges permitted for operation of the vehicle.” (Murphy, 15:9-31.) Murphy discloses that “[f]or each authorized driver... in the database..., information in... the following categories may be stored...: (1) name or other identifier; (2) corresponding ident indicium...; (3) schedule applicable to driver; (4) actual range of vehicle locations; (5) actual range of vehicle speed; (6) actual times of vehicle operation; (7) present ‘state’ of the vehicle...; and (8) corresponding Control Actions applicable to various circumstances.” (*Id.*, 15:66-16:11; *see also* 5:12-6:17.) *See also supra* Ground 1, Claim 1[C]. This “database” can be stored in its controller’s memory or in a schedule module. (*Id.*, 16:9-11; *see also* Fig. 6, 13:35-41, 14:51-54, 14:62-65, Fig. 7, 15:55-15:65.)

Murphy further discloses its database can be “programmed” remotely by an “authorized monitoring agency or person.” (*Id.*, 2:6-9; *see also* 7:40-48.)

¹¹ The ’508 broadly describes “program modules” as including “routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types.” (’508, 4:48-51.)

Specifically, Murphy teaches that “[t]he present invention allows downloading from a *remote facility to modify or add* to the extant *parameters* for vehicle operation or for vehicle driver identification, where the parameters are *included in the operating code, stored data* and the like.” (*Id.*, 14:40-45.) To do so, Murphy’s system includes a “telecommunication module 185... including an antenna 187 and associated receiver/transmitter 189 that exchanges information signals with an information processing facility... that is spaced apart” from the system. (*Id.*, 14:23-27, Fig. 6.) Murphy adds that using “[s]uitable telecommunication systems” (*e.g.*, networks), the remote facility can transmit “change or reprogramming signal[s]” that “modify, add or delete vehicle operation restrictions, for receipt by the apparatus [], and that allow downloading of commands that alter restrictions on present location, speed and/or present time, accumulated operating time and accumulated mileage items that determine the conditions under which a vehicle operation restriction is imposed.” (*Id.*, 14:27-40, Abstract; *see also* 12:16-27, Fig. 1, 16:12-50, 16:50-17:63, 4:15-27, Cls. 7, 9, 12, 15, 18.)

b) Claim 3: The system of claim 2, wherein the driver identification interface in conjunction with a remote computer loads the operating profile in the driver authentication system for the at least one driver.

Murphy anticipates and renders obvious Claim 3. (Ehsani, ¶¶88-96.)

Murphy’s in-vehicle system allows for “*downloading from a remote facility* to modify or add to the extant *parameters for vehicle operation or* for vehicle *driver*

identification.” (Murphy, 14:23-45; *see also* Fig. 6, 2:6-9; 7:40-48, Abstract, 12:16-27, Fig. 1, 16:12-50, 16:50-17:63, 4:15-27, Cls. 7, 9, 12, 15, 18.) As such, Murphy’s “driver identification interfaces” (*e.g.*, BIRAM, TRAM and token, and data entry device and PIA) work with its “remote computer” (*e.g.*, remote facility) in multiple ways to “load” a driver’s profile into the system.

First, the “remote facility” can transmit new “parameters for... **driver identification**” to the in-vehicle system, which the driver can use with the driver identification interface to authenticate herself and “load” her operating profile. (*Id.*, 13:28-15:8, Fig. 6; *see also* Abstract, Fig. 7, 15:8-54, Fig. 2, 7:40-8:53, 4:39-5:12, 6:55-7:14.) For example, if the in-vehicle system downloads a new “biometric indicium” like a new “facial image,” or a new “coded sequence of characters” for use with the data entry module, then the driver can use these new parameters from the remote computer to authenticate herself using the system’s BIRAM and data entry module, respectively, and use the vehicle. (Ehsani, ¶¶89-92.) *See also supra* Ground 1, Claim 1[A] (discussing driver providing “ident indicium” via driver identification interface to authenticate herself). Thereby, the system’s driver identification interfaces work in conjunction with the remote computer to load the “operating profile” of the driver. (Ehsani, ¶¶89-92.) *See also supra* Ground 1, Claim 1[B] (discussing system allowing driver to operate vehicle in accordance with profile loaded based on identity of driver).

Second, the “remote facility” can “**transmit signals** that modify, add or delete vehicle operation restrictions, for receipt by the [in-vehicle system], and that allow downloading of commands **that alter restrictions** on present location, speed and/or present time, accumulated operating time and accumulated mileage items **that determine the conditions under which a vehicle operation restriction is imposed.**” (Murphy, 14:27-37.) Once “download[ed]” to Murphy’s in-vehicle system, these “alter[ed] restrictions” would be stored in the operating profiles of the drivers whose restrictions are being altered. (*Id.*, 15:66-16:11, Fig. 6, 13:28-15:8, Fig. 7, 15:9-65, 16:50-17:62; Ehsani, ¶¶93-96.) *See also supra* Ground 1, Claim 1[B] (discussing system storing different operating for different drivers). In conjunction with this, when a driver whose restrictions were altered authenticates herself using a “driver identification interface” (*e.g.*, BIRAM, TRAM and token, and data entry device and PIA), the system will use the “operating profile” with the “alter[ed] restrictions” that were “download[ed]” from the “remote facility.” (Murphy, 15:66-16:11, Fig. 6, 13:28-15:8, Fig. 7, 15:9-65, 16:50-17:62; Ehsani, ¶¶93-96.) Thus, in this way, too, the system’s driver identification interfaces work in conjunction with the remote computer to load the “operating profile” of the driver. (*Id.*)

c) **Claim 4: The system of claim 1, further comprising: a GPS module; a memory module; and a function indicator module.**

Murphy anticipates and renders obvious Claim 4. (Ehsani, ¶¶97-106.)

Murphy's system includes a "GPS module." *See supra* Ground 1, Claim 11[B].

Murphy further discloses that its system includes a "memory module." For example, the in-vehicle system includes "controller 179 and **associated memory module 180**." (Murphy, 13:35-41, Fig. 6; *see also* 15:15-21 (discussing same controller with memory), Fig. 7 (depicting said controller).) Similarly, Murphy discloses that this memory and its system include a "**database** of authorized vehicle operators." (*Id.*, 15:15-21, 13:35-41, 14:51-54, 14:62-65; *see also* 15:66-16:11, 2:24-29, 4:39-5:16, 7:49-63, 10:45-57, 16:50-17:62.) Murphy further discloses that its system can include a "schedule module 211" (*e.g.*, memory) that "**contains** various limitations on vehicle operation and each authorized operator..." (*Id.*, 15:21-31, Fig. 7.) Finally, Murphy adds that its system can include other memories as well, such as in its token and in its operations log. (*Id.*, 6:55-7:14, 12:1-5; *see also* 16:30-49.)

Murphy discloses its in-vehicle system includes numerous "function indicator modules."¹² For example, Murphy's system, such as its controller, can monitor the

¹² The '508 broadly describes the "function indicator module" as a module that can "monitor various functions in association with the vehicle... such [sic] for example, power, fault detection and monitoring, and other functions." ('508, 8:4-7.)

functioning of the “location determination (LD) module.” (*Id.*, 13:11-26, Fig. 5; *see also* 3:64-4:14, Fig. 6, 13:28-52.) Specifically, the system “determines if sufficient LD signals of acceptable quality are being received so that the vehicle location can be determined,” and, if they are not, it can “take one or more of the 12 Control Actions.” (*Id.*) Similarly, the system can include an “inertial navigation system [INS] device... or similar **location indicating device**” that can monitor whether “LD [*e.g.* GPS] information is lost or corrupted,” and, if it is, can use its own “INS information” to “estimate the present location and/or speed and/or accumulated mileage.” (*Id.*, 4:28-38, 13:28-52.)

As an additional example, Murphy’s system can include a “vehicle interface module” with “one or more interface input terminals” for monitoring the functioning of certain “components (doors, ignition, alarm system, vehicle cargo, accessories, etc.) whose activation may **indicate** that someone is preparing to drive the vehicle.” (Murphy, 13:66-14:17, Fig. 6; *see also* Fig. 7 (depicting same as “control action interface module”), 15:37-54.) If the interface module receives an indication that any such component is being used, then it can “activate a driver interrogation sequence” requesting the driver to provide identification information. (*Id.*; *see also* Abstract,

Moreover, the ’508 broadly describes the term “module” as a “physical hardware component and/or a software module.” (*Id.*, 5:64-6:10.)

13:28-15:8, Fig. 2, 7:49-63.)

As another example, Murphy's system can include a "display system" which can be used to monitor how the vehicle has been functioning and indicate to the driver that "a violation has occurred and/or that the vehicle will become disabled" after a period of time if corrective action is not taken. (*Id.*, 10:29-40, 5:29-60.) For example, "[a]s the number of consecutive hours of vehicle operation approaches the specified limit" that the vehicle can be driven without a rest, "the driver can be advised, using a visually perceptible and/or audibly perceptible presentation device, that this specified limit is being approached" and "the vehicle can be disabled (or some other suitable penalty imposed) when this specified limit is exceeded." (*Id.*, 10:29-40; *see also* 12:6-15, Fig. 6, 13:61-65, Fig. 7, 15:47-50.)

As further examples of "function indicator modules," Murphy's system can include (1) "a vehicle odometer... or similar ***distance indicating device***" that monitors the distance traveled and can use this to supplement LD or GPS module information (*id.*, 13:44-44); (2) a BIRAM that can monitor how many times it has been used with "biometric indicium" that is not "legible/interrogatable" and take a "control action" after a "sequence of N consecutive" failed attempts (*id.*, 5:13-16, 6:19-39); and (3) a "governor" that can monitor "vehicle speed" to "reduce[] the vehicle speed to a selected speed range" (*id.*, 5:29-60, 6:8-17, 17:30-63).

- d) **Claim 5: *The system of claim 4, wherein the operating profile is loaded into the memory module for enabling controlled operation of the vehicle when the at least one driver is authenticated.***

Murphy anticipates and renders obvious Claim 5. (Ehsani, ¶¶107-10.)

Murphy discloses that different vehicle drivers can have different “operating profiles” loaded into the in-vehicle system’s “database” or “memory.” *See supra* Ground 1, Claim 1[B]. Murphy specifically teaches that the memory that the profiles are loaded into can be the “memory” of its “controller” (*e.g.*, the memory module). (Murphy, 13:35-41, 14:51-54, 14:62-65, Fig. 6, 15:15-21, Fig. 7, 15:66-16:11; see also 2:24-29, 4:39-5:16, 7:49-63, 10:45-57, 16:50-17:62.)¹³ Once a driver authenticates or identifies herself using the system, her corresponding profile loaded in the memory is used to control operation of the vehicle. *See supra* Ground 1, Claim 1[B].

In addition, Murphy’s system can include a “schedule module 211” (*e.g.*, memory) that contains the “various limitations on vehicle operation for each authorized vehicle operator.” (Murphy, 15:9-54, Fig. 7; *see also* 16:30-49.) Murphy teaches that this information, along with “ident information” of the “authorized drivers,” can be loaded into the “controller” (with its “memory unit”) to enable it to

¹³ “Operating profiles” can also be loaded into the system from the token. (Murphy, 6:55-7:14, 14:46-54, Abstract, 2:33-35, Cl. 20; Ehsani, ¶108.)

authenticate the driver and “determine[] which Control Action(s), if any, should be imposed on vehicle use.” (*Id.*)

- e) **Claim 6: *The system of claim 4, wherein the GPS module provides location information to the driver authentication system indicating a physical location of the vehicle.***

Murphy anticipates and renders obvious Claim 6. (Ehsani, ¶111.) *See supra* Ground 1, Claim 11[B].

- f) **Claims 8/13: *The system of claim [2/11], wherein [the/the operating profile comprises] at least one operating parameter [comprises/including] at least one of: a maximum allowable vehicle speed; an allowable vehicle location; allowable hours of operation; and seatbelt usage.***

Murphy anticipates and renders obvious Claims 8 and 13. (Ehsani, ¶¶112-13.)

Murphy’s operating profiles include parameters for at least “maximum allowable vehicle speed,” “allowable vehicle location,” and “allowable hours of operation.” For example, Murphy discloses its operating profiles include “***parameters for vehicle operation***” and that these parameters can include (a) “restriction to a selected maximum speed” (*i.e.*, maximum allowable vehicle speed), (b) “restriction to a selected geographic region” and “restriction to one or more specific routes” (*i.e.*, allowable vehicle locations), and (c) “restriction of vehicle operation to one or more selected time intervals during the day, or to selected days of the week” (*i.e.*, allowable hours of operation). (Murphy, 17:14-28, 14:40-45; *see*

also Abstract, 5:12-54, 11:60-67, 2:46-53, 6:8-17, Fig. 2, 8:5-67, 12:16-35, 15:66-16:11.) See also *supra* Ground 1, Claim 1[B].

- g) **Claims 9/14: The system of claim [1/11], wherein the driver authentication system generates an alarm signal for [remotely] alerting [said/the] authorized user when the at least one driver violates [the/said] operating profile.**

Murphy anticipates and renders obvious Claims 9 and 14. (Ehsani, ¶¶114-16.)

Murphy's in-vehicle system monitors whether a driver is operating the vehicle in accordance with her operating profile, and, if the driver violates her profile, the system can take numerous "control actions," including generating "alarm signals." See *supra* Ground 1, Claim 1[C]. For example, if the system determines the "present time" is not within the driver's "permitted time intervals" or the "vehicle present location and/or speed" is not within the driver's "permitted travel region or speed range," the system can (a) "**audibly announce[] or visually display[]** an announcement that a **violation has occurred...**" (e.g., alert the driver); (b) "**transmit[] a selected alarm signal to a selected facility** that is spaced apart from the vehicle" (e.g., alert the authorized person at the remote facility); and (c) "activate[] an on-board alarm the [sic] is visually or audibly perceptible **to a person outside the vehicle**" (that is, alert others). (Murphy, 5:13-60, Cl. 1; see also Abstract, 17:30-63, Cl. 20, 2:6-9, 4:15-27, 12:8-12, Fig. 6, 13:60-65, 14:23-45, Fig. 7, 15:37-50, 16:11-49.)

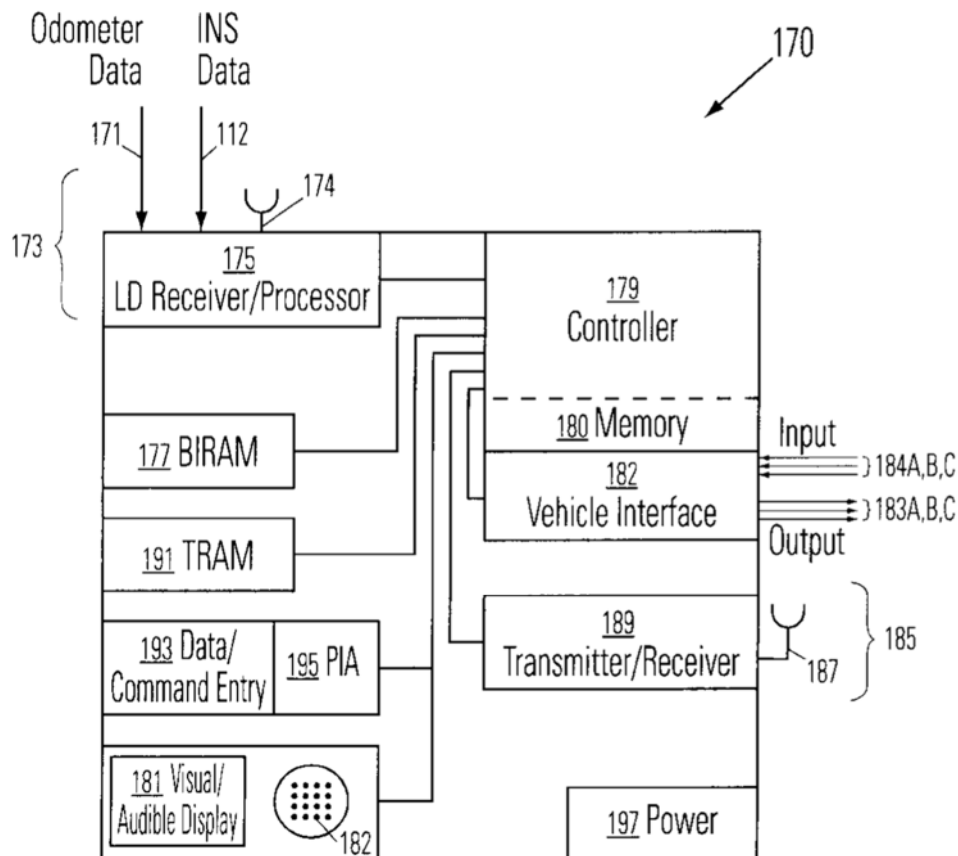
- h) **Claim 10: The system of claim 1, wherein the driver identification interface comprises at least one of: a portable handheld device; a radio frequency identification device; and a USB compatible device.**

Murphy anticipates and renders obvious Claim 10. (Ehsani, ¶¶117-21.)

For example, Murphy’s driver identification interface can include a “token or **smart card** (referred to collectively as a ‘token’).” *See supra* Ground 1, Claim 1[A]. The token may be “specific for the **person** who **presents** the token,” have “**built into it a circuit** or pre-programmed information in a storage medium that imposes selected restrictions on operation of the vehicle and/or that identifies the token holder,” and rely “upon digitized data stored in a flash **memory**, in a (re)programmable ROM or in similar information storage media.” (Murphy, 6:55-7:14; *see also* 2:33-34, 14:46-65, Cl. 38.) Murphy further teaches that the TRAM in the vehicle can accept “insertion or presentation” of the token. (*Id.*) Thus, as the token is a smart card with circuitry and memory that can be held and inserted or presented by a driver, it is both a “portable handheld device” and a “radio frequency identification device.” (Ehsani, ¶¶118-21.)

As an additional example, Murphy’s entire in-vehicle system, including the driver interface(s) therein, can be a “portable handheld device.” Specifically, Murphy teaches that “apparatus 170” shown below—which includes the “driver identification interfaces” (*e.g.*, BIRAM, TRAM and token, and data entry device and PIA)—can be “installed in the vehicle dashboard or elsewhere in the vehicle” or

“[a]lternatively... provided as a *stand-alone device* that communicates directly” with vehicle accessories. (Murphy, 15:1-8.)



(*Id.*, Fig. 6.)

B. Ground 2 – Murphy-Adams Renders Obvious Claim 10

Adams, filed August 16, 2006, and published February 21, 2008, is prior art under at least pre-AIA §102(e). Adams discloses a “smart card (SC)” and “smart card reader (SCR).” (Adams, [0001], [0022].) Similar to Murphy, Adams discloses that “smart cards” can be “contactless” and can “communicate with their smart card readers” wirelessly. (*Id.*, [0027].) Adams expressly discloses that such wireless

communication can be using “**radio frequency identification (RFID)**.” (*Id.*, [0027].)

It would have been obvious to a POSITA to apply this teaching to Murphy to have its token use RFID and thus be a “radio frequency identification device” as recited in Claim 11. (Ehsani, ¶¶125-27.) Such would have been the simple combination of well-known prior art elements according to known methods to yield predictable results. (*Id.*) Indeed, both Murphy and Adams teach that smart cards were known in the art and can communicate with an interface or reader wirelessly. (Adams, [0001], [0022]-[0030]; Murphy, 6:55-59, Abstract, 14:46-54.) Adams simply adds an express recitation that this wireless communication can be RFID. (Adams, [0027].) Applying this to Murphy, Murphy would operate in the exact same fashion—for example, authenticating or identifying drivers as it did before—only now its token (or smart card) would use the well-known RFID protocol to communicate with the TRAM when “present[ed]” to the TRAM. (Ehsani, ¶¶125-27.)

Moreover, both references provide teachings that would have led a POSITA to the combination, as they disclose that smart cards are used for “authentication” and to control access and describe smart cards in a similar fashion (*e.g.*, as handheld devices with circuitry, memory, and security features). (Adams, [0001], [0023]; Murphy, 6:55-7:14, 2:33-34, 14:46-65, Cl. 38.) A POSITA would have also been motivated to use RFID in Murphy’s token (or smart card), as taught by Adams, as

such would have provided the token with a standardized, established protocol that could be easily implemented to effectively enable wireless communications between the token and TRAM and that would obviate the need for a driver to insert her token into the TRAM. (Ehsani, ¶¶125-27.)

C. Ground 3 – Murphy-Wu Renders Obvious Claims 7/12

Murphy, including in view of Wu, renders obvious Claims 7 and 12. (Ehsani, ¶¶130-36.) Claims 7 and 12 simply add that the system includes certain well-known components ubiquitous to vehicles—specifically, that the “driver authentication system further comprises a power regulator module; a starter relay module; a definable relay module; a slave microcontroller; and an alarm synthesizer.” Each of these well-known components is disclosed or would have been obvious based on Murphy alone or, at minimum, based on Murphy in view of Wu. (*Id.*)

Wu, filed November 15, 2006, and published February 21, 2008, is prior art under at least pre-AIA §§102(a), (e). Wu discloses a vehicle control system with “a controller 20, a battery 40... an engine control module 60... a starter motor 80, a fuel pump 90, and an ignition circuit 100.” (Wu, [0020]-[0022], [0025]-[0027], Figs. 1-2.) Wu’s controller, like Murphy’s, controls vehicle operations, such as “starting” the vehicle and enabling or disabling the ignition, as well as additional “accessories” like lights. (*Id.*, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039].) These control operations are performed by using a processor in the controller to send signals to

“relays,” which activate or disable the different components. (*Id.*, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2.)

First, Murphy discloses and it would have been obvious for its system to include a “slave microcontroller.” (Ehsani, ¶¶130-36.) Murphy’s “controller module” is connected to its “vehicle interface module,” which “is in turn connected to at least one vehicle component... for use in controlling or restricting operation of the vehicle.” (Murphy, 13:53-14:17, Fig. 6, 15:32-54, Fig. 7.) As the “control actions” that the vehicle interface module takes (*e.g.*, what components it controls) are dictated to it by the controller module,¹⁴ the vehicle interface module is a “slave” to the controller module. (Ehsani, ¶¶130-36.) Moreover, when controlling other components (*e.g.*, “vehicle engine, vehicle transmission system, vehicle fuel supply, vehicle power supply and accessories”), the vehicle interface module will communicate instructions to them “according to serial data communications standards between **microcomputers in a vehicle**, as set forth in S.A.E. Documents J1708 and J1587.” (Murphy, 13:66-14:17.) Because these “microcomputers” of the components that are being controlled take the actions that the vehicle interface module instructs them to, they too are “slave microcontrollers.” (Ehsani, ¶¶130-36.)

¹⁴ The controller module itself can include a “specially programmed computer to carry out the tasks assigned to the controller module.” (Murphy, 14:18-20.)

Second, Murphy discloses and it would be obvious for its system to include an “alarm synthesizer.” (*Id.*, ¶130-36.) Murphy’s “display system” can include a “screen or monitor 181” and a “**loudspeaker** 182.” (Murphy, Fig. 6, 12:8-12, Fig. 7, 15:37-50.) When the controller module determines a driver has violated or will soon violate her profile, the display system (including the speaker) can synthesize, or electronically generate, an “audibly perceptible presentation to the driver,” such as an “**audibl[e]... announcement** that a violation has occurred and/or that the vehicle will become disabled...” (*Id.*, 15:47-50, 5:13-60; *see also* Cl. 1, 17:30-63, 13:60-65.) Similarly, Wu discloses this same type of audible alert can be done with a synthesizer, including an “operational amplifier” and “resistor,” and a POSITA would have readily understood this to be a common, simple way to implement Murphy’s audible alerts. (Wu, [0030]; Ehsani, ¶133.)

Third, Murphy discloses and it would have been obvious for its system to include a “power regulator module.” (Ehsani, ¶134.) Murphy’s system includes a “power supply 197” that regulates power, as it “supplies power to operate one or more of the components” in the in-vehicle system. (Murphy, 14:66-15:8; Ehsani, ¶134.) Moreover, Wu discloses it was “standard” to include a power (or voltage) regulating device in vehicle controllers, like Murphy’s, to “regulate the voltage level to 5V” or to levels the system “requires.” (Wu, [0020], [0022], [0027]-[0028].) It would have been obvious to a POSITA to include a voltage regulator in Murphy’s

system, as taught by Wu, including to ensure that Murphy's controller module receives the appropriate voltage it "requires" to operate. (Wu, [0020], [0028]; Ehsani, ¶134.) A POSITA would have understood this to merely be the use of a well-known, standard component to perform its intended function. (*Id.*, ¶134.)

Fourth, Murphy discloses and it would have been obvious for its system to include a "starter relay module." (Ehsani, ¶135.) Murphy's system includes an "ignition circuit," and if a driver is authenticated after providing "ident indicium" and is in compliance with her operating profile, then the system can "enabl[e]" this "ignition circuit," allowing the engine to be started. (Murphy, Abstract, 6:55-59, 8:10-14.) Further, Wu discloses a "starter relay" controlled by a processor in a controller to start the engine of a vehicle. (Wu, 0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2.) When the controller receives a command to start the vehicle, the processor can send a signal to initiate the starter relay, which will engage a starter motor and cause the engine to start. (*Id.*, [0025], [0027], [0031].) A POSITA would have been motivated to include such a "starter relay," as taught by Wu, in Murphy's system to provide a well-known, commonly-used mechanism for starting the engine. (Ehsani, ¶135.)

Fifth, Murphy discloses and it would have been obvious for its system to include a "definable relay module." (Ehsani, ¶136.) Murphy's "vehicle interface module" includes "interface output terminals" connected to other vehicle

components, and the vehicle interface module can use these to cause the activation of specific circuitry for defined periods of time, such as “turn[ing] on at least one of the lights, exterior flashers or horn continuously or periodically.” (Murphy, 5:29-60, 13:66-14:17, Fig. 6, 15:32-54, Fig. 7; Ehsani, ¶136.) In addition, Wu discloses that components such as the ignition system, lights, and accessories can be controlled by a processor sending a signal to a “defined relay” for such components. (Wu, 0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2.) A POSITA would have been motivated to use such definable “relays,” as taught by Wu, for such components in Murphy. (Ehsani, ¶136.) A POSITA would have understood using such “relays” in Murphy would have merely been the implementation of known components (relays) for their intended purpose and would have allowed the processor in Murphy’s controller module to selectively activate and deactivate the ignition, lights, and other accessories. (*Id.*)

D. Ground 4 – Petrik Anticipates and Renders Obvious Claims 1-6, 8-11, 13-14

Petrik anticipates and renders obvious Claims 1-6, 8-11, and 13-14. (Ehsani, ¶¶141-90.) Petrik was filed August 9, 2005, and published July 19, 2007. Petrik is prior art under at least pre-AIA §§102(a), (e).

1. Independent Claims

a) Claim 1

Petrik anticipates and renders obvious Claim 1. (Ehsani, ¶¶141-58.)

1[pre]: A system comprising:

To the extent limiting, Petrik discloses Claim 1[pre]. (Ehsani, ¶142.)

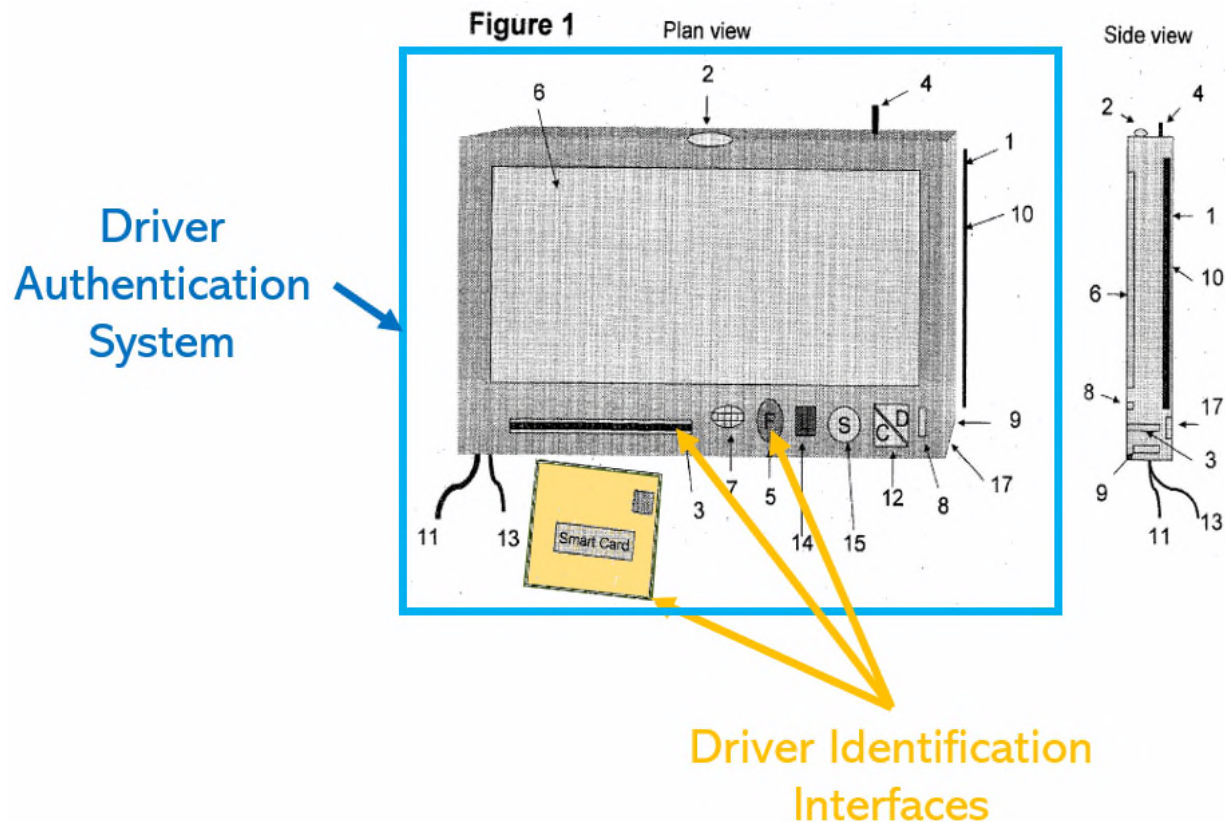
Petrik discloses a “GPS based vehicle monitoring, management and cruise control” system with an “in-vehicle monitoring unit.” (Petrik, Abstract, [0016]-[0025], [0030], Figs. 1-3.) *See also infra* Ground 4, Claim 1[A]. Drivers are issued “smart cards,” which are read by a smart card reader in the unit to confirm driver identity and allow operation of the vehicle within “vehicle and driver related operational parameters.” (Petrik, [0017]-[0018].) These parameters can include, for example, an intended “rout plan,” required “rest times,” and speed limits. (*Id.*, [0024]-[0026].) The in-vehicle unit is further connected to an engine management system, which is programmed to take instructions from it. (*Id.*, [0020], [0025]-[0026], [0030].)

1[A]: a driver authentication system for authenticating at least one driver via a driver identification interface,

Petrik discloses and renders obvious Claim 1[A]. (Ehsani, ¶¶143-45.)

In Petrik, an in-vehicle monitoring unit (*e.g.*, driver authentication system) is installed in a vehicle and includes a “micro computer, a GPS receiver module, a smart card reader/writer, a SATELITE/GPRS/GSM/BLEETOOTH module, a fingerprint verification module, a display, a beeper,... an engine management system connector and a battery charger integrated into a small, single, sealed unit.” (Petrik, [0016], [0069], Figs. 1-3.) To authenticate themselves, “[d]rivers are issued

with their logbook smart cards with their fingerprint template recorded in the card,” and the in-vehicle unit uses multiple interfaces—including (1) a “smart card reader/writer” and smart card and (2) a “fingerprint reader”—to “confirm [the driver’s] identity”:



(*Id.*, Fig. 1 (annotated), [0017], [0022], [0025], [0069].) See also *infra* Ground 4, Claim 10.

For example, “the driver inserts his smart card into the units’ smart card reader/writer and places his finger on the fingerprint reader to confirm his identity,” which “automatically logs him in as the current driver and enables engine ignition.” (*Id.*, [0025], [0069].) If an “invalid driver card and fingerprint combination is

presented,” the system does not authenticate the driver and the “engine will not start.” (*Id.*) *See also infra* Ground 4, Claim 1[B].

1[B]: wherein the driver authentication system receives a unique identification code to permit the at least one driver to operate the vehicle within an operating profile associated with the at least one driver; and

Petrik discloses and renders obvious Claim 1[B]. (Ehsani, ¶¶146-51.)

Petrik’s in-vehicle unit receives a “unique identification code” to permit a driver to operate a vehicle within an “operating profile” associated with that driver. For example, drivers are given “secure smart cards” with “their fingerprint template recorded in the card.” (Petrik, [0017], [0022], [0025].) Each fingerprint and fingerprint template would be unique to the driver and, therefore, be a unique code identifying such driver. (*Id.*; Ehsani, ¶¶147-48.) Prior to vehicle operation, “the driver inserts his smart card into the units’ smart card reader/writer and places his finger on the fingerprint reader to confirm his identity,” and the in-vehicle unit “automatically logs him in as the current driver and enables engine ignition.” (Petrik, [0025].) Again, if an “invalid driver card and fingerprint combination is presented,” the system does not authenticate the driver and the “engine will not start.” (*Id.*) That is, the engine is only started, and the driver is only allowed to operate the vehicle, when the proper smart card and fingerprint combination is received and the driver authenticated. (Ehsani, ¶¶148-49.)

Moreover, Petrik’s in-vehicle unit receives an “intended vehicle rout plan”

and calculates “required driver rest times” for the driver (*e.g.*, an operating profile associated with the driver). (Petrik, [0024]-[0026], [0028], [0030].) The “intended rout plan” limits the geographic locations the driver is allowed to go and is associated with the driver when it is loaded for the logged-in driver. (*Id.*, [0024]-[0026]; *see also* [0030] (indicating remote command center may be notified if driver diverts from “rout plan” and that the vehicle can be “disabled.”).) Similarly, the “required rest times” stored for the driver limit the number of hours and time the driver can operate the vehicle. (*Id.*, [0025], [0028].) The in-vehicle unit warns the driver when a rest break is due, and “confirms” rest start and stop times/locations to ensure driver compliance. (*Id.*, [0028], [0003]-[0006].)

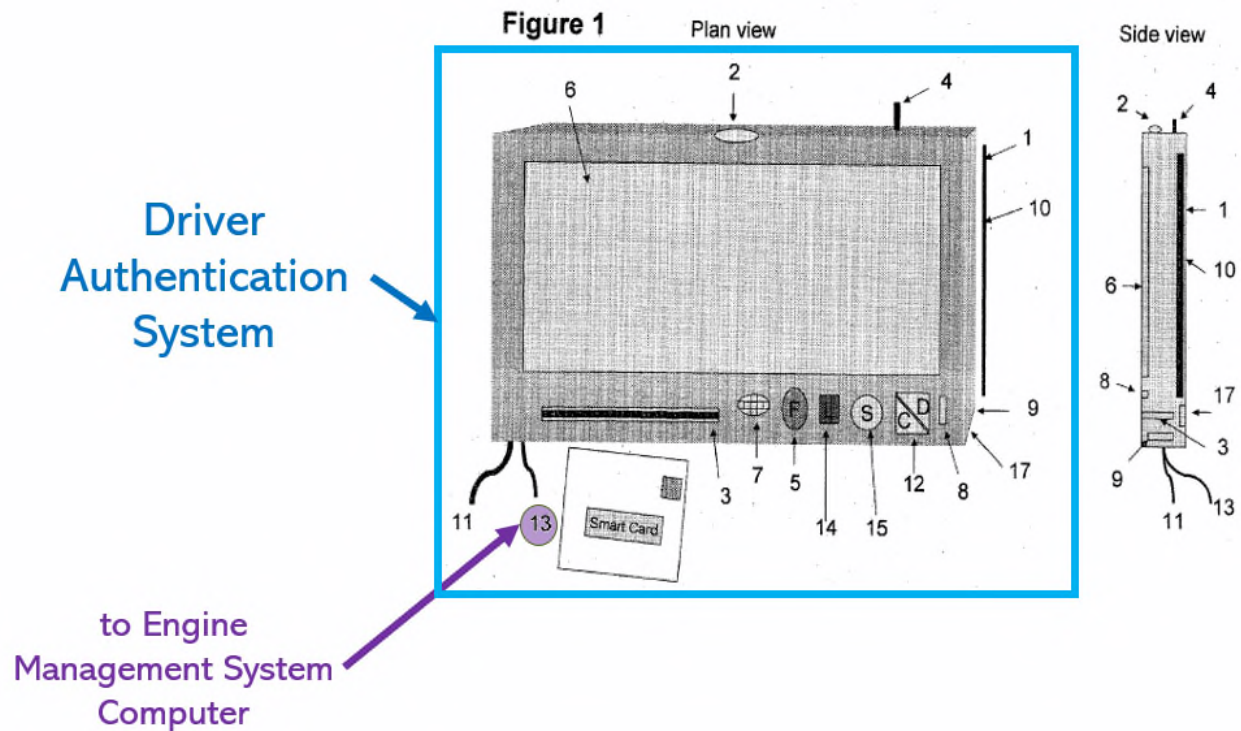
The operating profile further includes “speed zones” for the allowed “rout plan” and a “set absolute maximum speed.” (*Id.*, [0025]-[0026].) The driver is required to operate the vehicle within these operating profile speed limits. (*Id.*, [0024]-[0026], [0028], [0030]; Ehsani, ¶¶150-51.) For example, the system may “beep” to warn the driver of an upcoming speed “zone change,” indicating that the driver may need to slow down to stay within the speed limit. (*Id.*, [0025]-[0026].) The system can also provide “automated intelligent speed adaptation,” by using “geographically based speed location tables” to “interact[] with the engine management system to slow down or speed up the vehicle” to ensure the driver stays within speed limits. (*Id.*, [0025]-[0026].) The system can even “disable” the vehicle

by locking up the engine management system if a driver is “hostile” or “out of control,” including where the driver is trying to operate the vehicle outside of the allowed operating profile. (*Id.*, [0025]-[0026], [0028], [0030].) *See also infra* Ground 4, Claim 1[C].

1[C]: [i] at least one computer associated with the driver authentication system, said driver authentication system in communication with said computer and [ii] configured to monitor operation of the vehicle and generate a signal if the at least one driver violates the operating profile thereby providing feedback to the driver authentication system about usage of the vehicle, and [iii] wherein the driver authentication system cooperates with the at least one computer to control operation of the vehicle.

Petrik anticipates and renders obvious Claim 1[C]. (Ehsani, ¶¶152-58.)

Petrik discloses multiple “computers” associated with its in-vehicle unit (*e.g.*, driver authentication system). First, Petrik’s in-vehicle unit is associated with and connects to an “engine management system” computer through “engine management system connector” (13):



(Petrik, Fig. 1 (annotated), [0069]; *see also* [0016], [0020].) The in-vehicle unit and engine management computer communicate with each other, such as by the engine management computer being “programmed” to receive instructions from the in-vehicle unit and the in-vehicle unit receiving from the engine management computer data that it logs. (*Id.*, [0020]; *see also* [0016], [0018], [0025], [0032]; Ehsani, ¶¶153-56.)

Petrik’s in-vehicle unit is also configured to “monitor operation of the vehicle.” (*Id.*, ¶¶155-56.) For example, it “provides 24 hour a day 365 day per year monitoring of vehicle activity,” logs “operational parameters such as drivers’ work and rest time, vehicle location, vehicle speeds,” and records these parameters “on a secure smart card as well as in the vehicle units’ memory.” (Petrik, [0020], [0009],

[0018], [0025]; *see also* [0028] (indicating system logs information regarding driver rest breaks, including start and stop times and location.)) Petrik’s in-vehicle unit also “stores” data “logged by the engine management system.” (*Id.*, [0018], [0032].)

Petrik’s system can also “generate a signal if the driver violates the operating profile thereby providing feedback to the driver authentication system about usage of the vehicle.” (*Id.*, [0016], [0018], [0024]-[0026], [0028], [0030].) For example, Petrik’s system generates a signal causing the in-vehicle unit to “beep” to warn the driver when approaching a speed change zone, if the driver is not below the maximum speed limit for that zone, thereby providing feedback that the vehicle needs to be slowed down. (*Id.*, [0025]-[0026]; Ehsani, ¶¶155-57.) The in-vehicle unit is further provided with feedback regarding vehicle operation, as it gets a record of “the date, time, location and current actual speed of the vehicle” in the case of “speeding violations within each speed zone.” (Petrik, [0025]-[0026].) Similarly, the system receives a log regarding the driver’s rest breaks to confirm compliance. (*Id.*, [0028].)

Finally, the in-vehicle unit can “cooperate” with the engine management computer to “control operation of the vehicle,” including by interacting “with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits.” (*Id.*, [0025]-[0026].) Moreover, the two also cooperate by “locking up” the engine management system to disable and stop the

vehicle if a driver violates his operating profile and is considered “hostile” or “out of control.” (*Id.*, [0030].)

Petrik has additional “computers” associated with its in-vehicle unit (*e.g.*, driver authentication system) that, with the in-vehicle unit, monitor vehicle operation, generate a signal if the driver violates her profile (thereby providing feedback), cooperate to control vehicle operations. (Ehsani, ¶¶157-58.) For example, Petrik’s in-vehicle unit is in communication with a “base station” and a “Transport Management Command Centre” through SATELITE/GPRS/GSM two-way communications. (Petrik, [0030], Cls. 48-51.) Both the base station and Command Centre comprise computers, as they can receive and send communications over the SATELITE/GPRS/GSM, receive a “filed” route plan, and send “commands” to the in-vehicle unit. (*Id.*; Ehsani ¶¶157-58.) Petrik’s in-vehicle unit and the remote Command Centre monitor operation of the vehicle, including whether the vehicle is adhering to the “route plan.” (Petrik, [0030], [0010].) If the vehicle is not adhering to this, an alarm signal can be generated and sent from the in-vehicle unit to the Command Centre, and the Command Centre can send the in-vehicle unit a “disable” command. (*Id.*) This command not only provides feedback to the in-vehicle unit, but also controls operation of the vehicle, as it can be passed to the engine management system to “lock up” and stop the vehicle. (Ehsani ¶¶157-58.)

b) Claim 11

Petrik anticipates and renders obvious Claims 11. (Ehsani, ¶¶159-65.)

11[pre]: A system comprising:

Petrik discloses a system. (Ehsani, ¶160.) *See supra* Ground 4, Claim 1[pre].

11[A]: a driver authentication system in a motor vehicle for authenticating at least one driver via driver identification and associating an operating profile with the at least one driver;

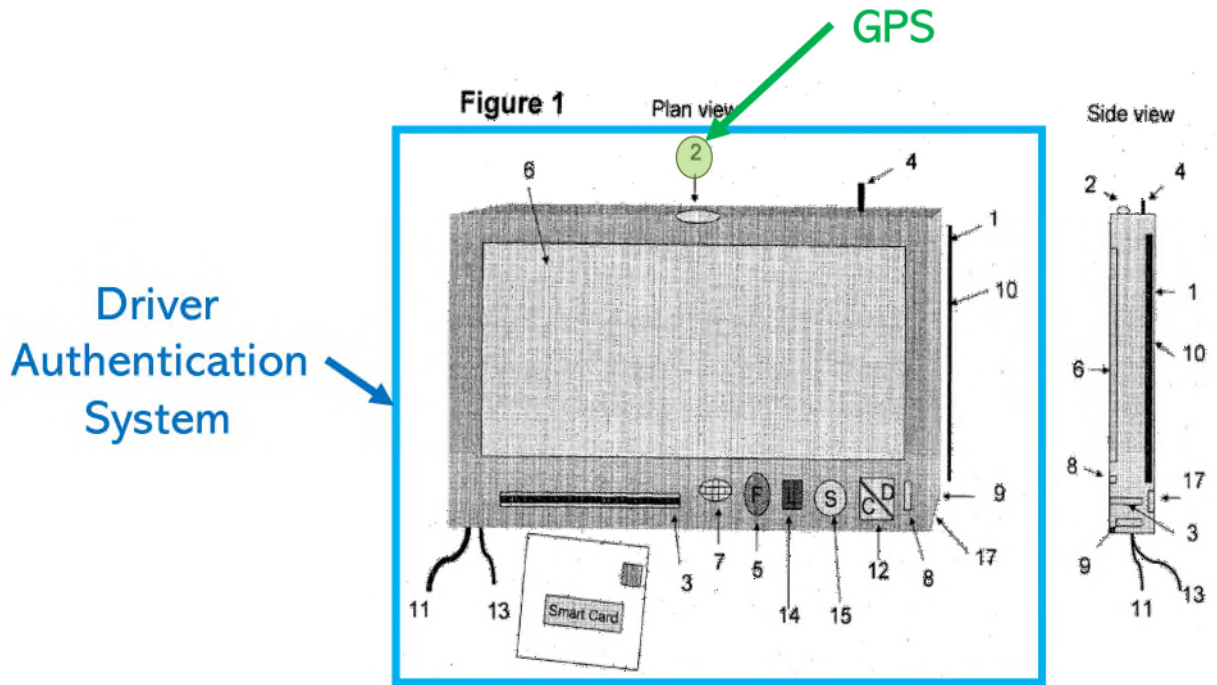
Petrik discloses Claim 11[A]. (Ehsani, ¶161.)

Petrik discloses a “driver authentication system” for “authenticating at least one driver via a driver identification interface.” *See supra* Ground 4, Claim 1[A]. Petrik’s system is used in a motor vehicle. *Id.* (*See also* Petrik, Abstract, Fig .1, [0016], [0020], [0069].) Petrik’s system also “associates an operating profile” with at least one driver. *See supra* Ground 4, Claim 1[B].

11[B]: a GPS module providing at least location and speed information in association with movement of the motor vehicle; and

Petrik discloses Claim 11[B]. (Ehsani, ¶162.)

Petrik’s in-vehicle unit includes a “GPS receiver module” (2):



(Petrik, Fig. 1 (annotated), [0016], [0018], [0025], [0069].) This GPS module provides location and speed information associated with movement of the vehicle to the in-vehicle unit, as it “keeps a constant log of the date, time, location, distance travelled and speed of the vehicle both in the units’ memory and in the smart card.” (*Id.*, [0025]-[0026], [0009], [0040].) The GPS information regarding vehicle speed and location used by the in-vehicle unit, which provides “GPS based cruise control” functionality including, for example, preventing the vehicle from exceeding a “set absolute maximum speed,” beeping to alert a driver of upcoming “speed zone” changes, and automatically speeding up or slowing down to “stay within appropriate speed limits in each zone” as the vehicle traverses the “rout plan.” (*Id.*, [0025]-[0026], [0030]; Ehsani, ¶162.)

11[C]: a data logging device recording vehicle operation data associated with use of the motor vehicle by the at least one driver including location and speed information from the GPS module;

Petrik discloses Claim 11[C]. (Ehsani, ¶163.)

For example, Petrik discloses that, “[d]uring the [driver’s] trip the GPS keeps a *constant log* of the date, time, location, distance travelled and speed of the vehicle both *in the units’ memory and in the smart card.*” (Petrik, [0025]; *see also* [0009], [0018].) Thus, both the smart card and in-vehicle unit’s memory are “data logging devices” that record GPS vehicle location and speed. (Ehsani, ¶163.)

11[D]: wherein said driver authentication system is coupled to at least one computer associated with the motor vehicle, and is configured to monitor operation of the motor vehicle and generate a signal to the driver authentication system if the at least one driver violates the operating profile, and wherein the driver authentication system cooperates with the at least one computer to control operation of the vehicle;

Petrik discloses Claim 11[D]. (Ehsani, ¶164.) *See supra* Ground 4, Claim 1[C].

11[E]: wherein the driver authentication system permits the at least one driver to operate the vehicle within an operating profile if the driver authentication system receives at least one of a unique identification code to permit the at least one driver to operate the vehicle within an operating profile and the at least one driver has not violated the operating profile.

Petrik discloses Claim 11[E]. (Ehsani ¶165.)

Petrik’s system “permits the at least one driver to operate the vehicle within an operating profile” after the system receives “a unique identification code.” *See supra* Ground 4, Claim 1[A]-1[B]. After the system authenticates the driver by

confirming her identity, the system allows operation of the vehicle within the driver's profile, so long as the driver does not violate restrictions therein. *Id.* For example, if the driver violates the profile, the system can “automatically speed up or slow down” the vehicle, and it can also “disable” the vehicle if a driver is “hostile” or “out of control.” (*Id.*, [0025]-[0026], [0028], [0030].) *See also supra* Ground 4, Claim 1[C].

2. Dependent Claims

- a) ***Claim 2: The system of claim 1, further comprising a database comprising a program module including at least one operating parameter associated with a vehicle, the program module remotely accessible by an authorized user to program an operating profile with respect to at least one driver, the program module accessed by the authorized user via a network utilizing a remote computer.***

Petrik anticipates and renders obvious Claim 2. (Ehsani, ¶¶166-169.)

Petrik's system includes a “Command Centre with an up to date database of road conditions” that includes operating parameters associated with a vehicle, such as “accidents, road closures, detours, adverse weather, etc.” (Petrik, [0010]-[0011], [0024], [0030], Cl. 49.) Petrik discloses that an authorized user (*e.g.*, dispatcher) at a dispatch, or base station, has access to the information in the Command Centre database via the SATELITE/GPRS/GSM link. (*Id.*, [0024], [0030], Cls. 49-51.) The dispatcher can use this information from the Command Centre database to program the operating profile of the driver. (*Id.*; Ehsani, ¶¶166-69.) For example, if the

dispatcher receives information regarding road closures or detours on an initial intended vehicle route from the database, the dispatcher could program a new intended route for the driver that accounts for this information. (Petrik, [0010]-[0011], [0024], [0030], Cls. 49-51; Ehsani, ¶¶166-69.) A POSITA would have understood, at the very least, that it would have been obvious for a dispatcher to create a new intended route plan upon receiving information from the database to avoid obstacles and more efficiently route the driver. (Ehsani, ¶¶166-69.)

Further, Petrik's "software program" in the in-vehicle unit is "upgradable," and includes a "table of the geographical location of every speed zone change as per the... road speed signs throughout the country." (Petrik, [0018]-[0019], Cls. 49-51.) It would have been obvious to a POSITA that an authorized user, such as a driver or dispatcher, could upgrade the software program with new speed limits by remotely accessing a database of speed zones. (Ehsani, ¶¶168-69.) A POSITA would have understood that this could be done, for example, by including current speed limits in the "up to date database of road conditions" at the Command Centre that can be accessed over the SATELITE/GPRS/GSM network communication link. (Petrik, [0010], [0018], [0024], [0030].) This would have allowed dispatchers to update the software program such that the table therein accounts for any new speed or changed limits. (*Id.*; Ehsani, ¶¶168-69.) A POSITA would have had a reasonable expectation of success in using the Command Centre database to remotely update speed limits

in the vehicle software program, as the Command Centre keeps “up to date” information on road conditions, and a speed limit can be considered such a road condition. (Ehsani, ¶¶168-69.)

b) Claim 3: *The system of claim 2, wherein the driver identification interface in conjunction with a remote computer loads the operating profile in the driver authentication system for the at least one driver.*

Petrik anticipates and renders obvious Claim 3. (Ehsani, ¶¶170-71.)

Petrik discloses that a “dispatcher” at a remote computer “files” the “intended rout plan” for the driver, which is part of the driver’s operating profile, in the in-vehicle unit using a “SATELLITE/GPRS/GSM” communication link. (Petrik, [0024], [0011], [0016]-[0018].) In addition, the “driver inserts his smart card into the units’ smart card reader/writer and places his finger on the fingerprint reader to confirm his identity.” (*Id.*, [0025], [0016]-[0018].) This “automatically logs him in as the current driver,” and “[s]imultaneously the monitoring unit displays the ‘filed’ truck [*e.g.*, vehicle] rout plan and a time chart showing the required driver rest times calculated from the drivers’ current work/rest status recorded on the smart card.” (*Id.*, [0025].) Thus, the smart card, smart card reader/writer, and fingerprint reader (*e.g.*, driver authentication interfaces), in conjunction with the remote computer used by the dispatcher, load the operating profile, including the “intended rout plan” and “required driver rest times,” into the in-vehicle unit. (*Id.*, [0024]-[0025]; Ehsani, ¶¶170-71.)

c) Claim 4: *The system of claim 1, further comprising: a GPS module; a memory module; and a function indicator module.*

Petrik anticipates and renders obvious Claim 4. (Ehsani, ¶¶172-78.)

First, Petrik discloses a “GPS module.” *See supra* Ground 4, Claim 11[B].

Second, Petrik’s system includes a “memory module,” as the in-vehicle unit includes a “memory,” and data and information can also be “recorded” on the smart card’s memory. (Petrik, [0009], [0017], [0018], [0035], [0069], Fig. 1; *see also* [0025], [0032], [0028].)

Third, Petrik’s system includes multiple “function indicator modules.” For example, Petrik’s system includes a “beeper” that beeps to alert the driver of a speed zone change such that the vehicle will need to be operated at a different speed, and interacts with the engine management system to slow or accelerate the vehicle if necessary. (Petrik, [0016], [0025], [0069], Fig. 1; Ehsani, ¶¶174-78.) As another example, Petrik’s system includes an “accelerometer” and GPS, which monitor functioning of the vehicle and can detect instances of “accidents” when there is a “sudden change of speed.” (Petrik, [0010], [0032].) When such an accident is detected, the system can automatically generate and send a report to the “Command Centre.” (*Id.*) The GPS and accelerometer also monitor when the vehicle stops moving and provide information regarding the duration of vehicle stops that is logged by the unit to ensure compliance with mandated rest periods. (*Id.*, [0019],

[0028].)

- d) **Claim 5: *The system of claim 4, wherein the operating profile is loaded into the memory module for enabling controlled operation of the vehicle when the at least one driver is authenticated.***

Petrik anticipates and renders obvious Claim 5. (Ehsani, ¶¶179-80.)

Petrik's operating profile, including the route plan, driver rest times, and speed restrictions, is loaded into the in-vehicle unit's memory when the driver is authenticated, thereby allowing controlled operation of the vehicle. (Petrik, [0011], [0024]-[0026].) For example, "[a]t the start of the journey the driver inserts his smart card into the units' smart card reader/writer and places his finger on the fingerprint reader to confirm his identity. This automatically logs him in as the current driver and enables engine ignition. Simultaneously the monitoring unit displays the 'filed' truck rout plan and a time chart showing the required driver rest times calculated from the drivers' current work/rest status recorded on the smart card. The engine will not start if the monitoring unit is disconnected or an invalid driver card and fingerprint combination is presented." (*Id.*, [0025].) Further, the confirmed driver can operate the vehicle within the operating profile, and the system provides alerts and can even slow down or disable the vehicle if the operating profile is violated. (*Id.*, [0025]-[0026], [0028], [0030].) *See also supra* Ground 4, Claim 4.

- e) **Claim 6: *The system of claim 4, wherein the GPS module provides location information to the driver authentication system indicating a physical location of the vehicle.***

Petrik anticipates and renders obvious Claim 6. (Ehsani, ¶181.) *See supra* Ground 4, Claim 11[B].

- f) **Claims 8/13: *The system of claim [2/11], wherein [the/the operating profile comprises] at least one operating parameter [comprises/including] at least one of: a maximum allowable vehicle speed; an allowable vehicle location; allowable hours of operation; and seatbelt usage.***

Petrik anticipates and renders obvious Claims 8 and 13. (Ehsani, ¶¶182-85.)

First, the driver's operating profile in Petrik includes an operating parameter of "maximum allowable vehicle speed." (Petrik, [0019], [0025]-[0026].) Petrik discloses the operating profile can include maximum speeds for different "speed zones," and warns the driver with a "beep" when approaching a speed change zone. (*Id.*) If the driver is not below the maximum speed limit for that zone, the system can interact "with the engine management system to slow down or speed up the vehicle to automatically stay within appropriate speed limits." (*Id.*, [0025].) In addition, Petrik discloses a "set absolute maximum speed" that the driver is not allowed to exceed. (*Id.*, [0025]-[0026].)

Second, Petrik's operating profile includes an operating parameter of an "allowable vehicle location," as it includes an "intended vehicle rout plan" for the

driver. (*Id.*, [0024]-[0025], [0011], [0030].) This route plan contains the allowable vehicle locations where the driver can travel. (*Id.*; Ehsani, ¶¶183-85.) If the driver “diverts inappropriately from the ‘filed’ route plan the unit notifies” the Command Center, teaching that the driver is only allowed to operate the vehicle along the intended route. (Petrik, [0030]; Ehsani, ¶¶183-85.)

Third, Petrik’s operating profile includes an operating parameter of “allowable hours of operation,” as the driver’s profile includes required “rest times” for the driver. (Petrik, [0003], [0009], [0025], [0028].) That is, the driver is only allowed to operate the vehicle for a certain number of hours before the driver is required to take a rest, and the system “warns the driver every time he is due to take a rest break.” (*Id.*, [0028], [0009], [0025]; Ehsani, ¶¶183-85.)

g) Claims 9/14: *The system of claim [1/11], wherein the driver authentication system generates an alarm signal for [remotely] alerting [said/the] authorized user when the at least one driver violates [the/said] operating profile.*

Petrik anticipates and renders obvious Claims 9 and 14. (Ehsani, ¶¶186-87.)

Petrik’s in-vehicle unit generates an alarm signal for remotely alerting an authorized user when the driver violates the operating profile. (Petrik, [0030].) In particular, the in-vehicle unit generates an alarm signal which “notifies” an authorized user at a “Transport Management Command Centre” via the unit’s “SATELITE/GPRS/GSM” communication link when a driver violates the operating

profile by “divert[ing] inappropriately from the ‘filed’ route plan.” (*Id.*)

- h) Claim 10: *The system of claim 1, wherein the driver identification interface comprises at least one of: a portable handheld device; a radio frequency identification device; and a USB compatible device.***

Petrik anticipates and renders obvious Claim 10. (Ehsani, ¶¶188-90.)

Petrik’s “driver identification interface” can comprise a “smart card.” See *supra* Ground 4, Claim 1[A]. This “smart card” has the driver’s “fingerprint template recorded in the card,” and at the “start of the journey, the driver inserts his smart card into the units’ smart card reader/writer and places his finger on the fingerprint reader to confirm his identity.” (Petrik, [0022], [0025], [0069], Fig. 1.) Thus, the “smart card” is a “portable handheld device,” as it contains information recorded thereon identifying the driver and is “inserted” by the driver into the smart card reader in the in-vehicle unit as part of confirming the driver’s identity. (Ehsani, ¶¶189-90.)

E. Ground 5 – Petrik-Schanz Render Obvious Claims 1-6, 8-11, 13-14

Petrik in view of Schanz renders obvious Claims 1-6, 8-11, 13-14. (Ehsani ¶¶191-207.)

1. Independent Claims

a) Claim 1

Petrik in view of Schanz renders obvious Claim 1. (Ehsani, ¶¶192-199.)

Petrik discloses Claim 1[pre]. See supra Ground 4, Claim 1[pre].

Petrik in view Schanz renders obvious Claim 1[A]-1[B]. Petrik discloses Claims 1[A]-1[B]. *See supra* Ground 4, Claims 1[A]-1[B].

In addition, regarding receiving a “unique identification code” for a driver and permitting the driver to “operate the vehicle within an operating profile associated with the at least one driver” based on this, Schanz, in the same field as Petrik, discloses a “driver authentication system” having a “device 1” including a “recognition device 3 which identifies the driver” using driver identification interfaces, including a “reading device for recognizing ***an identification code***” that identifies the driver. (Schanz, [0006]-0009, [0018]-[0020].)

After a driver is identified using the “recognition device,” *e.g.*, by Schanz’s reading device receiving the “identification code” identifying the driver, device 1 can check “whether special vehicle parameters 6 are stored for the respective driver 4” and, if so, the system “can assign individual vehicle parameters 6 to... driver 4, whereby the driving dynamic characteristics of the vehicle can be adjusted in relation to the driving skills of... driver 4.” (*Id.*, [0020]-[0022], *see also* [0006]-[0009], [0019], [0026].) Such “individual parameters” that can be assigned to each driver include, for example, “maximum power... and/or maximum torque... of the vehicle’s internal combustion engine and/or a maximum vehicle speed... and/or a maximum longitudinal... and/or transversal acceleration... and/or a [minimum] distance... to the vehicle driving ahead.” (Schanz, [0019]-[0022], [0006]-[0009],

[0026].)

It would have been obvious to modify Petrik to include an identification interface to read an “identification code” specific to a driver, as taught by Schanz — *e.g.*, the reading device for identifying a driver using an “identification code”—to authenticate drivers and assign them additional parameters. (Ehsani, ¶¶195-98.) A POSITA would have been motivated to add this “reading device” to Petrik, or to modify Petrik’s smart card reader to read smart cards that contain “identification codes” or smart cards with fingerprint templates, to provide alternative methods for authenticating drivers. (*Id.*) This would have given greater flexibility and allowed for authentication of drivers who do not have a smart card with a fingerprint stored therein, as well allow for additional customized parameters for different drivers. (*Id.*) A POSITA would have had a reasonable expectation of success, as Petrik and Schanz both disclose similar “driver identification” interfaces (Petrik, [0022]-[0025]; Schanz, [0006], [0018]; Ehsani, ¶¶195-98), and this addition would have simply been the use of a known driver identification interface for its intended purpose in a similar system, with Petrik continuing to operate in the same way as before, only with a reader (that could be a modified version of Petrik’s smart card reader) that now checks for “identification codes.” (Ehsani, ¶¶195-98.) This would have allowed, for example, different drivers with unique codes to be authenticated and allowed to operate a vehicle without requiring their fingerprints to first be

scanned. (*Id.*) *See supra* Ground 4, Claim 1[A].

Moreover, it would have been obvious to a POSITA to modify Petrik to include additional individual driver parameters specific to different drivers, such as maximum power, maximum speed, and minimum distance to other vehicles, as taught by Schanz in order to have more flexibility and to tailor parameters to driver skill. (Schanz, [0019]-[0022], [0006]-[0009], [0026]; Ehsani, ¶¶195-98.) A POSITA would have had a reasonable expectation of success, as Petrik's system already includes similar parameters such as maximum speed (Petrik, [0025]-[0026]), and including the additional driver-specific parameters of Schanz would have simply involved recording the additional driver-specific parameters (for example, based on skill level) in Petrik's in-vehicle monitoring unit. (Ehsani ¶¶197-98.)

Petrik discloses Claim 1[C]. (Ehsani, ¶161.) *See supra* Ground 4, Claim 1[C].

b) Claim 11

Petrik in view of Schanz renders obvious Claim 11. (Ehsani, ¶¶200-06.)

Petrik discloses Claim 11[pre]. *See supra* Ground 4, Claim 1[pre].

Petrik in view of Schanz renders obvious Claim 11[A]. (Ehsani, ¶202.) *See supra* Ground 4, Claim 11[A]; Ground 5, Claims 1[A]-1[B].

Petrik discloses Claim 11[B]. (Ehsani, ¶165.) *See supra* Ground 4, Claim 11[B].

Petrik discloses Claim 11[C]. (Ehsani, ¶166.) *See supra* Ground 4, Claim

11[C].

Petrik discloses Claim 11[D]. (Ehsani, ¶205.) *See supra* Ground 4, Claim 11[D].

Petrik in view of Schanz renders obvious claim 11[E]. (Ehsani, ¶206.) *See supra* Ground 4, Claim 11[E]; Ground 5, Claims 1[A]-1[C].

2. Dependent Claims 2-6, 8-10, 13-14

Petrik in view of Schanz renders obvious 2-6, 8-10, and 13-14. (Ehsani, ¶207.) *See supra* Ground 4, Claims 2-6, 8-10, and 13-14. As discussed, Petrik discloses the features of these claims, and Petrik, as modified as by Schanz, would continue to operate in the same way with the same components. (Ehsani, ¶207.) *See also supra* Ground 5, Claims 1, 11.

F. Ground 6 – Petrik (Alone or as Modified by Schanz) in View of Adams Renders Obvious Claim 10

Petrik (alone or as modified by Schanz) in view of Adams renders obvious Claim 10. (Ehsani, ¶¶208-10.) Adams discloses a “smart card (SC)” and “smart card reader (SCR).” (Adams, [0001], [0022].) Similar to Petrik, Adams discloses the smart card can be “inserted” into the smart card reader for reading the information on the smart card. (*Id.*, [0022]-[0027], Fig. 1; Petrik, [0025], Fig. 1).) Adams also discloses that “smart cards” can be “contactless” and can “communicate with their smart card readers” wirelessly using “**radio frequency identification (RFID)**.” (*Id.*, [0027].)

It would have been obvious to a POSITA to apply this teaching to Petrik to have its smart card use RFID, instead of requiring insertion, and thus be a “radio frequency identification device” as recited in Claim 11. (Ehsani, ¶¶208-10.) This would have been a simple substitution, as both Petrik and Adams teach that smart cards were known in the art and can communicate with an interface by being inserted into a smart card reader. (Adams, [0001], [0022]-[0030]; Petrik, [0025].) Adams simply teaches that a known alternative is to have a smart card reader that does not require physical insertion, but instead reads the same information from the smart card via RFID. (Adams, [0027].) Applying this to Petrik, Petrik would operate in the same fashion—for example, authenticating drivers as it did before—only now its smart card would use the RFID protocol to communicate with the reader, rather than requiring physical insertion. (Ehsani, ¶¶208-10.) At the very least, it would have been obvious to try, and a POSITA would have had a reasonable expectation of success, implementing Petrik’s smart card with RFID as taught by Adams, as using RFID is one known alternative to a smart card that is physically inserted into a smart card reader. (*Id.*, ¶¶208-10.)

**G. Ground 7 – Petrik (Alone or as Modified by Schanz) in View of Wu
 Renders Obvious Claims 7/12**

Petrik (alone or as modified by Schanz), including in view of Wu, renders obvious Claims 7 and 12. (Ehsani, ¶¶211-17.) Each of the well-known components recited in claims 7 and 12—“a power regulator module; a starter relay module; a

definable relay module; a slave microcontroller; and an alarm synthesizer”—is disclosed or would have been obvious based on Petrik (alone or as modified by Schanz) or, at minimum, based on these references in view of Wu. (*Id.*)

First, Petrik discloses and it would have been obvious for its system to include a “slave microcontroller,” as Petrik’s in-vehicle unit includes “a custom designed micro computer.” (Petrik, [0016].) Moreover, a POSITA would have understood Petrik’s “engine management system” to include a slave microcontroller, as the engine management system is “programmed” by instructions from the in-vehicle unit. (*Id.*, [0016], [0018], [0020]; Ehsani, ¶¶211-12.)

Second, Petrik discloses and it would have been obvious for its system to include an “alarm synthesizer,” as it includes a “beeper 7” that “beeps” to warn a driver. (Petrik, [0016], [0025]; Ehsani ¶213.) Such a “beeper” includes an alarm synthesizer to produce, or electronically generate, the beeping sound. (Ehsani, ¶213.) Moreover, Wu discloses a synthesizer, including an “operational amplifier” and “resistor,” can produce such beeping, and a POSITA would have understood this to be a common and simple way to implement beeper alerts in Petrik. (Wu, [0030]; Ehsani, ¶213.)

Finally, Petrik discloses and it would have been obvious to include in its system a “power regulator,” “starter relay,” and “definable relay.” Petrik’s in-vehicle unit has a “power connector,” and because the unit is an electronic component a

POSITA would have understood the system to have a “power regulator” to ensure the unit received a stable supply of the required voltage, including as taught by Wu. (Petrik, [0016], [0069], Fig. 1; Wu, [0020], [0022], [0027]-[0028]; Ehsani, ¶¶214-17.) Petrik further discloses the vehicle will not “start” unless the monitoring unit confirms a valid smart card and fingerprint, after which the engine ignition is “enabled.” (Petrik, [0025], Ehsani, ¶¶214-17.) Thus, a POSITA would have understood the system to include a “starter relay” as part of this process to start the engine and enable ignition, including as taught by Wu. (Wu, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039], Figs. 1-2; Ehsani, ¶¶214-17.) And, Petrik’s system can “speed up and slow down” or “disable” the vehicle, thus a POSITA would have understood Petrik’s system to include “definable relays” to assist in performing these functions, including as taught by Wu. (Petrik, [0025]-[0025]-[0026]; Wu, [0020]-[0021], [0025]-[0026], [0030]-[0031], [0039] (also indicating definable relays would be used to control accessories and the fuel pump), Figs. 1-2; Ehsani, ¶¶214-17.) Again, Wu expressly discloses each of these well-known components, and it would have been obvious in view of Wu to include a power regulator, starter relay, and definable relays in Petrik’s system. *See supra* Ground 3. This would have been the implementation of known vehicle components for their intended purposes, such that Petrik’s in-vehicle unit could operate, including with regulated power to the electronic components, and interact with components such as a starter relay and

ignition (definable) relay to selectively start and disable the vehicle. (Ehsani, ¶¶214-17.)

IX. DISCRETIONARY CONSIDERATIONS UNDER 314(A) AND 325(D) STRONGLY FAVOR INSTITUTION.

A. The *Fintiv* Factors Strongly Favor Institution.

The Board should institute review because Petitioner has been diligent in filing its Petition and the circumstances surrounding the parallel district court case do not warrant discretionary denial under §314(a). *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 11-21 (Dec. 1, 2020) (precedential) (citations omitted). The case was recently transferred to NDGA, and the Georgia court has not yet set an initial conference or issued a case schedule. Moreover, even before the transfer, the case was still in the early stages in EDTX. Little fact discovery had taken place (including no depositions); *Markman* proceedings had not yet commenced; and trial was not scheduled until February 2026 at the earliest.

B. *Advanced Bionics* Strongly Favors Institution.

Analysis under the framework from *Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH* demonstrates that denial under §325(d) is not appropriate. IPR2019-01469, Paper 6 at 8-9 (P.T.A.B. Feb. 13, 2020) (precedential). The grounds in this Petition are not the same or substantially the same as art and arguments raised during prosecution.

Under part one, the same or substantially the same art or arguments were *not*

previously presented to the Office, ending the inquiry in favor of institution. The “new, noncumulative prior art asserted in the Petition” strongly favors IPR. *Oticon Medical AB v. Cochlear Ltd.*, IPR2019-00975, Paper 15 at 20 (P.T.A.B. Oct. 16, 2019) (§§II.B and II.C precedential). Should PO attempt to analogize any previously considered art or arguments to those here, Petitioner reserves the right to respond.

The Board should institute review because the merits are strong and the circumstances here trigger none of the discretionary denial policy considerations. Should PO raise any discretionary denial theory not addressed above, Petitioner reserves the right to respond before institution.

X. CONCLUSION

For the reasons above, *inter partes* review and cancellation of claims 1-14 of US9,908,508 are requested.

Date: March 21, 2025

/s/ Celine J. Crowson

Celine J. Crowson (Reg. No. 40,357)

Joseph J. Raffetto (Reg. No. 66,218)

Scott Hughes (Reg. No. 68,385)

HOGAN LOVELLS US LLP

555 13th Street N.W.

Washington, D.C. 20004

Telephone: 202.637.5600

Facsimile: 202.637.5710

TABLE OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 9,908,508 (“ ’508 Patent ”)
1002	File History for the ’508 Patent
1003	Reserved
1004	Declaration of Dr. Mark Ehsani
1005	Curriculum Vitae of Dr. Mark Ehsani
1006	U.S. Patent No. 6,225,890 to Murphy (“ Murphy ”)
1007	German Patent Application Publication No. DE 10,323,723 A1 to Schanz (“ Schanz ”)
1008	English Translation of Schanz
1009	U.S. Patent Application Publication No. 2007/0168125 A1 (“ Petrik ”)
1010	U.S. Patent Application Publication No. 2008/0046739 to Adams (“ Adams ”)
1011	U.S. Patent Application Publication No. 2008/0114501 to Wu (“ Wu ”)

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing Petition for *Inter Partes* Review contains 13950 words, excluding those portions identified in 37 C.F.R. § 42.24(a), as measured by the word-processing system used to prepare this paper.

/s/ Celine J. Crowson
Celine J. Crowson
(Reg. No. 40,357)
Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105, the foregoing Petition for *Inter Partes* Review and exhibits thereto were served on March 21, 2025, by Overnight Courier at the following address of record and address known to Petitioner:

64064 - Ortiz & Lopez, PLLC P.O. BOX 4484 Albuquerque, NM 87196 United States	Ortiz & Lopez, PLLC 6605 UPTOWN BLVD NE 260 ALBUQUERQUE, NM 87196 United States
--	--

/s/ Jason A. Bradley
Jason A. Bradley