

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VOLKSWAGEN GROUP OF AMERICA, INC.,
Petitioner,

v.

LONGHORN AUTOMOTIVE GROUP LLC,
Patent Owner.

IPR2025-00925
U.S. Patent 8,085,192

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

	Page
I. Introduction.....	1
II. Statement of Precise Relief Requested.....	1
III. '192 Patent Overview	2
IV. The Prior Art.....	6
A. Background	6
B. <i>Fish</i>	11
C. <i>Ziv</i>	13
D. <i>Gehlot</i>	16
E. <i>Stevenson</i>	18
V. Level of Ordinary Skill.....	19
VI. Claim Construction.....	20
A. “a locational information module for determining” (Claims 1, 13, 19, 22).....	21
B. “an encryption module for encrypting” (Claims 1, 13, 19, 22)	22
C. “a storage module for storing” (Claims 13, 22)	22
D. “a removable storage module for storing” (Claims 1, 19)	23
E. “a processing module for sending” (Claims 1, 13, 19, 22) and “the processing module selectively decrypts” (Claims 3, 16)	24
F. “an input module disposed on the housing configured for receiving” (Claims 2, 15)	25
G. “a user verification module for verifying the identity of [the] user” (Claims 3-5, 16-18).....	27

H.	“a transmission module for transmitting” (Claims 12, 14, 22)	28
VII.	Ground 1: <i>Fish</i> (Claims 1, 11-14, 19-22)	29
A.	Claim 1	29
1.	[1pre] A location information device with secure data storage comprising:	29
2.	[1a] a housing;	31
3.	[1b] a locational information module for determining location information of the device, the determined location information being at least one route traveled by the device;	32
4.	[1c] an encryption module for encrypting the determined location information;	35
5.	[1d] a removable storage module for storing the encrypted location information, the removable storage module being removably disposed in the housing; and	38
6.	[1e] a processing module for sending the encrypted location information to the removable storage module removably disposed in the housing and retrieving the encrypted location information from the removable storage module.	39
B.	Claim 11	42
1.	[11] The device as in claim 1, wherein the location information further includes at least one of a home address, destination addresses and velocity of the device at predetermined times.	42
C.	Claim 12	44
1.	[12] The device as in claim 1, further comprising a transmission module for transmitting the encrypted location information to an external computing device.	44

D.	Claim 13	46
1.	[13pre] A location information device with secure data storage comprising:	46
2.	[13a] a housing;	46
3.	[13b] a locational information module for determining location information of the device, the determined location information being at least one route traveled by the device;	47
4.	[13c] an encryption module for encrypting the determined location information;	47
5.	[13d] a storage module for storing the encrypted location information; and	47
6.	[13e] a processing module for sending the encrypted location information to the storage module and retrieving the encrypted location information from the storage module.	47
E.	Claim 14	48
1.	[14] The device as in claim 13, further comprising a transmission module for transmitting the encrypted location information from the storage module to an external computing device.	48
F.	Claim 19	48
1.	[19pre] A system for controlling and storing location information comprising:	48
2.	[19a] a location information device with secure data storage comprising:	48
3.	[19b] a housing;	49
4.	[19c] a locational information module for determining location information of the location information device,	

	the determined location information being at least one route traveled by the location information device;	49
5.	[19d] an encryption module for encrypting the determined location information;.....	49
6.	[19e] a removable storage module for storing the encrypted location information, the removable storage module being removably disposed in the housing; and.....	49
7.	[19f] a processing module for sending the encrypted location information to the removable storage module removably disposed in the housing and retrieving the encrypted location information form [sic] the removable storage module; and	49
8.	[19g] a computing device comprising:	50
9.	[19h] a reader configured for reading the removable storage module of the location information device when [t]he removable storage module [i]s removably disposed in the reader; and.....	50
10.	[19i] a processor configured to execute a decryption program for decrypting the encrypted location information on the removable storage module removably disposed in the reader.....	51
G.	Claim 20	52
1.	[20] The system as in claim 19, wherein the location information further includes at least one of a home address, destination addresses and velocity of the device at predetermined times.	52
H.	Claim 21	52
1.	[21] The system as in claim 19, wherein the computing device further comprises a memory for storing a plurality of geographical maps and the processor is configured to overlay the location information on at least one of the plurality of geographical maps.....	52

I.	Claim 22	53
1.	[22pre] A system for controlling and storing location information comprising:.....	53
2.	[22a] a location information device with secure data storage comprising:	53
3.	[22b] a housing;	54
4.	[22c] locational information module for determining location information of the location information device, the determined location information being at least one route traveled by the location information device;	54
5.	[22d] an encryption module for encrypting the determined location information;.....	54
6.	[22e] a storage module for storing the encrypted location information;.....	54
7.	[22f] a processing module for sending the encrypted location information to the storage module and retrieving the encrypted location information from the storage module; and.....	54
8.	[22g] a transmission module for transmitting the encrypted location information from the storage module to an external computing device; and	55
9.	[22h] the external computing device comprising: a connectivity device configured for receiving the encrypted location information form [sic] the location information device; and	55
10.	[22i] a processor configured to execute a decryption program for decrypting the encrypted location information received from the location information device.	57
VIII.	Ground 2: <i>Fish In View of Ziv</i> (Claims 2-4, 15-17)	57

A.	Motivation to Combine <i>Fish</i> and <i>Ziv</i>	57
B.	Claim 2	62
1.	[2] The device as in claim 1, further comprising an input module disposed on the housing configured for receiving a code string input by a user, wherein the user inputted code string is used for encrypting and decrypting the location information stored in the removable storage module.....	62
C.	Claim 3	66
1.	[3] The device as in claim 1, further comprising a user verification module for verifying the identity of user of the device, wherein the processing module selectively decrypts the location information stored in the removable storage module based on the identity of the user.....	66
D.	Claim 4	69
1.	[4] The device as in claim 3, wherein the user verification module executes a password protection algorithm for verifying the identity of the user of the device.	69
E.	Claim 15	72
1.	[15] The device as in claim 14, further comprising an input module disposed on the housing configured for receiving a code string input by a user, wherein [t]he user inputted code string is used for encrypting and decrypted the location information stored in the storage module.	72
F.	Claim 16	72
1.	[16] The device as in claim 14, further comprising a user verification module for verifying the identity of [the] user of the device, wherein the processing module selectively decrypts the location information stored in the storage module based on the identity of the user.	72
G.	Claim 17	72

1.	[17] The device as in claim 16, wherein [t]he user verification module executes a password protection algorithm for verifying the identity of the user of the device.	72
IX.	Ground 3: <i>Fish In View of Ziv and Gehlot</i> (Claims 5-8, 18)	73
A.	Motivation to Combine <i>Fish</i> , <i>Ziv</i> , and <i>Gehlot</i>	73
B.	Claim 5	78
1.	[5] The device as in claim 3, wherein the user verification module further comprises an identity capture device for verifying the identity of the user of the device.	78
C.	Claim 6	80
1.	[6] The device as in claim 5, wherein the identity capture device is a biometric device.	80
D.	Claim 7	81
1.	[7] The device as in claim 5, wherein the identity capture device is a retinal scanning device.	81
E.	Claim 8	82
1.	[8] The device as in claim 5, wherein the identity capture device is a finger print reader.	82
F.	Claim 18	83
1.	[18] The device as in claim 16, wherein the user verification module further comprising an identity capture device for verifying the identity of the user of the device.	83
X.	Ground 4: <i>Fish, Ziv, Gehlot, and Stevenson</i> (Claims 9-10)	83
A.	Motivation to Combine <i>Fish</i> , <i>Ziv</i> , <i>Gehlot</i> , and <i>Stevenson</i>	83
B.	Claim 9	85

1.	[9] The device as in claim 5, wherein the identity capture device is a facial recognition reader.	85
C.	Claim 10	86
1.	[10] The device as in claim 5, wherein the identity capture device is a DNA detection device.	86
XI.	Discretionary Denial Is Not Warranted.....	86
A.	35 U.S.C. § 325(d) Denial Is Improper.....	86
B.	<i>Fintiv</i> Denial Is Improper.....	87
XII.	Mandatory Notices Under 37 C.F.R. § 42.8.....	89
A.	Real Parties-in-Interest.....	89
B.	Related Matters.....	89
C.	Lead and Back-Up Counsel.....	89
XIII.	Standing	90
XIV.	Conclusion	90

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH,</i> IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020).....	86, 87
<i>Amazon.com, Inc. v. Nokia Techs. Oy,</i> IPR2024-00799, Paper 9 (P.T.A.B. Jan. 8, 2025)	87
<i>Apple Inc. v. Fintiv, Inc.,</i> IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020).....	87, 88
<i>Becton, Dickinson & Co. v. B. Braun Melsungen AG,</i> IPR2017-01586, Paper 8 (P.T.A.B. Dec. 15, 2017)	86, 87
<i>CoolIT Sys., Inc. v. Asetek Danmark A/S,</i> IPR2021-01195, Paper 10 (P.T.A.B. Dec. 28, 2021)	88
<i>Microsoft Corp. v. Parallel Networks Licensing LLC,</i> IPR2015-00486, Paper 10 (P.T.A.B. July 15, 2015).....	87
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.,</i> 868 F.3d 1013 (Fed. Cir. 2017)	6
<i>Phillips v. AWH Corp.,</i> 415 F.3d 1303 (Fed. Cir. 2005)	2
<i>Rain Computing, Inc. v. Samsung Elecs. Am., Inc.,</i> 989 F.3d 1002 (Fed. Cir. 2021)	<i>passim</i>
<i>SharkNinja v. iRobot Corp.,</i> IPR2021-00545, Paper 11 (P.T.A.B. Sept. 8, 2021).....	87
<i>Sisvel Int’l S.A. v. Sierra Wireless, Inc.,</i> 82 F.4th 1355 (Fed. Cir. 2023)	3
<i>Williamson v. Citrix Online, LLC,</i> 792 F.3d 1339 (Fed. Cir. 2015)	<i>passim</i>

Statutes

35 U.S.C. § 102(b)	1
35 U.S.C. § 103	<i>passim</i>
35 U.S.C. § 112, ¶6	<i>passim</i>
35 U.S.C. § 311	1
35 U.S.C. § 325(d)	86

Other Authorities

37 C.F.R. § 42.8	89
------------------------	----

LIST OF EXHIBITS

Exhibit	Description
Ex-1001	U.S. Patent No. 8,085,192 (“the ’192 patent”)
Ex-1002	Declaration of William R. Michalson, Ph.D. (“Michalson”)
Ex-1003	Prosecution History of the ’192 Patent (“Prosecution History”)
Ex-1004	U.S. Patent No. 6,490,513 to Fish et al. (“ <i>Fish</i> ”)
Ex-1005	U.S. Patent Publication No. 2004/0103288 A1 to Ziv et al. (“ <i>Ziv</i> ”)
Ex-1006	U.S. Patent No. 6,310,542 to Gehlot (“ <i>Gehlot</i> ”)
Ex-1007	European Patent Application No. EP0962894 A2 to Stevenson et al. (“ <i>Stevenson</i> ”)
Ex-1008	U.S. Patent No. 4,114,155 to Raab (“ <i>Raab</i> ”)
Ex-1009	U.S. Patent No. 5,751,228 to Kamiya et al. (“ <i>Kamiya</i> ”)
Ex-1010	U.S. Patent No. 4,161,730 to Anderson (“ <i>Anderson</i> ”)
Ex-1011	International Publication No. WO 91/09275 to Kyrtos et al. (“ <i>Kyrtos</i> ”)
Ex-1012	International Publication No. WO 89/05255 to Whyntie (“ <i>Whyntie</i> ”)
Ex-1013	U.S. Patent No. 5,525,998 to Geier (“ <i>Geier</i> ”)
Ex-1014	Reissued Patent No. RE 35,920 to Sorden et al. (“ <i>Sorden</i> ”)
Ex-1015	U.S. Patent No. 5,416,712 to Geier et al. (“ <i>Geier II</i> ”)
Ex-1016	U.S. Patent No 5,777,580 to Janky et al. (“ <i>Janky</i> ”)
Ex-1017	U.S. Patent No. 5,508,931 to Snider (“ <i>Snider</i> ”)
Ex-1018	U.S. Patent No. 6,791,472 to Hoffberg (“ <i>Hoffberg</i> ”)

Ex-1019	Model Year 2005 Acura RL Navigation System User Manual (“ <i>Acura User Manual</i> ”)
Ex-1020	U.S. Patent No. 6,801,855 to Walters et al. (“ <i>Walters</i> ”)
Ex-1021	U.S. Patent No. 6,748,536 to Madau (“ <i>Madau</i> ”)
Ex-1022	U.S. Patent No. 7,212,989 to Taniguchi et al. (“ <i>Taniguchi</i> ”)
Ex-1023	U.S. Patent No. 5,926,546 to Maeda et al. (“ <i>Maeda</i> ”)
Ex-1024	U.S. Patent No. 6,950,013 to Scaman et al. (“ <i>Scaman</i> ”)
Ex-1025	Prosecution History of U.S. Patent Application No. 13/326,214
Ex-1026	Curriculum Vitae of William R. Michalson, Ph.D.

*All emphasis is added unless otherwise indicated.

I. Introduction

The '192 patent describes storing and retrieving encrypted location data. All recited components are admittedly conventional, from the “locational information module” (GPS unit), to the “encryption module” (known encryption algorithms), to the “storage module” (memory), to the “processing module” (processor). The patent illustrates each as a nondescript box.

The sole stated reason for allowing claims 1-22 was the limitation: “A removable storage module for storing the encrypted location.” Ex-1003, 143. This was doubly incorrect. First, only independent claims 1 and 19 recite a “*removable* storage module.” Independent claims 13 and 22 more broadly recite a “storage module.” Second, *Fish*, which was not before the Examiner, expressly discloses a removable storage module in the same manner as the '192 patent itself—e.g., secure digital (SD) memory.

Nothing described or claimed in the '192 patent was new or inventive as of its claimed priority date, September 6, 2005. Each of claims 1-22 should be canceled.

II. Statement of Precise Relief Requested

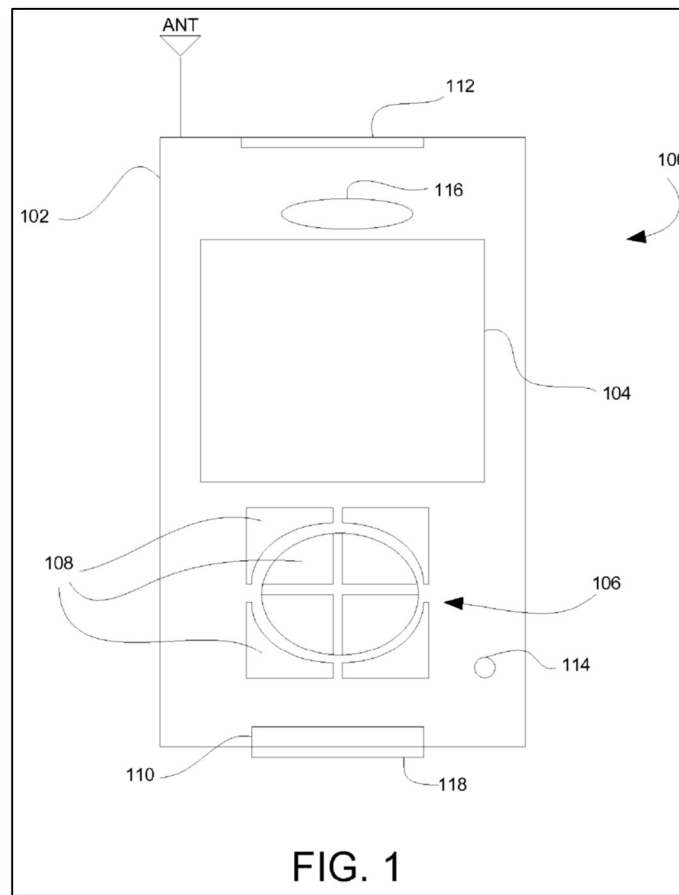
Petitioner requests review under 35 U.S.C. § 311 of claims 1-22 in view of the following grounds. Each reference is pre-AIA 35 U.S.C. § 102(b) prior art.

Exhibit	Prior Art
Ex-1004	U.S. Patent No. 6,490,513 to Fish et al. (“ <i>Fish</i> ”)
Ex-1005	U.S. Patent Publication No. 2004/1013288 A1 to Ziv et al. (“ <i>Ziv</i> ”)
Ex-1006	U.S. Patent No. 6,310,542 to Gehlot et al. (“ <i>Gehlot</i> ”)
Ex-1007	European Patent Application No. EP0962894 A2 to Stevenson et al. (“ <i>Stevenson</i> ”)

Ground	Challenged Claims	Basis	Prior Art
Ground 1	1, 11-14, 19-22	§ 103	<i>Fish</i>
Ground 2	2-4, 15-17	§ 103	<i>Fish</i> in view of <i>Ziv</i>
Ground 3	5-8, 18	§ 103	<i>Fish</i> in view of <i>Ziv</i> and <i>Gehlot</i>
Ground 4	9-10	§ 103	<i>Fish</i> in view of <i>Ziv</i> , <i>Gehlot</i> , and <i>Stevenson</i>

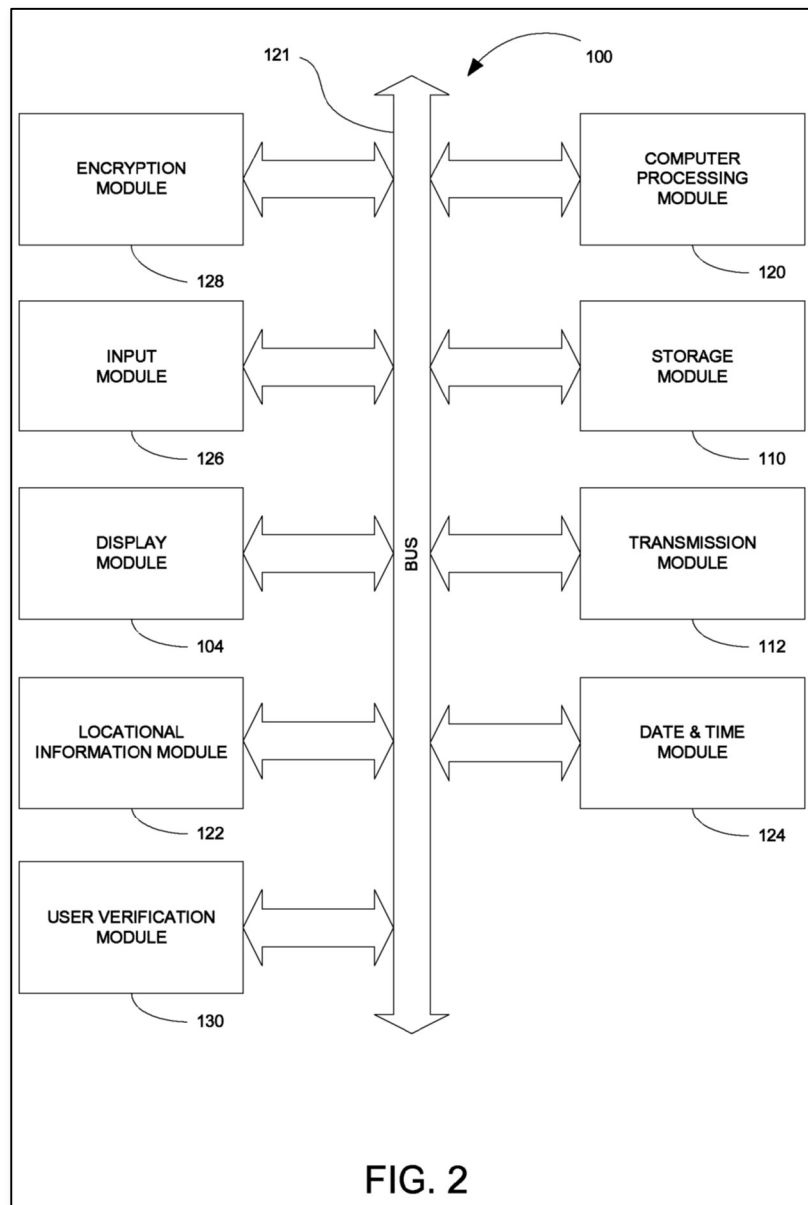
III. ’192 Patent Overview

The ’192 patent describes “navigational or positional information systems,” including “devices, systems and methods for controlling and storing sensitive information on a global positioning system (GPS) device.” Ex-1001, 1:15-19; Michalson, ¶54. Figure 1 illustrates a device 100—including housing 102, display module 104, input module 106, buttons 108, storage module 110, transmission module 112, microphone 114, speaker 116, and hardware interlock 118—for carrying out the disclosed steps:



Ex-1001, 3:7-24, Fig. 1.

The disclosed components—each a “module”—are shown in Figure 2 as boxes:



Id., Fig. 2, 3:25-27, 3:55-56, 4:2-7, 4:8-9, 4:16-18, 4:27-32, 4:47-54, 4:58-66. Each of these “modules” is disclosed as being a known, conventional component. For example, “GPS devices” are admittedly “ubiquitous,” GPS locational functionalities and memory storage abilities were known, and commercial providers are named. Ex-1001, 1:21-25, 3:56-62; Michalson, ¶¶57-59. Prior art

encryption and decryption algorithms are described as off-the-shelf tools, rather than a subject of innovation. Ex-1001, 4:60-66, 5:11-16; Michalson, ¶¶60-61.

Identity verification tools are also described as known, including “biometric device[s], such as a retinal scanning device, finger print reader, facial recognition reader,” and the patent “note[s] that identity detection devices such as biometric devices are common and are currently widely in use.” Ex-1001, 5:54-61, 5:62-64; Michalson, ¶62.

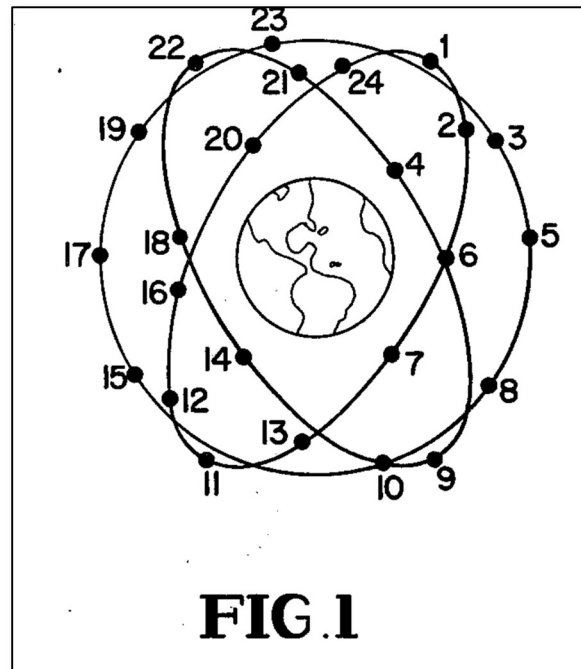
Rather than advance the state-of-the-art in GPS, encryption, user verification, or any other field, the ’192 patent teaches merely using these components for their known purpose. Michalson, ¶63. As discussed below regarding *Fish* and other references, these uses themselves were also prior art.

Prosecution of the ’192 patent included two substantive office actions, on September 9, 2010 and February 8, 2011. Ex-1003, 48-54, 88-96. After an Examiner interview on May 5, 2011, *id.*, 134, the Examiner allowed the claims on October 11, 2011, *id.* at 138-144. The sole stated reason for allowance was the recitation: “A removable storage module for storing the encrypted location . . .” *Id.*, 143. This statement appears incomplete, however, since independent claims 13 and 22 do not require “removable” storage.

IV. The Prior Art

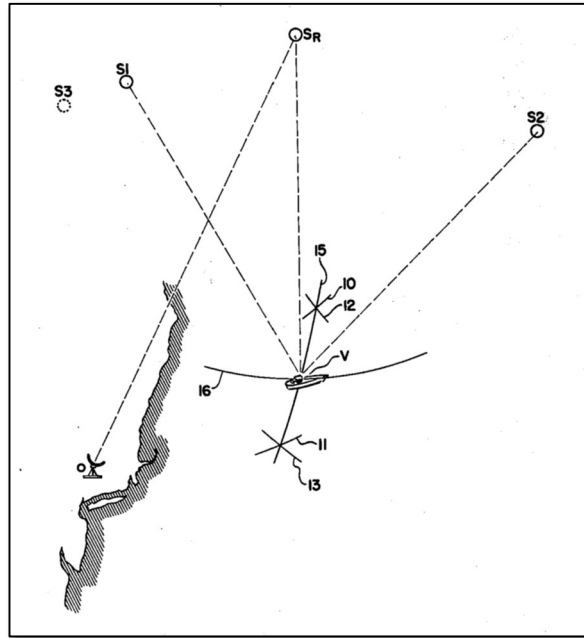
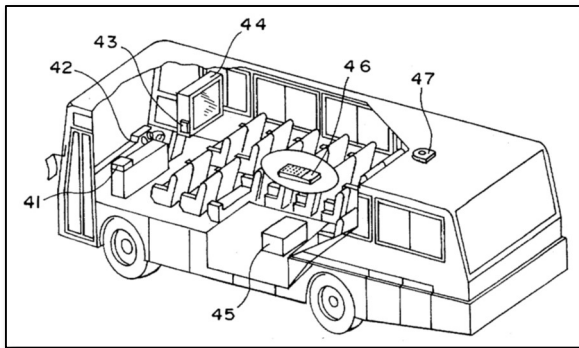
A. Background

As Dr. Michalson explains, GPS and encryption technologies were well known before the '192 patent. GPS began in the 1970s as a U.S. government-maintained, satellite-based system developed for civilian and military uses. Michalson, ¶65. An early example is shown below, with 24 orbiting spacecraft:



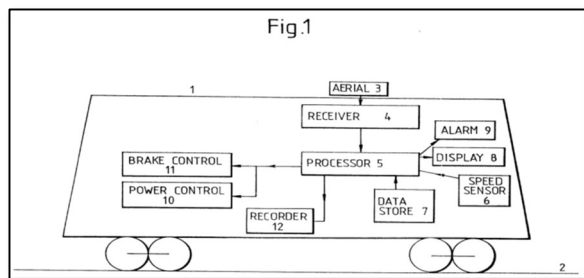
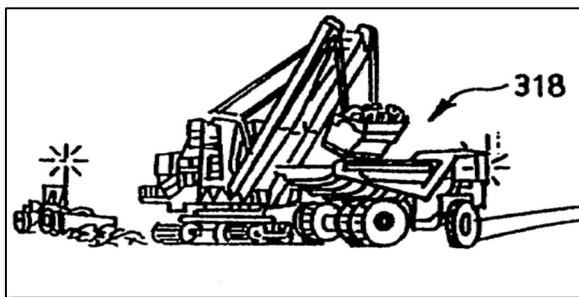
Ex-1008, Fig. 1; Michalson, ¶65.

GPS was rapidly adopted across numerous fields, including, especially, transportation. Examples before 1995 include buses and ships:



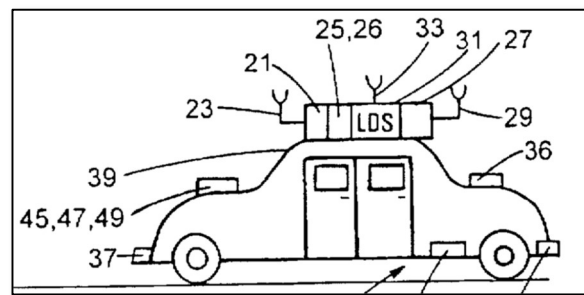
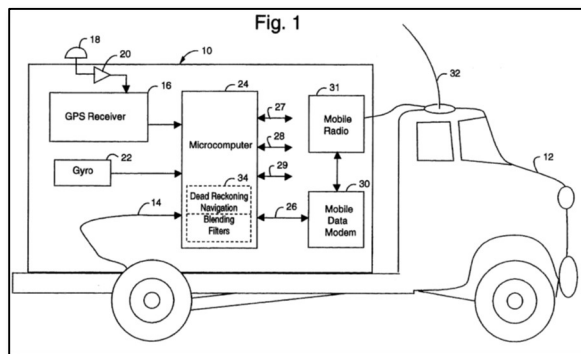
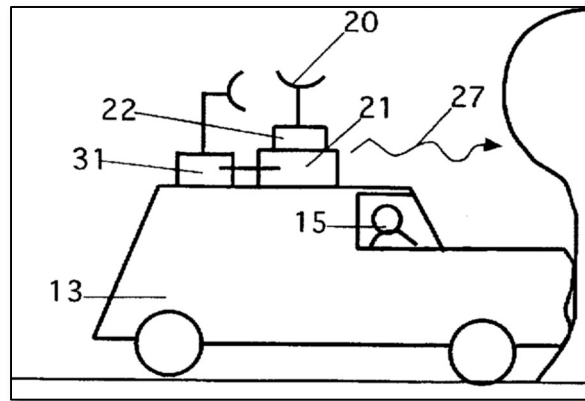
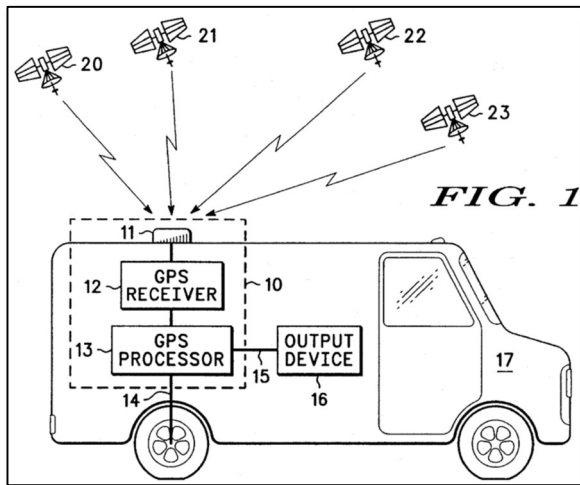
Ex-1009, Fig. 16; Ex-1010, Fig. 1; Michalson, ¶¶66-67.

Heavy machinery and locomotives also utilized GPS technologies before 1990:



Ex-1011, Fig. 3; Ex-1012, Fig. 1; Michalson, ¶¶68-69.

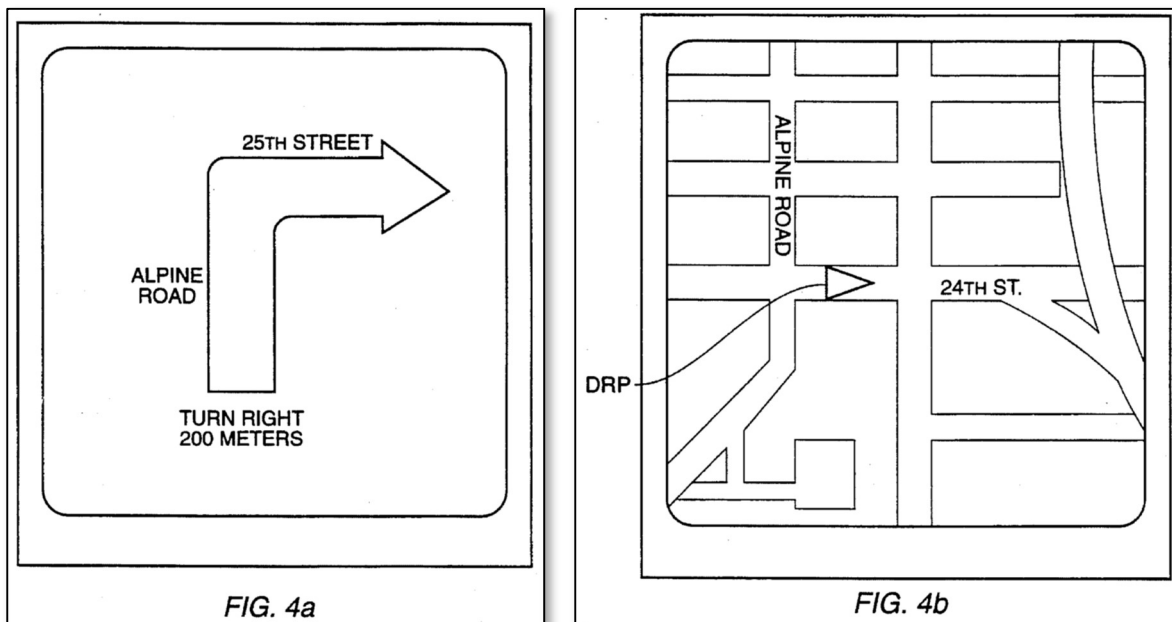
Many other GPS implementations focused on automobiles, including the following from the early 1990s:



Ex-1013, Fig. 1; Ex-1014, Fig. 1; Ex-1015, Fig. 1; Ex-1016, Fig. 1; Michalson,

¶70. GPS usage in vehicles included visual displays of navigation guidance to track the position of a vehicle with reference to its route and destination. Michalson, ¶71.

Examples from 1992 include the following:



Ex-1017, Figs. 4a, 4b; Michalson, ¶¶71.

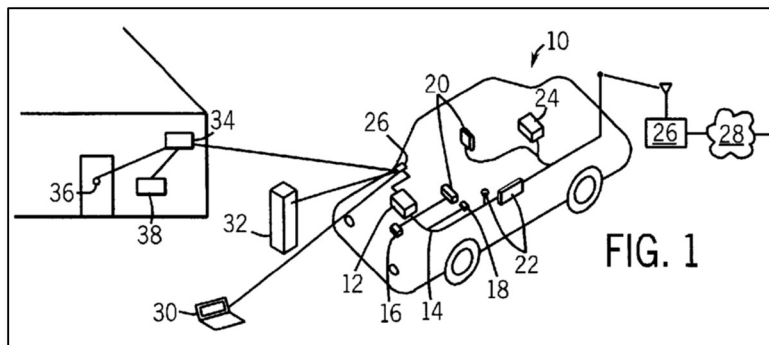
The '192 patent acknowledges that GPS devices were “everywhere,” including vehicles. Ex-1001, 1:21-34; Michalson, ¶¶72. Indeed, GPS systems were “well known” and “navigational purposes were prime motivators for the creation of these systems.” Ex-1018, 8:24-27, 9:14-24, 10:1-18:14; Michalson, ¶¶72.

Manufacturers of in-vehicle and handheld electronic navigation devices included OnStar, Alpine, Clarion, Philips, Pioneer, Visteon, Delphi, and Garmin International. Ex-1020, 1:55-2:9; Ex-1019, 7; Michalson, ¶¶76.

Before the '192 patent, navigation systems in vehicles used map displays which, when given start and end locations, displayed routes. Ex-1018, 7:13-17; Michalson, ¶¶73. For instance, the General Motors 1994 Oldsmobile included such a display and allowed a driver to pinpoint a desired destination and be guided

along the most efficient route which was calculated by an onboard computer. Ex-1018, 7:13-33; Michalson, ¶74.

Before the '192 patent, users could store locations in navigation systems, including current GPS locations, points of interest, and destinations. Ex-1019, 4, 19, 24, 29, 43, 59, 77; Ex-1018, 18:66-19:17; Michalson, ¶¶75, 77. Stored data was secured within the navigation system with a PIN or password. Ex-1019, 29, 43, 76, 79, 118; Michalson, ¶75. Indeed, data encryption and decryption in vehicles were also well known before the '192 patent. Ex-1001, 4:60-66 (disclosing “conventional code encryption algorithms”); Ex-1018, 9:25-45; Michalson, ¶78. An example from 2000 described “key-based access to data stored on a vehicle,” such as “user specific data including passwords, preference settings, and driving log data.” Ex-1021, Abstract; Michalson, ¶79.



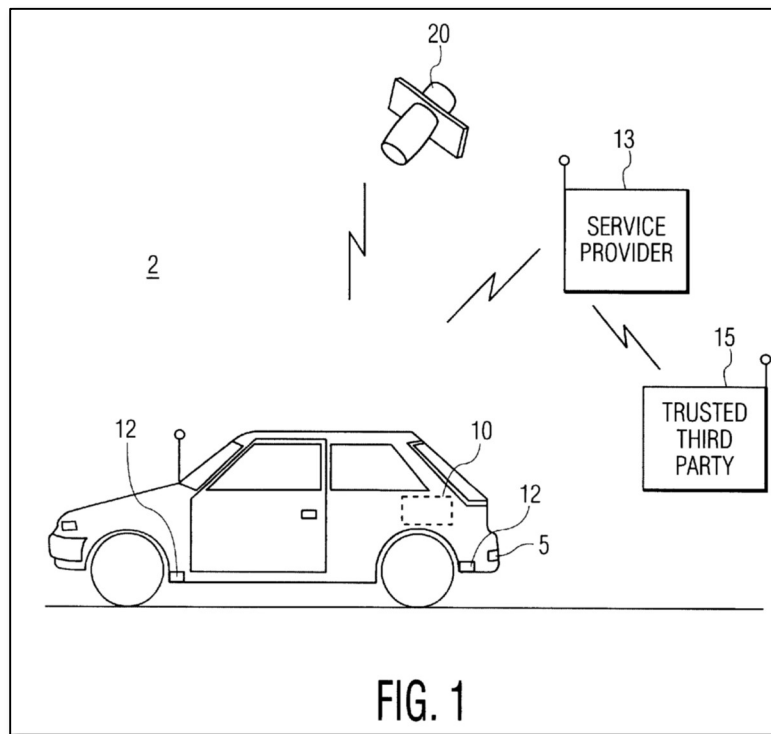
Ex-1021, Fig. 1, 4:7-15, 4:49-5:4; Michalson, ¶79. The disclosed “encryption engine 82” is described in much the same way as the encryption module 128 of the '192 patent. Ex-1021, 6:23-28, 6:65-7:2, Fig. 3; Michalson, ¶79.

An example from 1997 described “[e]ncrypted route information and the like” that are stored in a “vehicle-mounted apparatus 30.” Ex-1022, Abstract; Michalson, ¶80. A further example from 1995 described encryption in vehicles for toll payments. Ex-1023, Abstract; Michalson, ¶80. Another example from 1998 described encrypted data storage in vehicles for incident verification. Ex-1024, Abstract; Michalson, ¶80.

Not only was storing location data in vehicles widely known in the prior art, but so too was storing data on removable media. Examples include a diskette or floppy disk (Ex-1018, 2:39; Ex-1022, 22:28-46), CD or DVD (Ex-1018, 27:42-43; Ex-1020, 18:3; Ex-1022, 22:48-53), and SD memory (Ex-1004, 7:10). Michalson, ¶80.

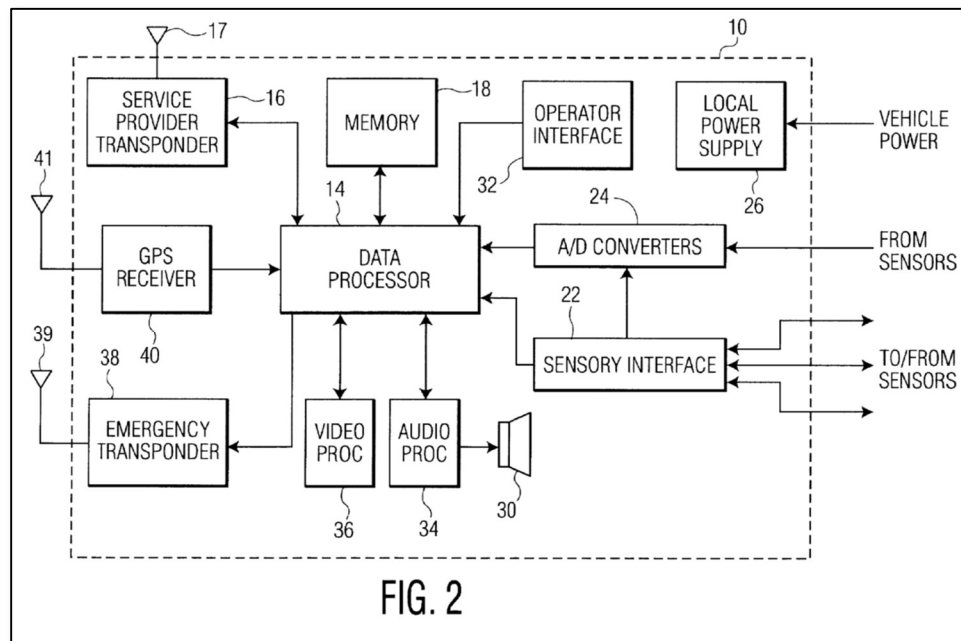
B. *Fish*

Fish describes a “vehicle data archive system” using encryption. Ex-1004, Abstract. Like the ’192 patent, *Fish* discloses storing sensitive vehicle data securely, including GPS location information. *Id.*, Abstract, 1:5-9, 4:22-29, 5:27-32, 7:6-52, Figs. 1-2; Michalson, ¶¶124-125. Vehicle 5 includes data archive 10:



Ex-1004, 2:45-52, Fig. 1; Michalson, ¶125.

Data archive 10 is illustrated in more detail in Figure 2:



Ex-1004, 4:22-29, Fig. 2; Michalson, ¶126.

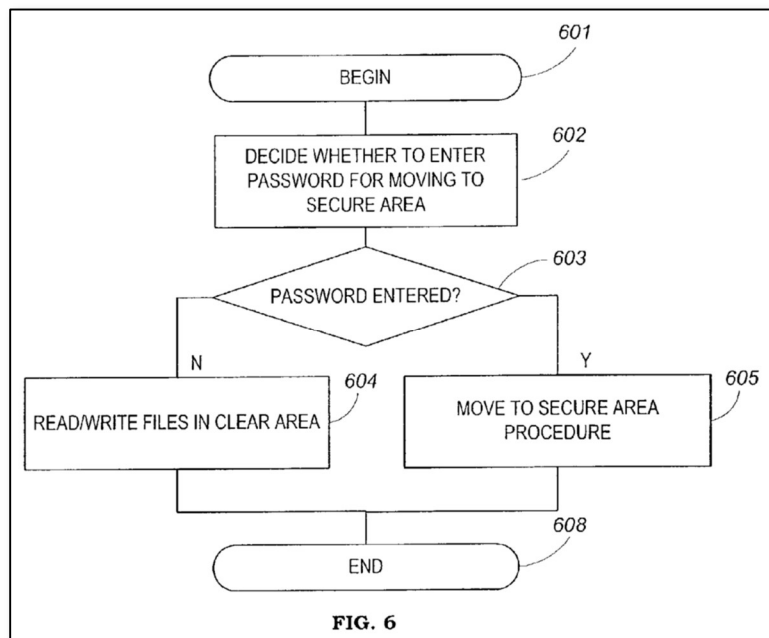
Like the '192 patent, *Fish* teaches encrypting location (and other) data for a vehicle. Ex-1004, 4:8-21, 5:26-38, 11:8-29; Michalson, ¶127. Also, like the '192 patent, *Fish* uses “a removable non-volatile memory device such as a secure digital (SD) memory device or any of a number of other commercially available non-volatile memory devices.” Ex-1004, 7:8-14; Michalson, ¶127.

C. *Ziv*

Ziv describes a “portable storage device including a microprocessor.” Ex-1005, Abstract. A “portable storage device” performs “on-the-fly encryption/decryption of secure data stored on the storage device under a user password,” and “exclude[s] access to the secure user data area unless the user password is provided.” Ex-1005, Abstract; Michalson, ¶¶128-129.

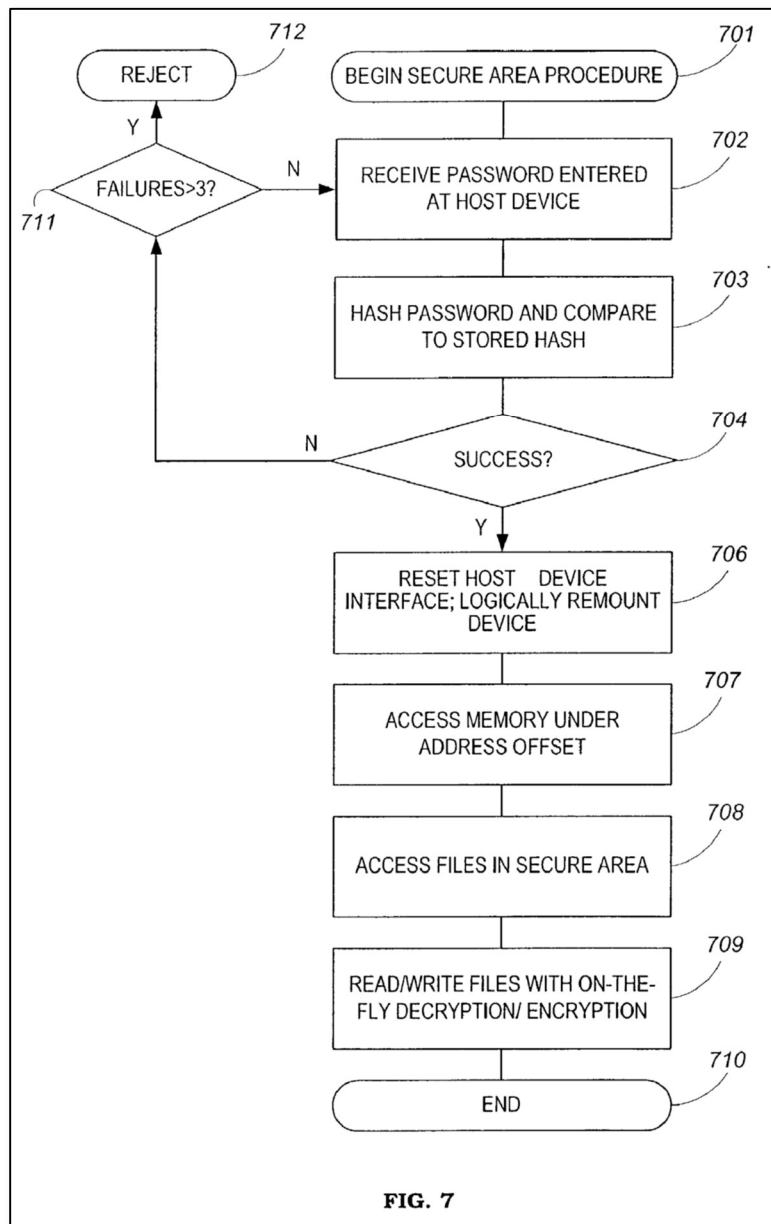
Ziv discloses using a password to selectively encrypt or decrypt data.

Michalson, ¶130. As shown in Figure 6, a user may enter a password in step 602, and if such a password is verified, the user may be able to access “secure user area 122” in step 605.



Ex-1005, ¶[0037], Fig. 6; Michalson, ¶130.

In Figure 7, *Ziv* describes entering a password and, if the password is verified, performing encryption or decryption operations in step 709.



Ex-1005, ¶¶[0038]-[0040], Fig. 7; Michalson, ¶131.

Like the '192 patent and *Fish*, *Ziv* discloses use of removable storage for sensitive information. Ex-1005, Abstract, ¶¶[0001], [0025]; Michalson, ¶132. Just as *Fish* uses removable storage media (e.g., SD memory), Ex-1004, 7:6-29, *Ziv* teaches the same types of memory, including SD memory, Ex-1005, ¶[0025];

Michalson, ¶132. *Ziv* confirms that its storage medium 113 may be “detachable from portable storage device 110.” Ex-1005, ¶[0025]; Michalson, ¶132. Also, like the ’192 patent and *Fish*, *Ziv* discloses encryption and decryption techniques for protecting data stored on a removable storage device, including the use of a user password or biometric identification (e.g., fingerprint) to provide further enhanced security. Ex-1005, Abstract, ¶¶[0026], [0031], [0033], [0037]-[0045]; Michalson, ¶132.

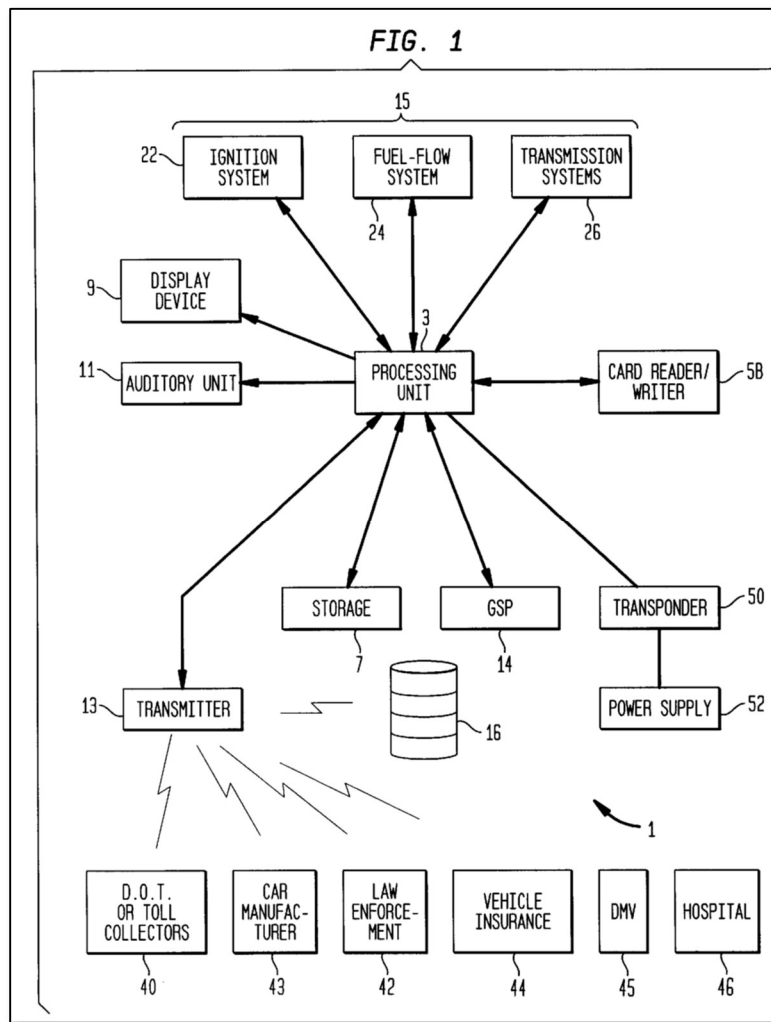
D. *Gehlot*

Similar to *Fish*, *Gehlot* discloses “receiving, processing, and storing real-time data from various types of input, including but not limited to information from a vehicle’s micro-processing systems, a driver information card, a vehicle information card, and physical attributes of the driver/owner.” Ex-1006, Abstract. *Gehlot* describes “collecting vehicle data and preventing unauthorized vehicle use” and “collecting data from various vehicle systems, information cards, and other external data sources and transmitting the collected data to external data receivers.” Ex-1006, 1:5-9; Michalson, ¶¶133-134.

A “vehicle data processor” prompts the user to “input some form of physical data, i.e. retinal scan, fingerprint, voice recognition,” whereby the VDP “matches the data to information stored in memory and grants authorization to the user” to drive the vehicle. Ex-1006, 2:3-8, 2:17-31, 6:1-12; Michalson, ¶135. The input

may alternatively be a “password via a keyboard.” Ex-1006, 6:6-8; Michalson, ¶135.

Like the ’192 patent and *Fish, Gehlot* discloses use of removable storage for vehicle-related information and collection and storage of vehicle data “such as average, maximum and minimum speeds driven, average fuel consumption, distance traveled, and the like,” which could be “displayed on a visual display unit.” Ex-1006, 4:24-5:33; Michalson, ¶136. The stored information can be transmitted to external entities. Ex-1006, 5:34-67; Michalson, ¶136. Data from a “GPS unit can also be routed by the processor unit 3 to transmitter 13 to be sent to law enforcement.” Ex-1006, 6:51-54; Michalson, ¶137.



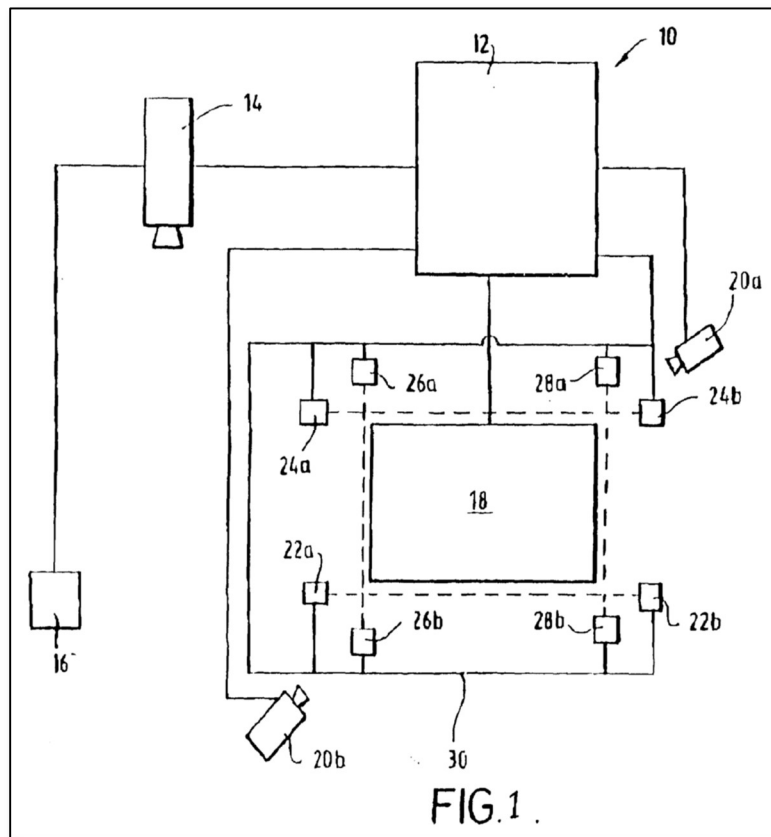
Ex-1006, Fig. 1; Michalson, ¶¶137.

E. *Stevenson*

Stevenson describes “a vehicle entry/exit control system.” Ex-1007, Cover.

Stevenson uses biometric sensing to confirm a driver’s identity for controlling entry and exit of vehicles within a restricted area. Ex-1007, Abstract, ¶¶[0001], [0004]-[0007]; Michalson, ¶¶138-139. The biometric sensing includes iris recognition, fingerprint, palm print, voice pattern and DNA, such as saliva.

Ex-1007, ¶¶[0007], [0019]-[0020]; Michalson, ¶139. System 10 may include control unit 12 and camera 14, and may compare obtained images of a user (e.g., face or eye) to verify the user before vehicle operations are permitted.



Ex-1007, ¶¶[0007]-[0010], Fig. 1; Michalson, ¶140.

V. Level of Ordinary Skill

A person of ordinary skill in the art (“POSITA”) would have possessed at least a four-year degree in electrical engineering or a closely related field, and at least two years of experience with navigation systems, or an equivalent advanced education

in the field of navigation systems. Additional education could substitute for professional experience and vice versa. Michalson, ¶¶81-82.

VI. Claim Construction

The Board construes claims according to *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). Petitioner presents below certain constructions of claim terms that invoke pre-AIA 35 U.S.C. § 112, ¶ 6. These constructions include the noted functions and corresponding disclosed structure—all simple, conventional components—as well as equivalents of such structure.

Petitioner does not concede that the '192 patent discloses adequate structure, such as algorithms, for purposes of definiteness for any term. But this does not prevent the Board from comparing the prior art to the claims here because the prior art discloses the same (and more) structure as found in the '192 patent itself. *See Sisvel Int'l S.A. v. Sierra Wireless, Inc.*, 82 F.4th 1355 (Fed. Cir. 2023) (Board may “resolve the prior-art challenge to the patentability of the claims despite the potential indefiniteness of the means-plus-function term” unless “impossible to adjudicate”). Claims should only be construed to the extent necessary to resolve a controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Because the prior art here discloses the same structure as the '192 patent, the Grounds here are possible to adjudicate.

A. “a locational information module for determining” (Claims 1, 13, 19, 22)

This term uses “module” as “a well-known nonce word that can operate as a substitute for ‘means’ in the context of § 112, para. 6.” *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1350 (Fed. Cir. 2015) (en banc); *Rain Computing, Inc. v. Samsung Elecs. Am., Inc.*, 989 F.3d 1002, 1006 (Fed. Cir. 2021) (“‘module’ here does not provide any indication of structure”). As in *Williamson* and *Rain Computing*, “locational information” does “not impart structure into the term ‘module.’” *Williamson*, 792 F.3d at 1351; Michalson, ¶90.

Function: Claims 1, 13, 19, and 22 recite the following function for the claimed “locational information module”: “determining location information of the [location information] device.”¹ *See also* Ex-1001, 3:55-56; Michalson, ¶91.

Structure: The locational information module “may include a receiver and an antenna ANT employing conventional locational information processing technology such as Global Positioning Satellite (GPS) Technology, Loran Technology, or any other available locational technology, to indicate the exact

¹ Claims 1 and 13 recite a “device” while claims 19 and 22 recite a “location information device.”

location, e.g., latitude, longitude and altitude, of the device 100.” Ex-1001, 3:56-62. Michalson, ¶¶92-93.

B. “an encryption module for encrypting” (Claims 1, 13, 19, 22)

This term uses “module” as “a well-known nonce word that can operate as a substitute for ‘means’ in the context of § 112, para. 6.” *Williamson*, 792 F.3d at 1350; *Rain Computing*, 989 F.3d at 1006. Here too, “encryption” does “not impart structure into the term ‘module.’” *Williamson*, 792 F.3d at 1351; Michalson, ¶94.

Function: Claims 1, 13, 19, and 22 recite the following function for the claimed “encryption module”: “encrypting the determined location information.” Michalson, ¶95.

Structure: The “encryption module” as disclosed is an encryption technique, such as symmetric-key techniques (e.g., DES, Triple-DES, Blowfish, RC2, RC4, and RC5) or asymmetric-key techniques (e.g., Diffie-Hellman, RSA, and ElGamal). *See* Ex-1001, 4:60-66; Michalson, ¶¶96-97.

C. “a storage module for storing” (Claims 13, 22)

This term again uses “module” as “a well-known nonce word that can operate as a substitute for ‘means’ in the context of § 112, para. 6.” *Williamson*, 792 F.3d at 1350; *Rain Computing*, 989 F.3d at 1006. The recited “storage” connotes a function or action, but does “not impart structure into the term ‘module.’” *Williamson*, 792 F.3d at 1351; Michalson, ¶98.

Function: Claims 13 and 22 recite the following function for the claimed “storage module”: “storing the encrypted location information.” Michalson, ¶99.

Structure: The “storage module may be internal memory.” Ex-1001, 2:4-5; *see also id.*, 2:21-22. In particular, “[t]he storage module 110 includes internal storage memory, e.g., random access memory (RAM), or removable memory such as magnetic storage memory; optical storage memory, e.g., the various known types of CD and DVD media; solid-state storage memory, e.g., a CompactFlash card, a Memory Stick, SmartMedia card, MultiMediaCard (MMC), SD (Secure Digital) memory; or any other memory storage that exists currently or will exist in the future.” *Id.*, 4:47-54; *see also id.*, Abstract, 1:66-2:4; Michalson, ¶¶100-101. In claims 13 and 22, which do not recite “removable” memory, the memory would include both removable and non-removable forms of memory. Michalson, ¶¶100-101.

D. “a removable storage module for storing” (Claims 1, 19)

Here too, the claimed “removable storage module” uses “module” as “a well-known nonce word that can operate as a substitute for ‘means’ in the context of § 112, para. 6.” *Williamson*, 792 F.3d at 1350; *Rain Computing*, 989 F.3d at 1006. The recited “removable storage” connotes functions of removing and storing, but does “not impart structure into the term ‘module.’” *Williamson*, 792 F.3d at 1351; Michalson, ¶102.

Function: Claims 1 and 19 recite the following function for the claimed “removable storage module”: “storing the encrypted location information.”

Michalson, ¶103.

Structure: A POSITA would have understood the structure of a “removable storage module” to be a “removable storage memory” such as those described above for the term “storage module” to the extent they are removable (e.g., “CD and DVD media; solid-state storage memory, e.g., a CompactFlash card, a Memory Stick, SmartMedia card, MultiMediaCard (MMC), SD (Secure Digital) memory”). Ex-1001, 2:18-19, 4:48-54; Michalson, ¶¶104-105.

E. “a processing module for sending” (Claims 1, 13, 19, 22) and “the processing module selectively decrypts” (Claims 3, 16)

The claimed “processing module” uses “module” as “a well-known nonce word that can operate as a substitute for ‘means’ in the context of § 112, para. 6.” *Williamson*, 792 F.3d at 1350; *Rain Computing*, 989 F.3d at 1006. As claimed, “processing” is a function, not a particular structure, and thus does “not impart structure into the term ‘module.’” *Williamson*, 792 F.3d at 1351; Michalson, ¶106.

Function: The “processing module” performs at least two functions. Claims 1, 13, 19, and 22 recite the following functions for the claimed “processing module”: “sending the encrypted location information to the [] storage module []

. . . and retrieving the encrypted location information from² the [] storage module.”

Claims 1 and 19, unlike claims 13 and 22, are directed to encrypted location information sent to and retrieved from a “removable” storage module. Michalson, ¶107.

Dependent claims 3 and 16 recite the following function for the claimed “processing module”: “selectively decrypts the location information stored in the [] storage module based on the identity of the user.” Michalson, ¶108. Claim 3, unlike claim 16, is directed to location information stored in the “removable” storage module. *Id.*

Structure: The disclosed structure is “a computer processing module 120, e.g., a microprocessor,” which “will use computer software instructions that have been programmed into the module and conventional computer processing power to interact and organize the traffic flow between the various other modules.”

Ex-1001, 3:26-34; Michalson, ¶¶109-110.

F. “an input module disposed on the housing configured for receiving” (Claims 2, 15)

Here too, the claimed “input module” uses “module” as “a well-known nonce word that can operate as a substitute for ‘means’ in the context of § 112,

² Claim 19 mistakenly recites “form” instead of “from.”

para. 6.” *Williamson*, 792 F.3d at 1350; *Rain Computing*, 989 F.3d at 1006. The term “input” connotes function, not particular structure, and thus does “not impart structure into the term ‘module.’” *Williamson*, 792 F.3d at 1351; Michalson, ¶111.

Function: Claims 2 and 15 recite the following function: “receiving a code string input by a user, wherein the³ user inputted code string is used for encrypting and decrypting the location information stored in the [] storage module.”

Michalson, ¶112. Claim 2, unlike claim 15, is directed to encrypting and decrypting the location information stored in the “removable” storage module. *Id.*

Structure: Claims 2 and 15 recite that the “input module” is “disposed on the housing.” Michalson, ¶113. The “[i]nput module 106 includes a plurality of buttons 108 for inputting data and navigating through a plurality of menus and/or maps.” Ex-1001, 3:14-16; Michalson, ¶113.

Additionally, “user input module 126” can “receive user instructions via text input by the way of buttons 108, a standard keyboard interface coupled to the device, or a character recognition capture device which translates user text input into alphanumeric characters,” and may also include a “touch screen,” “microphone 114” with an “analog-to-digital (A/D) converter,” or “voice

³ Claim 15 mistakenly recites “he” instead of “the.”

recognition processor.” Ex-1001, 4:27-46; Michalson, ¶114. These too are examples of the structure disclosed for the “input module.” Michalson, ¶114.

**G. “a user verification module for verifying the identity of [the] user”
(Claims 3-5, 16-18)**

The claimed “user verification module” uses “module” as “a well-known nonce word that can operate as a substitute for ‘means’ in the context of § 112, para. 6.” *Williamson*, 792 F.3d at 1350; *Rain Computing*, 989 F.3d at 1006. The recited “user verification” is a function or action, not a particular structure, and thus does “not impart structure into the term ‘module.’” *Williamson*, 792 F.3d at 1351; Michalson, ¶115.

Function: Claims 3 and 16 recite the following function for the claimed “user verification module”: “verifying the identity of user of the device.” Michalson, ¶116. Claims 4 and 17 recite the same function and further recite that the user verification module “executes a password protection algorithm for verifying the identity of the user of the device.” *Id.*, ¶117. Claims 5 and 18 further recite that the “user verification module” “compris[es] an identity capture device for verifying the identity of the user of the device.” *Id.*

Structure: User verification module 130 “will indicate and verify the identity of the user of the device 100.” Ex-1001, 5:49-51; Michalson, ¶118. “The user verification module 130 may execute a password protection algorithm or may

include an identity capture device, either incorporated into the device 100 or coupled externally via a cable.” Ex-1001, 5:51-54; Michalson, ¶118. An identity capture device “may be a biometric device, such as a retinal scanning device, finger print reader, facial recognition reader or another type of user identity verification input device which will collect information on the user to be compared to information that has previously been stored in the device’s memory.” Ex-1001, 5:54-59; Michalson, ¶118.

H. “a transmission module for transmitting” (Claims 12, 14, 22)

Once more, the claimed “transmission module” uses “module” as “a well-known nonce word that can operate as a substitute for ‘means’ in the context of § 112, para. 6.” *Williamson*, 792 F.3d at 1350; *Rain Computing*, 989 F.3d at 1006. Adding “transmission” before “module” invokes only the function of transmitting, not particular structure, and thus does “not impart structure into the term ‘module.’” *Williamson*, 792 F.3d at 1351; Michalson, ¶119.

Function: Claim 12 recites the following function for the claimed “transmission module”: “transmitting the encrypted location information to an external computing device.” Michalson, ¶120. Claims 14 and 22 more narrowly recite that the location information is transmitted “from the storage module to an external computing device.” *Id.*

Structure: The “GPS device may further include a transmission module or connection, e.g., hardwire or wireless, to port the information to a computer.” Ex-1001, 2:4-7; Abstract; Michalson, ¶121. The disclosed “transfer will be done by transmission module 112 including hardwired and/or wireless connectivity,” and may use “hard wire cabling e.g., parallel or serial cables, USB cable, Firewire (1394 connectivity) cables, and the appropriate port” or “various known wireless protocols including but not limited to Bluetooth™ interconnectivity, infrared connectivity, radio transmission connectivity including computer digital signal broadcasting and reception commonly referred to as Wi-Fi or 802.11.X (where x denotes the type of transmission), or any other type of communication protocols or systems currently existing or to be developed for wirelessly transmitting data.” Ex-1001, 6:26-40; Michalson, ¶121.

VII. Ground 1: *Fish* (Claims 1, 11-14, 19-22)

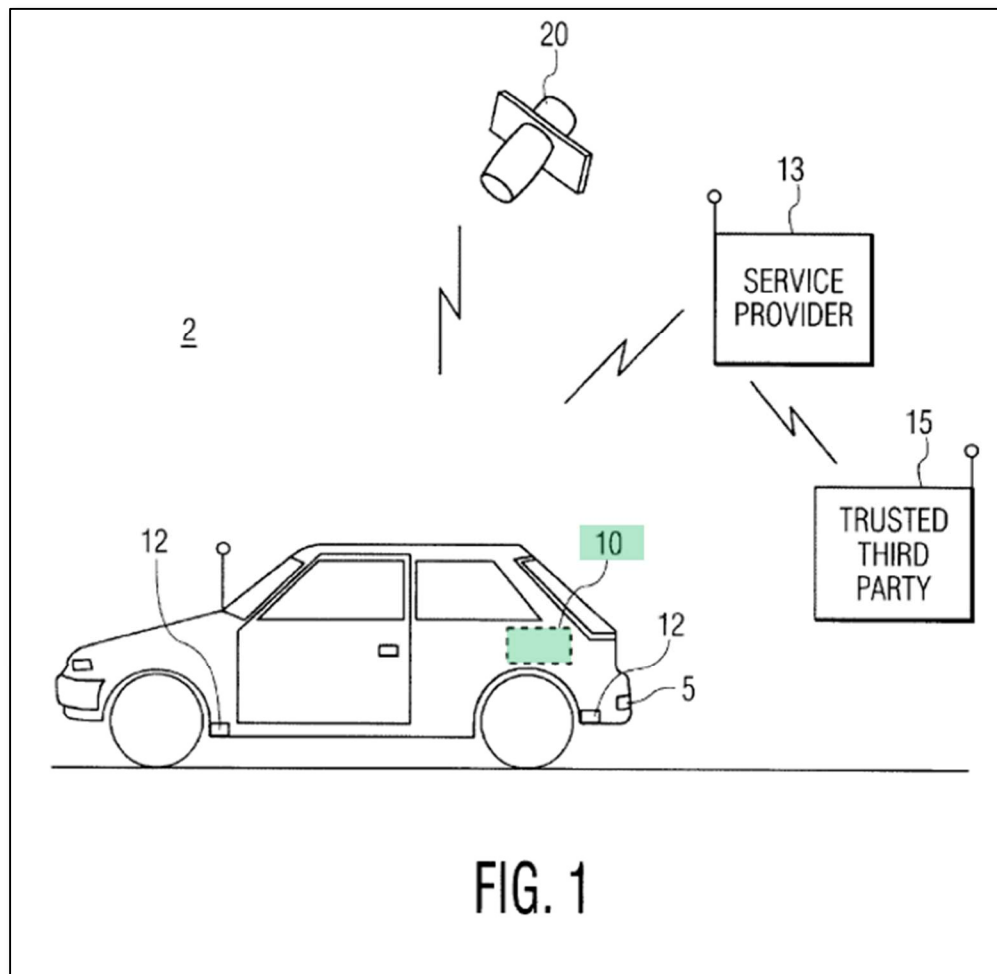
Claims 1, 11-14, and 19-22 are unpatentable under § 103 in view of *Fish*, alone or with the knowledge of a POSITA.

A. Claim 1

1. [1pre] A location information device with secure data storage comprising:

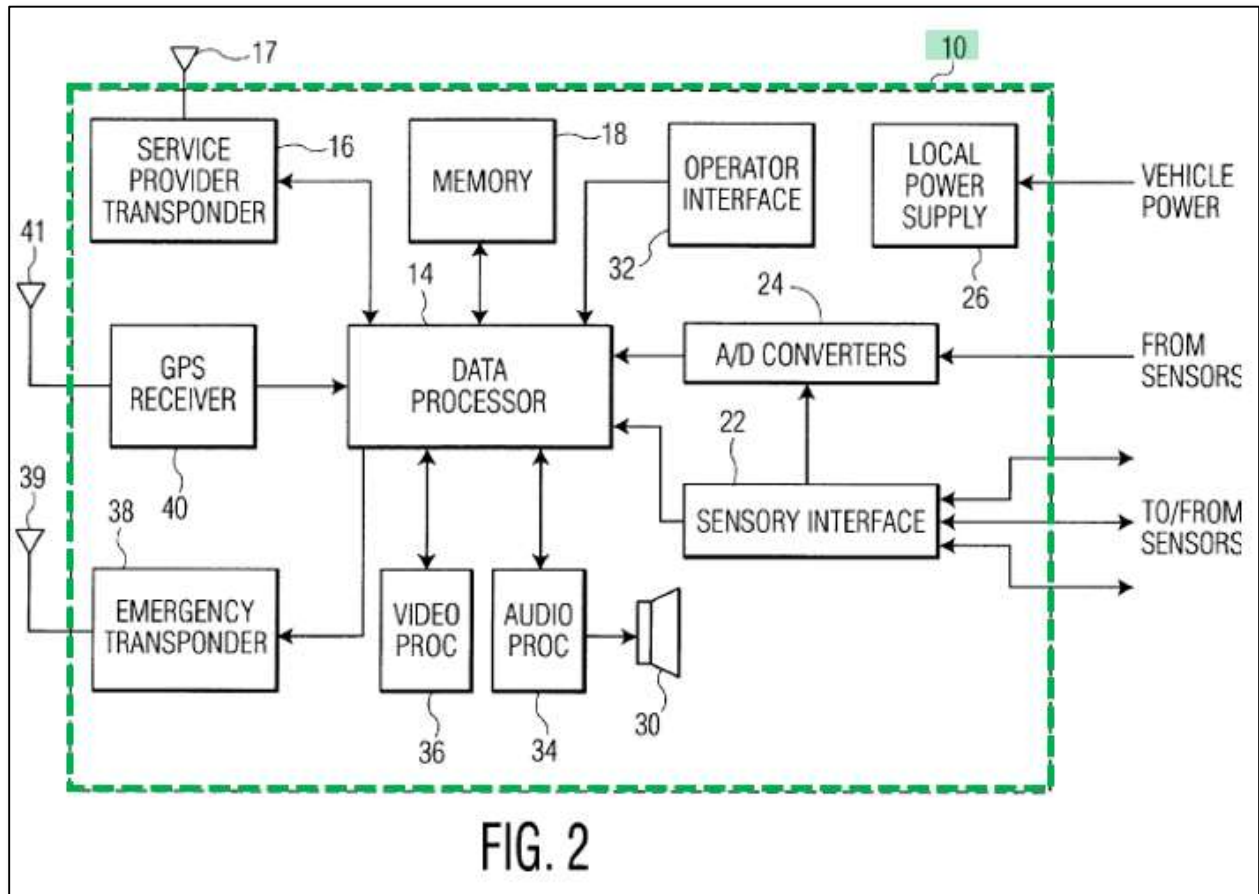
To the extent the preamble is limiting, *Fish* teaches a location information device with secure data storage. *E.g.*, Ex-1004, Abstract, 2:45-57, 3:10-27, 4:8-15, 4:57-59, 7:30-56, 8:41-53, 11:8-14, Fig. 1; Michalson, ¶¶142-143.

Fish discloses a “vehicle **data archive** system” with an “instrumentation interface [that] receives at least one sensory data signal of the vehicle” and stores it in memory. Ex-1004, Abstract; Michalson, ¶144. The information may be encrypted (i.e., “secure,” as claimed) with its **data archive** “securely archiving signals,” such as “situational data concerning a vehicle.” Ex-1004, 1:6-9, 1:36-54, 2:16-43; Michalson, ¶144. *Fish* teaches storing and encrypting information in “**data archive 10** located in [the] vehicle.” Ex-1004, 2:45-57, Fig. 1; Michalson, ¶144.



Ex-1004, Fig. 1; Michalson, ¶144. *Fish*'s **data archive 10** is illustrated further in

Figure 2:



Ex-1004, Fig. 2; Michalson, ¶144.

Location (e.g., GPS) information is stored in memory 18 of “**data archive 10**.” Ex-1004, 3:10-27, 4:8-15, 4:22-29, 4:57-59, 7:30-56, 8:41-53, 11:8-14, Fig. 1; Michalson, ¶145.

2. [1a] a housing;

Fish teaches obvious a housing for the location information device. Ex-1004, 2:66-3:9; Michalson, ¶146.

“The data archive 10 of the exemplary embodiment is preferably **housed** in a **sealed cabinet**.” Ex-1004, 3:2-4; Michalson, ¶¶147-148. This housing “is desirably fire and water resistant and designed to offer significant resistance to crush forces typically encountered in catastrophic vehicle wrecks.” Ex-1004, 3:6-9; Michalson, ¶¶147-148. A POSITA would have understood this teaches the “housing” of claim 1, which is not claimed or described as requiring unique physical or functional attributes. Michalson, ¶148.

3. [1b] a locational information module for determining location information of the device, the determined location information being at least one route traveled by the device;

Fish discloses and renders obvious a locational information module for determining location information of the device, the determined location information being at least one route traveled by the device. *E.g.*, Ex-1004, 4:22-29, 5:27-32, 7:23-51, Figs. 1-2; Michalson, ¶149.

The claimed “locational information module” is a means-plus-function term with a function of determining location information of the device and disclosed structure of a receiver and antenna employing conventional locational information processing technology such as GPS. Ex-1001, 3:56-62; Michalson, ¶150. *Fish* discloses this same function and structure with **GPS receiver 40** and **antenna 41**.

Data archive 10 may include **GPS receiver 40**, which determines location information. Ex-1004, 4:22-29, Fig. 2; Michalson, ¶151. **GPS receiver 40** also

records temporal data corresponding to the location information. Ex-1004, 4:22-29, 5:27-32; Michalson, ¶151. **GPS receiver 40** has an associated **antenna 41**.

Ex-1004, Fig. 2; Michalson, ¶151.

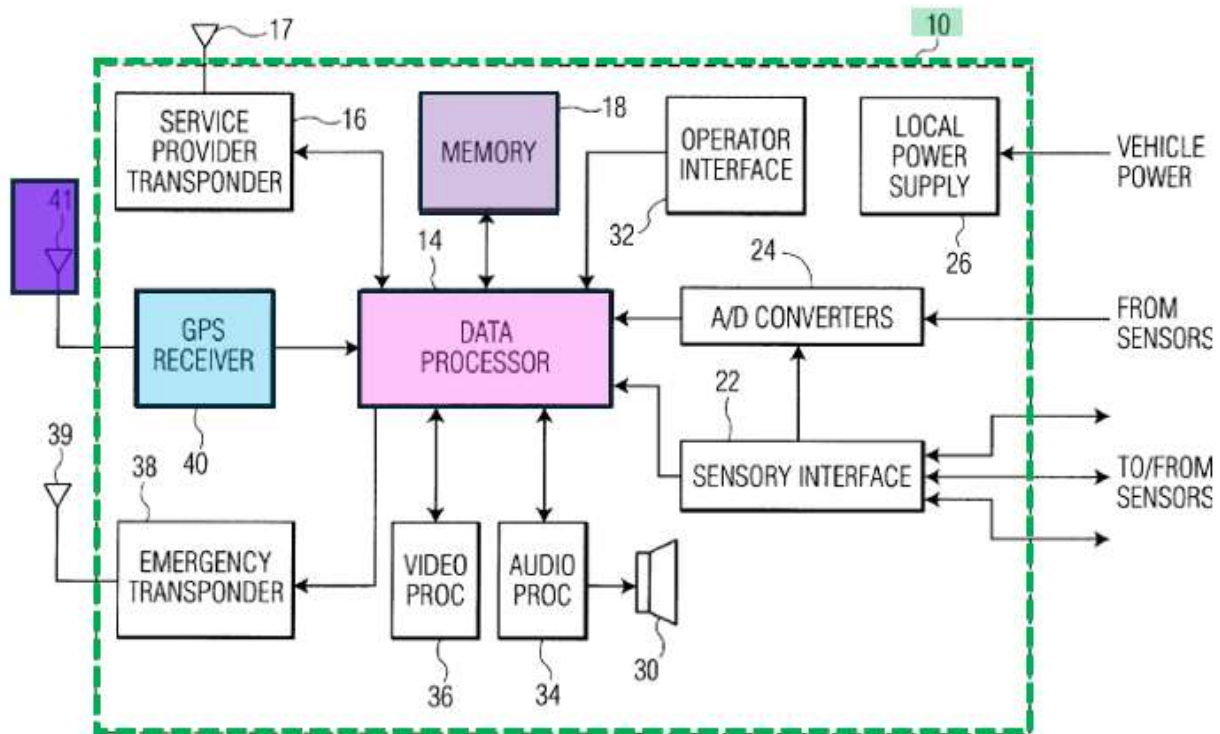


FIG. 2

Ex-1004, Fig. 2; Michalson, ¶151.

Fish also teaches storing location data at a “predetermined interval (e.g., 15 seconds)” in case of vehicle accidents. Ex-1004, 7:23-29; Michalson, ¶152. A POSITA would have understood that by storing location data collected at predetermined time intervals, the resulting data provides the route traveled by the device. Michalson, ¶¶152-153. This, too, discloses and renders obvious the

determined location information being at least one route traveled by the device, as claimed. Ex-1004, 5:27-32, 7:30-52, 11:8-26; Michalson, ¶¶152-155.

Fish also provides an example where a vehicle travels a particular route and data archive 10 stores encrypted route traveled data:

For example, where a vehicle is traveling 60 mph along US. route 1 going south at 4PM EST., the speed data and operational details such as the pressure on the accelerator pedal and break pedal and the direction of the steering wheel are continuously provided to data archive 10, the time, **location, and direction data can be derived from the data provided by GPS receiver 40.** . . . Upon a collision, the sensors produce the predetermined sensory data signal (e.g. airbag deployment) the data archive 10 would halt data collection operations encrypt and sign any pending sensory data. In this way, data archive could be accessed after the collision to assess the conditions which preceded the accident.

Ex-1004, 11:8-26, 5:27-32; Michalson, ¶¶156-157. This too discloses and renders obvious the determined location information being at least one route traveled by the device. Such a route includes the time, location, direction, and/or cartographic data of the traveling vehicle. Ex-1004, 11:8-26, 5:27-32; Michalson, ¶158.

As another example, *Fish* discloses **data processor 14** using a portion of **secure memory 18** with preloaded cartographic content in conjunction with GPS information to identify cartographic locations, i.e., map locations:

Although the primary function of the **secure memory 18** is to store the operational, situational and environmental data derived from the sensors 12, In the

exemplary embodiment, a portion of **secure memory 18** is reserved for use by the **data processor 14** to enable GPS functionality, sensory data signal conditioning, and audio/video processing functionality. In this embodiment, **cartographic content may be preloaded** into the **secure memory 18** upon manufacture for use in conjunction with **data processor 14** and **GPS receiver 40 for identifying a cartographic location corresponding to latitude and longitude coordinates derived from the GPS signal.**

Ex-1004, 7:30-41; Michalson, ¶159. Similarly, *Fish*'s claim 21 recites a GPS communication module "responsive to global positioning signals for identifying a cartographic location of the modular data archive." Ex-1004, 14:23-27; Michalson, ¶160. A "GPS signal for identifying the latitudinal and longitudinal coordinates of the data archive 10 [] may be translated to a geographical location if the secure memory 18 is preloaded with cartographic content." Ex-1004, 7:42-49; Michalson, ¶161. Also, latitude and longitude "may simply be recorded" without translation into cartographic location. Ex-1004, 7:49-51; Michalson, ¶161. *Fish* thus discloses cartographic locations are more than mere GPS coordinates, and a POSITA would have understood *Fish*'s cartographic locations to represent a route traveled. Michalson, ¶¶161-163.

4. [1c] an encryption module for encrypting the determined location information;

Fish discloses and renders obvious an encryption module for encrypting the determined location information. *E.g.*, Ex-1004, 1:35-54, 2:16-42, 3:10-37, 4:8-21,

5:27-32, 7:30-52, 13:9-22 (claim 10), 14:23-27 (claim 21), Figs. 1-3; Michalson, ¶164.

The claimed encryption module is a means-plus-function term, with a function of encrypting the determined location information and disclosed structure of an encryption technique, such as those referenced in the specification. Ex-1001, 4:60-66; Michalson, ¶165. *Fish* discloses this function and structure because its **data processor 14** or **data archive 10** performs the same conventional types of data encryption disclosed in the '192 patent. *E.g.*, Ex-1004, 4:43-5:3, 9:18-28, 10:16-30, 12:1-12; Michalson, ¶165.

Fish stores data on its data archive system using a “secret encryption key” and other encryption techniques. Ex-1004, 1:35-54, 2:16-24, 2:25-42, 3:10-37, 4:8-21, 5:27-38, Figs. 2-3; Michalson, ¶166. **Data processor 14** of **data archive 10** **may** receive keys from a service provider to encrypt and store information in **memory 18**. Ex-1004, 4:43-54, 13:9-22 (claim 10), Figs. 1-2; Michalson, ¶166.

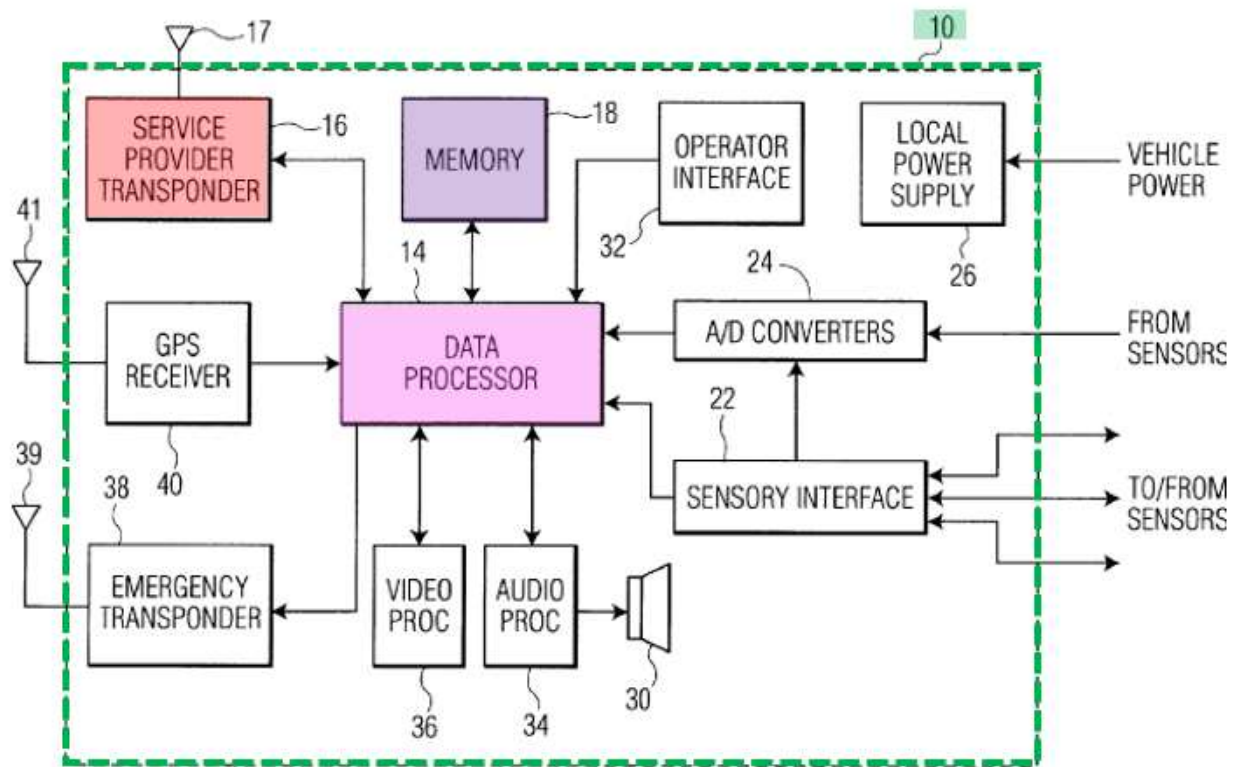


FIG. 2

Ex-1004, Fig. 2; Michalson, ¶166.

Encrypted and stored data includes GPS information and “cartographic information.” Ex-1004, 4:8-22, 5:27-32, 7:30-49, 14:23-27 (claim 21); Michalson, ¶167. The encryption techniques of *Fish*—similar to the ’192 patent itself—include Diffie-Hellman key exchange, and the like. Ex-1004, 4:66-5:4, 9:25-31, 10:5-11, 10:26-30, 12:1-5; *see also* Ex-1001, 4:60-5:3 (encryption techniques such as “DES, Triple-DES, Blowfish, RC2, RC4, RC5, etc.,” and “Diffie-Hellman, RSA, ElGamal, etc.”); Michalson, ¶167.

5. [1d] a removable storage module for storing the encrypted location information, the removable storage module being removably disposed in the housing; and

Fish discloses and renders obvious a removable storage module for storing the encrypted location information, the removable storage module being removably disposed in the housing, as claimed. *E.g.*, Ex-1004, 7:6-29; Michalson, ¶168.

The claimed removable storage module is a means-plus-function term, with a function of storing the encrypted location information and disclosed structure of storage removably disposed in the housing, e.g., magnetic memory, optical memory, CD and DVD media, solid-state memory, CompactFlash card, a Memory Stick, SmartMedia card, MultiMediaCard (MMC), or SD memory. Michalson, ¶169.

Fish's "secure memory 18 [may be] a **removable** non-volatile memory device such as a **secure digital (SD) memory device**." Ex-1004, 7:6-29; Michalson, ¶170. "[S]ecure memory 18 is **removable** to allow for easy access to the data after an accident." Ex-1004, 7:6-29; Michalson, ¶170. This includes encrypted location information stored in secure memory 18. Ex-1004, 11:44-51, 1:46-50, 3:10-4:7, Fig. 2; Michalson, ¶ *Fish* discloses and a POSITA would have understood that *Fish*'s housing or sealed cabinet for its data archive 10 would be a physical housing. Ex-1004, 3:2-9; Michalson, ¶170. According to such disclosure,

Fish's removable “**secure memory 18**” (e.g., SD memory, or the like) would be removably disposed in the housing. Michalson, ¶170.

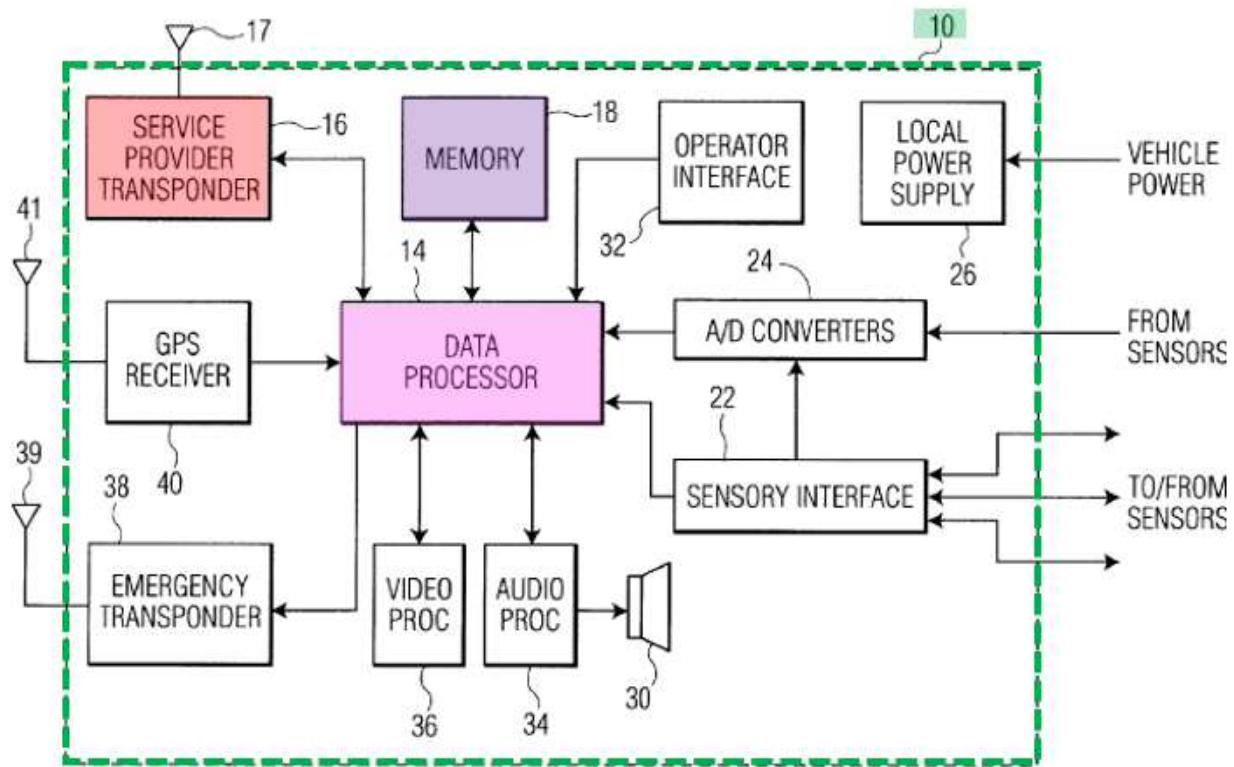


FIG. 2

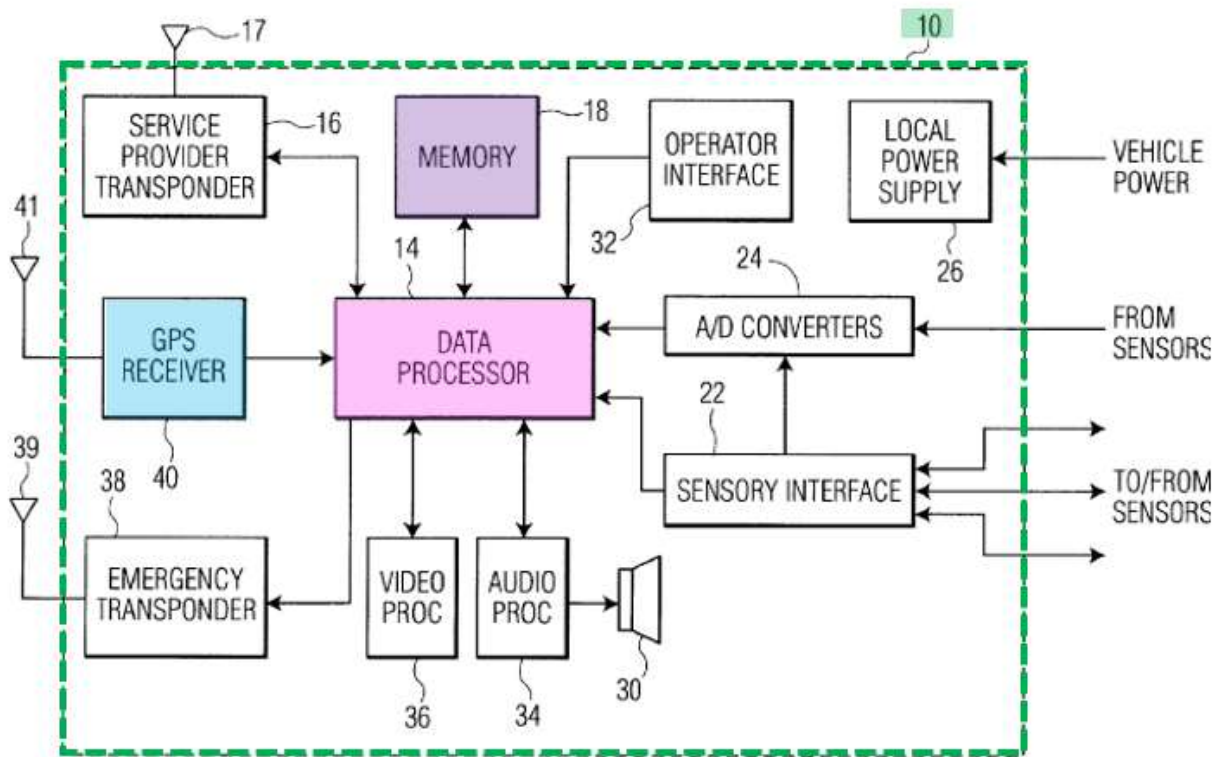
Ex-1004, Fig. 2; Michalson, ¶170.

6. [1e] a processing module for sending the encrypted location information to the removable storage module removably disposed in the housing and retrieving the encrypted location information from the removable storage module.

Fish discloses a processing module for sending the encrypted location information to the removable storage module removably disposed in the housing and retrieving the encrypted location information from the removable storage

module, as claimed. *E.g.*, Ex-1004, 4:8-22, 4:51-54, 5:27-32, 6:63-7:5, 7:30-49, Fig. 2; Michalson, ¶171.

The claimed processing module is a means-plus-function term, with functions of sending the encrypted location information to the removable storage module and retrieving the encrypted location information from the removable storage module, and disclosed structure of computer processing module 120, e.g., a microprocessor. Ex-1001, 3:26-34; Michalson, ¶172. *Fish* discloses this function and structure in terms of **data processor 14**, which is or includes a processing module that exchanges “control information and data” with “**secure memory 18**” and other system components, including **GPS receiver 40**. Ex-1004, 6:63-7:5; Michalson, ¶173. **Data processor 14** encrypts data and stores encrypted data, including location information. Ex-1004, 4:8-22 (GPS data “may be combined . . . with the sensory signal data prior to encryption”), 4:51-54 (**data processor 14** generates encryption key), 5:27-32 (data archive may encrypt temporal, cartographic, GPS, and sensory data), 6:63-7:5 (data processor 14 controls exchange of information), 7:30-49 (**data processor 14** “identif[ies] a cartographic location” and stores longitude, latitude, and cartographic data in **secure memory 18**), Fig. 2; Michalson, ¶173.



Ex-1004, Fig. 2; Michalson, ¶173.

Once encrypted location data is stored on *Fish*'s **secure memory 18**, it may be retrieved via **data processor 14**. Ex-1004, 7:6-29; Michalson, ¶174. Indeed, retrieving this data from data “archive” 10 is the purpose of data archive 10. Ex-1004, Abstract, 1:36-45, 5:51-54, 7:12-17, 10:16-30, 11:24-26; Michalson, ¶174.

B. Claim 11

1. [11] The device as in claim 1, wherein the location information further includes at least one of a home address, destination addresses and velocity of the device at predetermined times.

Fish discloses and renders obvious the device as in claim 1, wherein the location information further includes at least one of a home address, destination addresses, and velocity of the device at predetermined times. Michalson, ¶175.

Fish discloses and renders obvious that its location information includes each of home addresses, destination addresses, and velocities of the vehicle containing data archive 10.

First, *Fish* discloses storing location (e.g., **GPS** or **cartographic**) information as described above. *See supra* claim [1b]; Michalson, ¶176. According to *Fish*, its system identifies and stores “**cartographic locations.**” *E.g.*, Ex-1004, 7:30-41; Michalson, ¶176. *Fish* stores in data archive 10 a “cartographic location corresponding to latitude and longitude coordinates derived from the **GPS** signal.” Ex-1004, 7:30-41, 14:23-27 (claim 21); Michalson, ¶176. *Fish* notes that “location and temporal signals” from GPS receiver 40 are “widely available” in commercial devices, and a “GPS signal for identifying the latitudinal and longitudinal coordinates of the data archive 10 [] may be translated to a geographic location if the secure memory 18 is preloaded with cartographic content.” Ex-1004, 7:42-49;

Michalson, ¶176. A POSITA would have understood *Fish*'s GPS and cartographic locations to include destination, home, or any other addresses where the vehicle containing data archive 10 is located. Michalson, ¶176. Indeed, when a vehicle containing data archive 10 was positioned at a user's home or destination, *Fish*'s stored cartographic or GPS data would be their home or destination address.

Michalson, ¶176.

Second, *Fish* discloses storing **velocity** (speed and direction) data.

Michalson, ¶177. *Fish* stores **acceleration** (change in velocity over time) data.

Ex-1004, 2:58-65, 11:8-29; Michalson, ¶177. *Fish* also stores and encrypts “**speed data**” and multiple types of “**direction data**,” along with “**time**,” to data archive 10. Ex-1004, 11:8-26, 2:61-65; Michalson, ¶178. Further, *Fish* stores latitudinal and longitudinal information over time, which a POSITA would have understood represents motion of the vehicle. Ex-1004, 4:8-14, 7:30-55; Michalson, ¶178. It would have been known and obvious to a POSITA that the stored speed and directional data over time are velocity data. Michalson, ¶178.

C. Claim 12

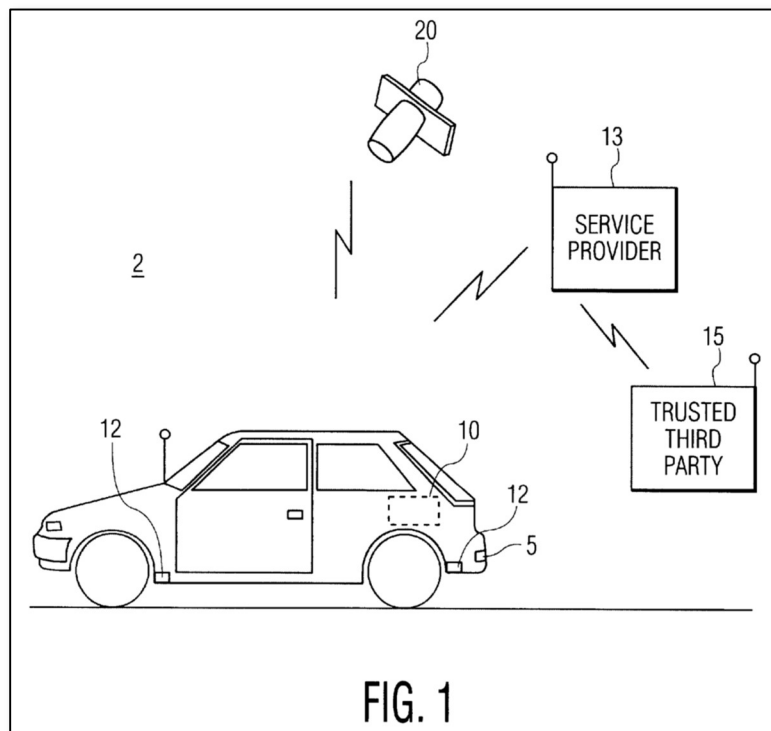
- 1. [12] The device as in claim 1, further comprising a transmission module for transmitting the encrypted location information to an external computing device.**

Fish discloses the device as in claim 1, further comprising a transmission module for transmitting the encrypted location information to an external computing device, as claimed. Michalson, ¶179.

The claimed “transmission module” is a means-plus-function term, with a function of transmitting the encrypted location information to an external computing device and disclosed structure of “a transmission module or connection, e.g., hardwire or wireless, to port the information to a computer.” Ex-1001, 2:4-7; Abstract, 6:26-40; Michalson, ¶180. *Fish* discloses and renders obvious this function and structure.

First, *Fish*’s **service provider transponder 16** is a transmission module of data archive 10, as recited in claim 12. Michalson, ¶181. **Service provider transponder 16** is a “communication module” for transmitting data via antenna 17 to service provider 13, and “[d]ata transmitted to the service provider 13 may include, for example, an electronic signature derived from the sensory data signals and location data.” Ex-1004, 4:43-65; Michalson, ¶181. *Fish* sends encrypted location information to service provider 13. Ex-1004, 5:4-38 (data archive 10 sends composite encrypted sensory and location data to service provider 13), 8:41-52,

10:16-31; Michalson, ¶181. Service provider 13 is an external computing device, as recited in claim 12. Ex-1004, 9:51-55 (service provider 13 comprises processor and memory), Figs. 1, 3; Michalson, ¶181. Indeed, service provider 13 is external to data archive 10:



Ex-1004, Fig. 1; Michalson, ¶181.

Second, *Fish*'s “**emergency transponder 38**” is also a transmission module of data archive 10 for sending location information via antenna 39 to remote computing devices, as recited in claim 12. Ex-1004, 8:9-40, 9:56-65; Michalson, ¶182.

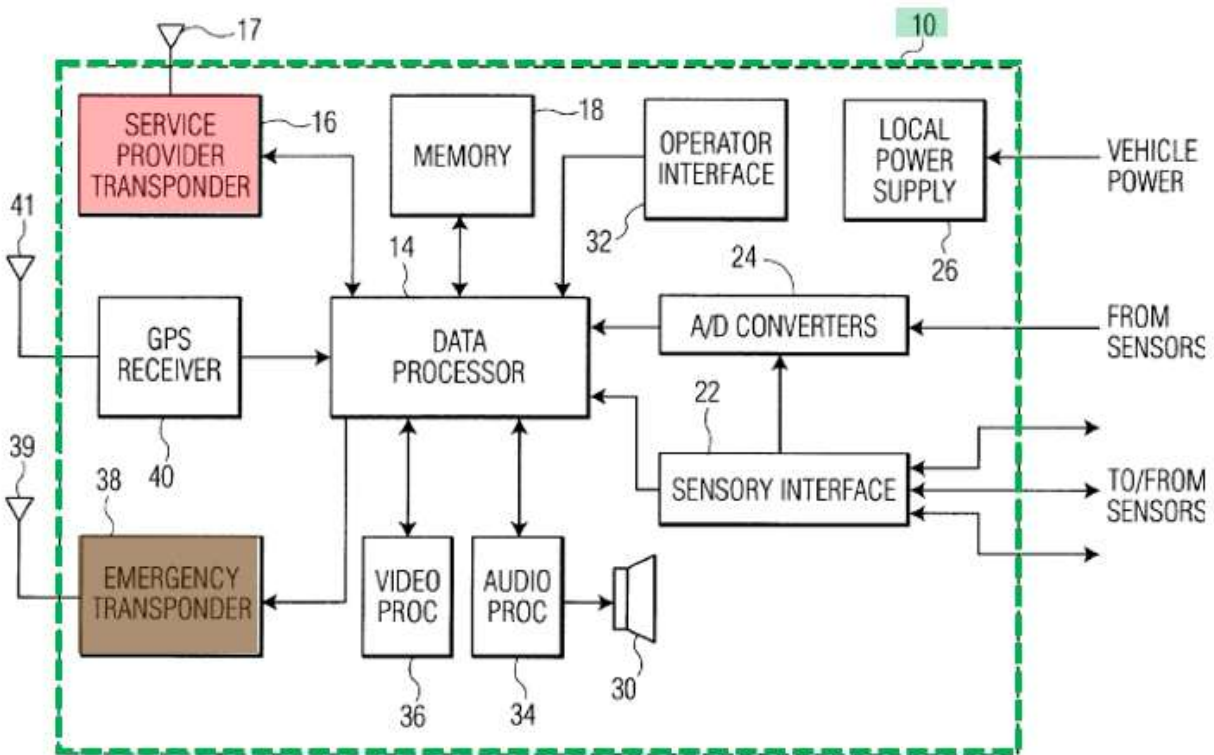


FIG. 2

Ex-1004, Fig. 2; Michalson, ¶182.

D. Claim 13

1. [13pre] A location information device with secure data storage comprising:

Fish discloses and renders obvious [13pre]. *See supra* claim [1pre];

Michalson, ¶183.

2. [13a] a housing;

Fish discloses and renders obvious [13a]. *See supra* claim [1a]; Michalson,

¶184.

3. **[13b] a locational information module for determining location information of the device, the determined location information being at least one route traveled by the device;**

Fish discloses and renders obvious [13b]. *See supra* claim [1b]; Michalson, ¶185.

4. **[13c] an encryption module for encrypting the determined location information;**

Fish discloses and renders obvious [13c]. *See supra* claim [1c]; Michalson, ¶186.

5. **[13d] a storage module for storing the encrypted location information; and**

See supra claim [1d]. Unlike claim 1, claim 13 does not recite that the “storage module” is “removable.” Michalson, ¶187. Claim 13 is thus broader in this respect and is taught by *Fish*. *Id.*

6. **[13e] a processing module for sending the encrypted location information to the storage module and retrieving the encrypted location information from the storage module.**

Fish discloses and renders obvious [13e]. *See supra* claim [1e]; Michalson, ¶188.

E. Claim 14

1. **[14] The device as in claim 13, further comprising a transmission module for transmitting the encrypted location information from the storage module to an external computing device.**

Fish discloses and renders obvious claim 14. *See supra* claim 12. Unlike claim 12, claim 14 more specifically recites that the encrypted location information comes “from the storage module.” Michalson, ¶189. This is taught by *Fish* for the reasons discussed regarding claim 12—i.e., *Fish*’s encrypted location information is stored in memory 18. *See supra* claim [1d]; Michalson, ¶189. This encrypted location information is then transmitted via *Fish*’s various transmission modules, as discussed above regarding claim 12. *See supra* claim 12; Michalson, ¶189.

F. Claim 19

1. **[19pre] A system for controlling and storing location information comprising:**

Fish discloses a system for controlling and storing location information, as recited in [19pre]. Michalson, ¶190. *Fish*’s data archive 10 is a system for controlling and storing location information, including GPS coordinates and identified cartographic locations. *See supra* claim [1pre]; Michalson, ¶190.

2. **[19a] a location information device with secure data storage comprising:**

Fish discloses and renders obvious [19a]. *See supra* claim [1pre]; Michalson, ¶191.

3. [19b] a housing;

Fish discloses and renders obvious [19b]. *See supra* claim [1a]; Michalson, ¶192.

4. [19c] a locational information module for determining location information of the location information device, the determined location information being at least one route traveled by the location information device;

Fish discloses and renders obvious [19c]. *See supra* claim [1b]; Michalson, ¶193.

5. [19d] an encryption module for encrypting the determined location information;

Fish discloses and renders obvious [19d]. *See supra* claim [1c]; Michalson, ¶194.

6. [19e] a removable storage module for storing the encrypted location information, the removable storage module being removably disposed in the housing; and

Fish discloses and renders obvious [19e]. *See supra* claim [1d]; Michalson, ¶195.

7. [19f] a processing module for sending the encrypted location information to the removable storage module removably disposed in the housing and retrieving the encrypted location information from [sic] the removable storage module; and

Fish discloses and renders obvious [19f]. *See supra* claim [1e]; Michalson, ¶196.

8. [19g] a computing device comprising:

Fish discloses and renders obvious a computing device, as recited in [19g]. Michalson, ¶197. *Fish* uses “facilities” to “directly read the contents of the memory.” Ex-1004, 7:6-29; Michalson, ¶197. A POSITA would have understood the “facilities” to be or be part of a computing device, as claimed. Michalson, ¶198.

9. [19h] a reader configured for reading the removable storage module of the location information device when [t]he removable storage module [i]s removably disposed in the reader; and

Fish discloses and renders obvious a reader configured for reading the removable storage module of the location information device when the removable storage module is removably disposed in the reader, as claimed. Michalson, ¶199. Indeed, this is a core purpose of *Fish*. Ex-1004, 1:28-33, 2:16-22, 10:22-25. *Fish*’s “secure memory 18 is a removable non-volatile memory device” (e.g., SD memory), and “is removable to allow for easy **access to the data** after an accident” as well as to be accessible to “facilities (e.g. an external port) provided to directly **read the contents of the memory** without removing it from the data archive 10.” Ex-1004, 7:7-17; Michalson, ¶¶198-200.

Fish’s “facilities” will “directly read the contents of memory” through a port and would have been equipped to read the SD card. Michalson, ¶201. Standard

computing devices at the time included the ability to read memory through external ports and SD cards when inserted. Michalson, ¶201. A POSITA would have found including SD card reading capabilities disclosed and obvious in light of this common technology and *Fish*'s goal of enabling third parties to identify conditions preceding an accident. Ex-1004, 1:6-33, 2:16-24, 7:23-29, 11:8-29; Michalson, ¶201.

10. [19i] a processor configured to execute a decryption program for decrypting the encrypted location information on the removable storage module removably disposed in the reader.

Fish discloses and renders obvious a processor configured to execute a decryption program for decrypting the encrypted location information on the removable storage module removably disposed in the reader, as claimed. Michalson, ¶202.

Fish decrypts stored encrypted data using cryptographic keys. Ex-1004, 3:50-4:7; Michalson, ¶203. A POSITA would have found it disclosed and obvious to include a decryption program on a device reading *Fish*'s SD card based on these teachings and *Fish*'s goal of enabling parties (e.g., law enforcement or insurers) to identify conditions preceding an accident. Ex-1004, 1:6-33, 2:16-24, 7:23-29, 11:8-29; Michalson, ¶203.

G. Claim 20

1. [20] The system as in claim 19, wherein the location information further includes at least one of a home address, destination addresses and velocity of the device at predetermined times.

Fish discloses and renders obvious claim 20. *See supra* claim 11. Michalson, ¶204.

H. Claim 21

1. [21] The system as in claim 19, wherein the computing device further comprises a memory for storing a plurality of geographical maps and the processor is configured to overlay the location information on at least one of the plurality of geographical maps.

Fish discloses and renders obvious the system as in claim 19, wherein the computing device further comprises a memory for storing a plurality of geographical maps and the processor is configured to overlay the location information on at least one of the plurality of geographical maps, as claimed. Michalson, ¶205.

Fish's data processor 14 uses a portion of secure memory 18 with **preloaded cartographic content** in conjunction with **GPS information** to identify a cartographic (map) location:

Although the primary function of the secure memory 18 is to store the operational, situational and environmental data derived from the sensors 12, In the exemplary embodiment, a portion of secure memory 18 is reserved for use by the data processor 14 to enable **GPS functionality**, sensory data signal conditioning, and audio/video

processing functionality. In this embodiment, **cartographic content may be preloaded into the secure memory 18 upon manufacture for use in conjunction with data processor 14 and GPS receiver 40 for identifying a cartographic location corresponding to latitude and longitude coordinates derived from the GPS signal.**

Ex-1004, 7:30-41; Michalson, ¶206.

It would have been obvious that a device reading *Fish*'s stored cartographic data in conjunction with GPS data would—as taught by *Fish* itself—include preloaded cartographic maps stored in data archive 10 to achieve *Fish*'s goals of representing and recreating vehicle travel information for later analysis. Ex-1004, 7:30-41; Michalson, ¶206. This overlaying of GPS data with map data was obvious and conventional. Ex-1004, 1:6-33, 2:16-24, 3:21-27, 6:25-29, 7:23-29, 8:2-9, 8:49-52, 10:19-25, 10:54-57, 11:8-29; Michalson, ¶207.

I. Claim 22

1. [22pre] A system for controlling and storing location information comprising:

Fish discloses and renders obvious [22pre]. *See supra* claim [19pre]; Michalson, ¶208.

2. [22a] a location information device with secure data storage comprising:

Fish discloses and renders obvious [22a]. *See supra* claim [1pre]; Michalson, ¶209.

3. [22b] a housing;

Fish discloses and renders obvious [22b]. *See supra* claim [1a]; Michalson, ¶210.

4. [22c] locational information module for determining location information of the location information device, the determined location information being at least one route traveled by the location information device;

Fish discloses and renders obvious [22c]. *See supra* claim [1b]; Michalson, ¶211.

5. [22d] an encryption module for encrypting the determined location information;

Fish discloses and renders obvious [22d]. *See supra* claim [1c]; Michalson, ¶212.

6. [22e] a storage module for storing the encrypted location information;

Fish discloses and renders obvious [22e]. *See supra* claim [1d]; Michalson, ¶213. Unlike claim 19, which recites a “removable” “storage module,” claim 22 more broadly recites a “storage module,” which *Fish* teaches as discussed above. Michalson, ¶213.

7. [22f] a processing module for sending the encrypted location information to the storage module and retrieving

the encrypted location information from the storage module; and

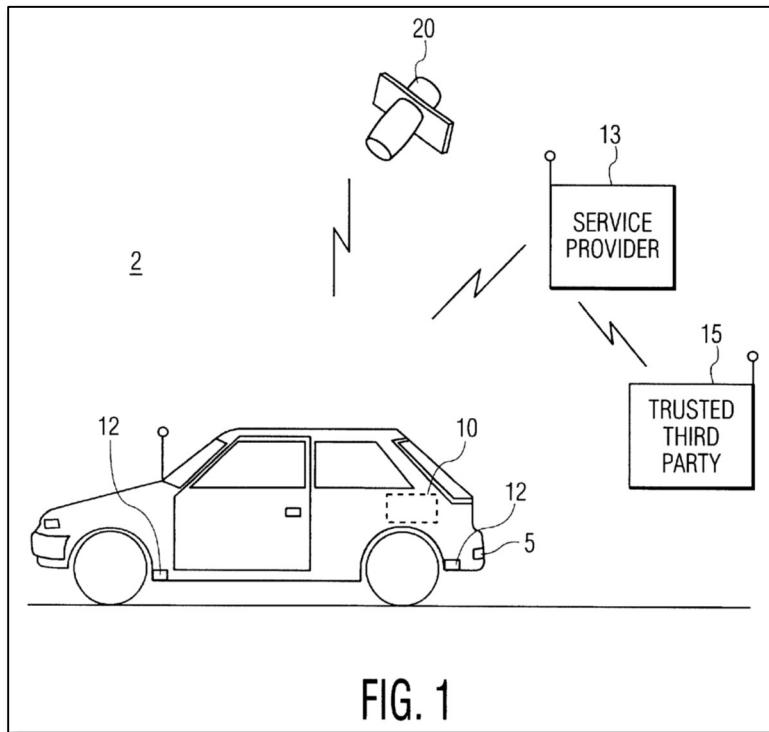
Fish discloses and renders obvious [22f]. *See supra* claim [1e]; Michalson, ¶214. Unlike claim 19, which recites a “removable” “storage module,” claim 22 more broadly recites a “storage module,” which *Fish* also teaches. Michalson, ¶214.

8. [22g] a transmission module for transmitting the encrypted location information from the storage module to an external computing device; and

Fish discloses and renders obvious [22g]. *See supra* claim 12; Michalson, ¶215.

9. [22h] the external computing device comprising: a connectivity device configured for receiving the encrypted location information form [sic] the location information device; and

Fish discloses and renders obvious the external computing device comprising a connectivity device configured for receiving the encrypted location information from the location information device, as claimed. Michalson, ¶216. *Fish*’s service provider 13 is an external computing device that includes a “data receiver,” which is a “connectivity device” as claimed. Ex-1004, 9:51-55, Fig. 3; Michalson, ¶217. Such a connectivity device is required for service provider 13 to communicate with data archive 10, as disclosed. Ex-1004, 4:43-65, 5:4-38, 8:41-52, 9:51-55, 10:16-31, Figs. 1, 3; Michalson, ¶217.



Ex-1004, Fig. 1.

Further, *Fish*'s "**emergency transponder 38**" is a transmission module of data archive 10 for sending location information to additional external computing devices, as claimed. *Id.*, 8:9-40, 9:56-65; Michalson, ¶218. Such external computing devices would necessarily have a connectivity device configured for receiving the encrypted location information from *Fish*'s data archive 10. Michalson, ¶218.

10. [22i] a processor configured to execute a decryption program for decrypting the encrypted location information received from the location information device.

Fish discloses and renders obvious a processor configured to execute a decryption program for decrypting the encrypted location information received from the location information device, as claimed. Michalson, ¶219.

Fish's external computing device includes a processor, as claimed. Ex-1004, 9:51-55, Fig. 3; Michalson, ¶220. Data archive 10 encrypts the data according to the key received from the service provider 13, and the processor of external service provider 13 decrypts the received encrypted data. Ex-1004, 9:51-10:36, Fig. 3; Michalson, ¶220. This is both disclosed and inherent in *Fish*, because service provider 13 requires a way to decrypt the received encrypted location data. *Id.*

VIII. Ground 2: *Fish* In View of *Ziv* (Claims 2-4, 15-17)

Claims 2-4 and 15-17 are unpatentable under § 103 in view of *Fish* and *Ziv*, alone or with the knowledge of a POSITA.

A. Motivation to Combine *Fish* and *Ziv*

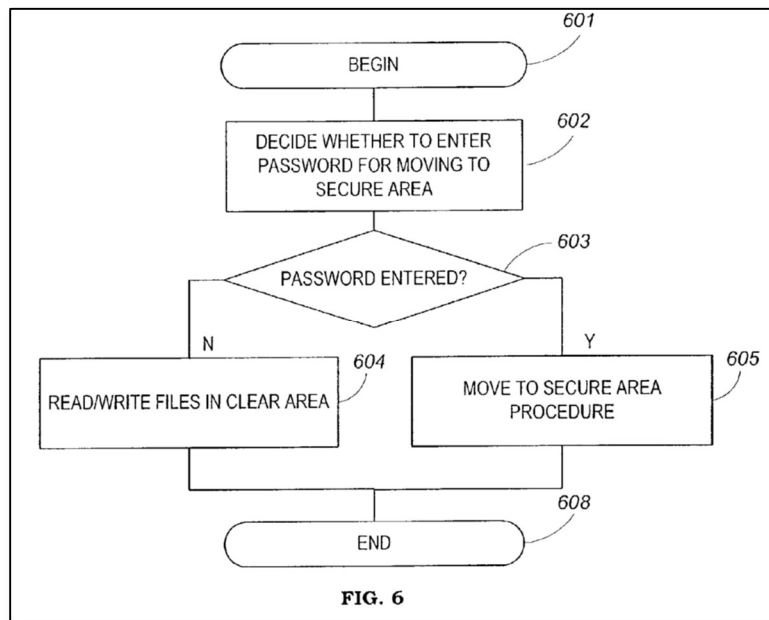
A POSITA would have been motivated to use *Ziv*'s password protection techniques to further enhance security in *Fish*. Michalson, ¶222. It would have been obvious and beneficial to utilize *Fish*'s "password" (used for data deletion) for other purposes as well, such as selective encryption and decryption of data, as

taught by *Ziv*, to ensure that these operations were performed with proper security.

Id.

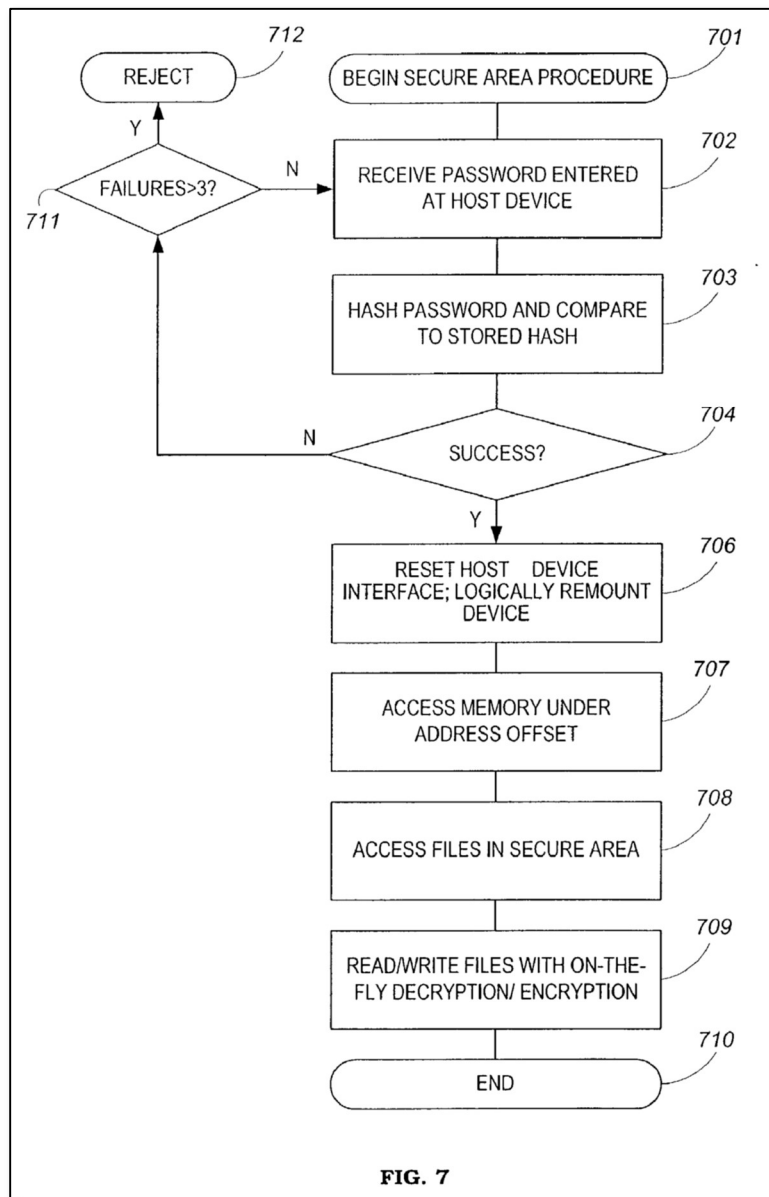
Ziv and *Fish* each disclose using removable (i.e., portable) data storage devices. Ex-1005, Abstract, ¶¶[0001], [0025]; Ex-1004, 7:6-29; Michalson, ¶223. Both describe techniques for ensuring data security through the use of encryption and user passwords. Ex-1005, Abstract, ¶¶[0026], [0031], [0033], [0037]-[0045]; Ex-1004, 3:49-4:7, 5:39-6:3; Michalson, ¶223. A POSITA implementing *Fish*'s data security techniques would have found it obvious and beneficial to enhance security with *Ziv*'s additional password protection techniques. Michalson, ¶¶223-224. This would also enhance flexibility and convenience by enabling different options for protecting encrypted and decrypted data. *Id.*

Fish teaches that, “[t]o ensure that data is not deleted accidentally, . . . the user may be required to enter a password or personal identification number (PIN) via the operator interface 32 before being allowed to delete any data.” Ex-1004, 5:60-64; Michalson, ¶225. The user may “confirm any command to delete the data before the data is actually deleted.” Ex-1004, 5:64-66; Michalson, ¶225. *Fish*'s password thus helps ensure the security of stored data. Michalson, ¶225. A POSITA would have found it obvious and advantageous to combine this with *Ziv*'s use of a password to move data to a secure storage area. Michalson, ¶225. *Ziv* teaches this in Figure 6:



Ex-1005, Fig. 6.

Similar to *Fish*'s secure storage of data in memory 18, *Ziv* stores data in "secure [user] area 122." *Id.*, ¶[0026]; Michalson, ¶226. Secure user area 122 stores "secure user data accessible only upon the provision of a password or biometric signature." Ex-1005, ¶[0026]; Michalson, ¶226; *see also* Ex-1005, ¶¶[0037], [0039], [0040], [0043]; Michalson, ¶¶226-227.



Ex-1005, Fig. 7.

Ziv's Figure 10 "expands the procedure of step 709 of FIG. 7" by describing "respectively on-the-fly encryption/decryption of data moving from/to host device 101 to/from secure data area 410." Ex-1005, ¶[0045]; Michalson, ¶[227. In **step 952** of Figure 10, the encrypted key is retrieved and decrypted using the password. *Id.*

The key may then be used to either encrypt or decrypt data in step 953. *Id.*

Encryption is performed in steps 961-964 and **decryption is performed in steps 972-973**. *Id.*

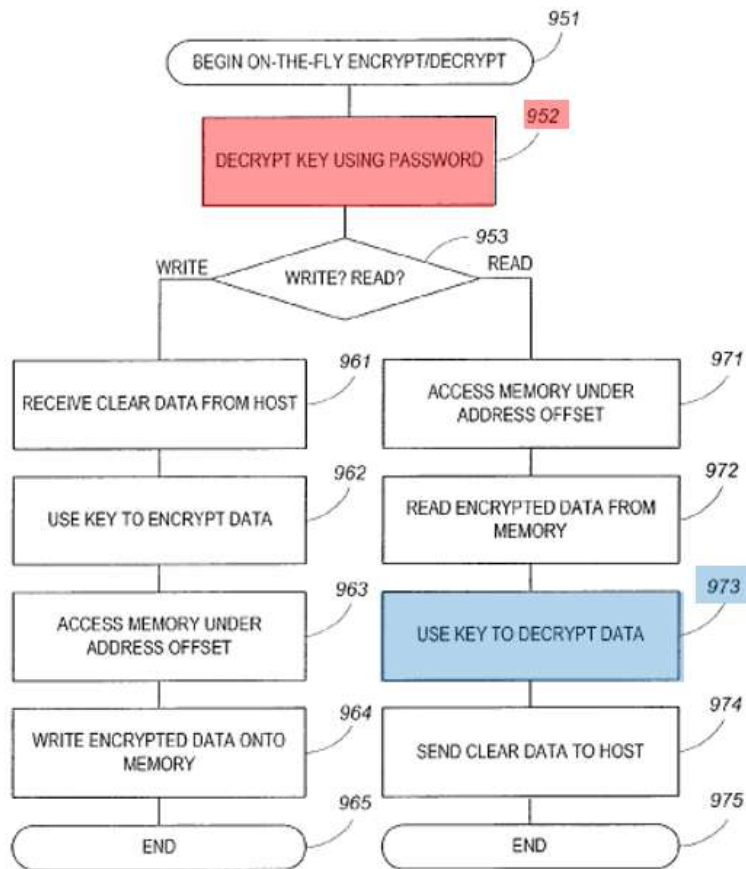


FIG. 10

Id., Fig. 10.

In this way, the user's **password**—as taught by *Fish*—selectively encrypts and **decrypts** stored data. Michalson, ¶¶227-228. It would have been obvious and beneficial to a POSITA to use a password in this manner, especially given *Fish*'s teaching of a password for selective data deletion. *Id.*

B. Claim 2

1. **[2] The device as in claim 1, further comprising an input module disposed on the housing configured for receiving a code string input by a user, wherein the user inputted code string is used for encrypting and decrypting the location information stored in the removable storage module.**

Fish in view of *Ziv* discloses and renders obvious the device as in claim 1, further comprising an input module disposed on the housing configured for receiving a code string input by a user, wherein the user inputted code string is used for encrypting and decrypting the location information stored in the removable storage module, as claimed. *E.g.*, Ex-1004, 5:39-6:3, Fig. 2; Michalson, ¶229.

The claimed “input module” is a means-plus-function term, with a function of receiving a code string input by a user, wherein the user inputted code string is used for encrypting and decrypting the location information stored in the removable storage module, and disclosed structure of “input module 106, [which] includes a plurality of buttons 108 for inputting data and navigating through a plurality of menus and/or maps.” Ex-1001, 3:14-16; Michalson, ¶230. This function and structure are disclosed by *Fish*.

Fish discloses an input module disposed on the housing configured for receiving a code string input by a user. Michalson, ¶231. **Data archive 10** includes

operator interface 32, which is an “input module” as claimed. Ex-1004, 5:39-6:3,
Fig. 2; Michalson, ¶231.

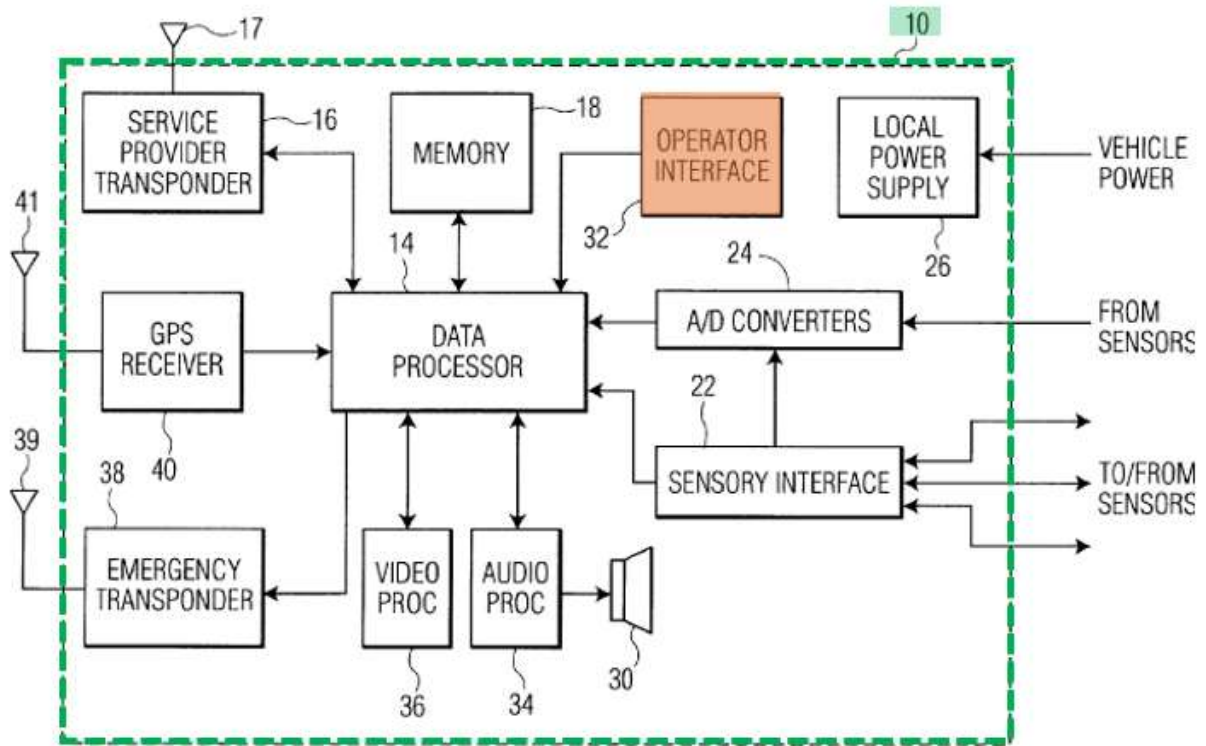
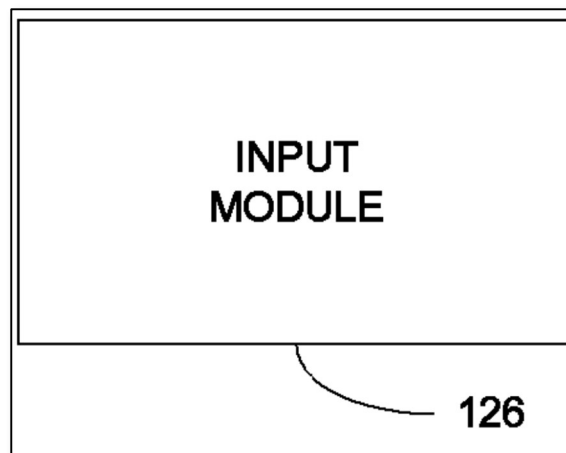


FIG. 2

Ex-1004, Fig. 2; Michalson, ¶231.

“The **data archive 10** of the exemplary embodiment is preferably housed in a sealed cabinet (not shown).” Ex-1004, 3:2-3; Michalson, ¶232. The housing “is desirably fire and water resistant and designed to offer significant resistance to crush forces typically encountered in catastrophic vehicle wrecks.” Ex-1004, 3:6-8; Michalson, ¶232. A POSITA would have understood that *Fish*’s **operator interface 32** is disposed “on the housing” in the same manner as the ’192 patent

itself. Michalson, ¶232. The patent discloses only that its various components are “disposed in a generally rectangular housing 102,” without specifics. Ex-1001, 3:7-9, Fig. 2 (element 126); Michalson, ¶232. The claimed input module 126 is shown below, and the input module 106 of Figure 1 is described as having buttons but no particular physical attributes. Ex-1001, 3:14-16; Michalson, ¶232.



Ex-1001, Fig. 2; Michalson, ¶232.

Comparably, *Fish*’s **operator interface 32** also has buttons. Ex-1004, 5:46-51 (“push-button switches”); Michalson, ¶233. With more detail than the ’192 patent, *Fish*’s controls 32 “may be physically located on the data archive 10, or positioned at a readily accessible location of the vehicle 5, such as an area of the passenger or engine compartments.” Ex-1004, 5:51-54; Michalson, ¶233.

Fish’s **data archive 10** receives “control parameters from **operator interface 32**” to delete or deactivate data. Ex-1004, 5:39-54; Michalson, ¶234. **Operator interface 32** “provide[s] an operator means for adjusting/controlling the

operation of **data archive 10**” and allows one to “control how and when the [stored] data is used.” Ex-1004, 5:39-60; Michalson, ¶234. *Fish*’s “controls may be physically located on the **data archive 10**,” i.e., disposed on the housing of the location information device, as claimed. *Id.*

For data deletion in *Fish*, “the user may be required to enter a password or personal identification number (PIN) via the **operator interface 32**.” Ex-1004, 5:55-6:3; Michalson, ¶235. A password or PIN is a code string input by the user, as claimed. Michalson, ¶235. The ’192 patent itself describes a “code string” as any characters a user may choose. Ex-1001, 5:4-9; Michalson, ¶235.

Fish’s secure storage of data in memory 18 is similar to *Ziv*’s storage of data in “secure [user] area 122.” Ex-1005, ¶[0026]; Michalson, ¶237. *Ziv*’s secure user area 122 stores “secure user data accessible only upon the provision of a password or biometric signature.” *Id.*; see also Ex-1005, ¶¶[0037], [0039], [0040]; Michalson, ¶237.

A POSITA would have found it obvious to use *Fish*’s password for other data security purposes, especially controlling encryption and decryption of stored data. Michalson, ¶236. *Ziv*’s portable storage device 110, like *Fish*’s data archive 10, includes a user interface for receiving a password. *Id.* *Ziv* teaches entering a password using an interface such as a screen. Ex-1005, ¶[0031]; Michalson, ¶236. As discussed above, *supra* §VIII.A, *Fish* in view of *Ziv* teaches

that the password (i.e., “user inputted code string”) is used for controlling encryption and decryption of location information stored in the removable storage module. *Id.*; *id.* ¶¶236-37. To achieve this, *Ziv*’s selective encryption and decryption of stored data (e.g., *Fish*’s stored location information) would be performed. *Id.*

The password is used with a clear key to encrypt stored data in *Ziv*. Ex-1005, ¶¶[0043]-[0045]; Michalson, ¶238. The encrypted key is retrieved and decrypted using the password, and may then be used to either “encrypt[]” or “decrypt[]” data via step 953. Ex-1005, ¶¶[0043]-[0045]; Michalson, ¶238. Encryption is performed in steps 961-964 and decryption is performed in steps 972-973. Ex-1005, ¶¶[0043]-[0045]; Michalson, ¶238. Thus, the password—as in *Fish*—is used to selectively encrypt and decrypt stored data. Michalson, ¶238. A POSITA would have readily and obviously appreciated this beneficial use of a password, especially given *Fish*’s use of a password for selective data deletion. *Id.*

C. Claim 3

1. **[3] The device as in claim 1, further comprising a user verification module for verifying the identity of user of the device, wherein the processing module selectively decrypts the location information stored in the removable storage module based on the identity of the user.**

Fish in view of *Ziv* discloses and renders obvious the device as in claim 1, further comprising a user verification module for verifying the identity of user of

the device, wherein the processing module selectively decrypts the location information stored in the removable storage module based on the identity of the user, as claimed. Michalson, ¶239.

The claimed “user verification module” is a means-plus-function term, with a function of verifying the identity of user of the device, and disclosed structure of “user verification module 130” that “will indicate and verify the identity of the user of the device 100.” Ex-1001, 5:49-59; Michalson, ¶240. *Fish* in view of *Ziv* discloses this function and structure multiple ways.

First, as discussed regarding claim 2, *Fish*’s operator interface 32 allows input of a password or PIN. Ex-1004, 5:55-6:3; Michalson, ¶241. A password or PIN is information that verifies the identity of a user, as claimed. *Id.* *Fish* in view of *Ziv* thus teaches using this password to selectively encrypt or decrypt data, such as *Fish*’s stored location data. *Id.*; *see supra* claim 2; Michalson, ¶¶241-243.

Ziv further discloses and renders obvious a user verification module for verifying the identity of a user of the device in *Ziv*’s disclosure of alternatives to passwords, such as “biometric identification data.” Ex-1005, ¶[0006]; Michalson, ¶244. *Ziv* explains a user may provide “a password or biometric signature.” Ex-1005, ¶[0026]. The user verification module of *Ziv* is “a biometric reader such as a fingerprint reader.” Ex-1005, ¶[0031]; Michalson, ¶244. *Ziv* teaches using biometric parameters as an alternative to a password for selectively encrypting and

decrypting stored data as discussed regarding claim 2. Ex-1005, ¶¶[0033], [0037]-[0038]; Michalson, ¶244. These biometric-based techniques of *Ziv* also disclose that the processing module of *Fish* selectively decrypts the location information stored in the removable storage module based on the identity of the user, as recited in claim 3. Michalson, ¶244.

A POSITA would have been motivated to use *Ziv*'s password techniques for selective encryption and decryption of *Fish*'s stored location data for the reasons discussed above regarding claim 2. Michalson, ¶244. Further, using *Ziv*'s biometric-based techniques for selective encryption and decryption of *Fish*'s stored location data would have been beneficial and obvious for other reasons, such as accepting biometric input (e.g., a fingerprint or retina scan) instead of a password to obviate a user manually typing password characters. Michalson, ¶244. A POSITA would have appreciated the benefits of obviating a full QWERTY keyboard in confined spaces, such as an automobile. Michalson, ¶244. Using a biometric identifier in place of a password, per *Ziv*, would also add heightened security to *Fish* because it is harder to “hijack” or copy biometric details than a password. Michalson, ¶244. A POSITA would thus have found it obvious and beneficial to use *Ziv*'s biometric selective encryption and decryption techniques for *Fish*'s stored location data. Michalson, ¶244.

D. Claim 4

- 1. [4] The device as in claim 3, wherein the user verification module executes a password protection algorithm for verifying the identity of the user of the device.**

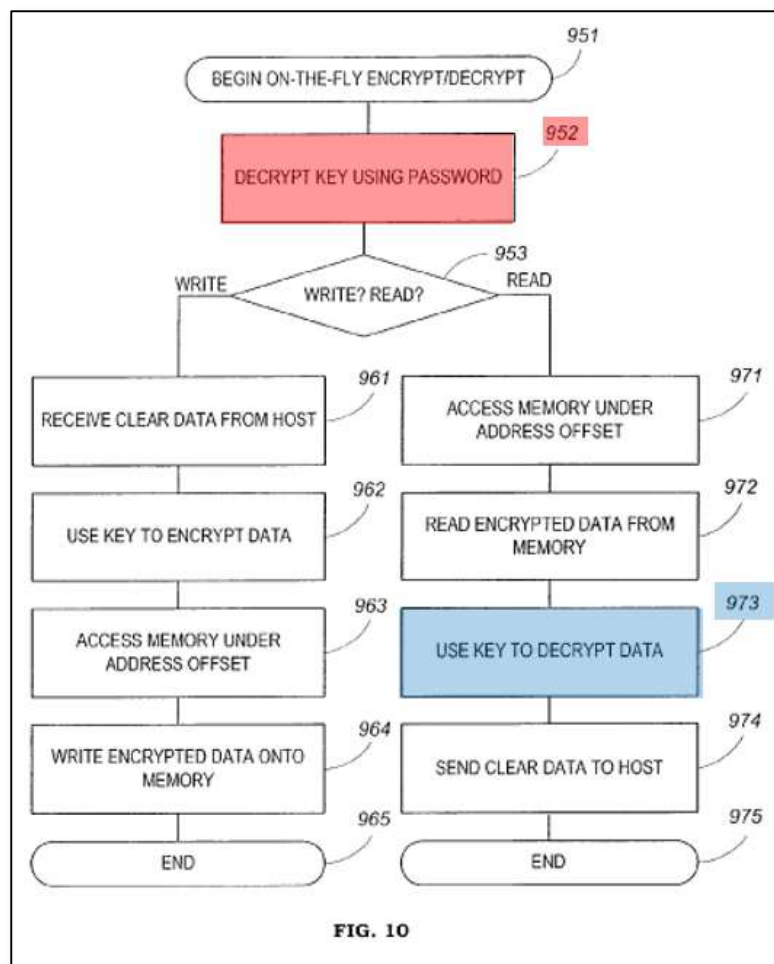
Fish in view of *Ziv* discloses and renders obvious the device as in claim 3, wherein the user verification module executes a password protection algorithm for verifying the identity of the user of the device, as claimed. Michalson, ¶245.

First, *Fish* discloses “the user may be required to enter a password or personal identification number (PIN) via the operator interface 32.” Ex-1004, 5:55-6:3; Michalson, ¶246. Password-based authentication is a password protection algorithm for verifying user identity, as claimed, as discussed above in connection with claims 2 and 3. Michalson, ¶246. A POSITA would have understood that *Fish*’s verification of a password involves executing a password protection algorithm, as claimed. Michalson, ¶246. The ’192 patent discloses nothing specific about any claimed algorithm, only requiring that it somehow verify the password itself. Ex-1001, 5:48-6:7; Michalson, ¶¶246-247.

Second, *Fish* in view of *Ziv* also discloses and renders obvious the user verification module executing a password protection algorithm for verifying the identity of the user of the device. *Fish* in view of *Ziv* teaches this at least two ways, as discussed regarding claims 2 and 3. For example, *Fish* in view of *Ziv* teaches using *Ziv*’s password verification techniques to identify a user and selectively

decrypt data. Michalson, ¶248; *see also supra* claims 2-3. A POSITA would have been motivated to use *Ziv*'s password protection related techniques to enhance the password protection and encryption techniques of *Fish* as described regarding claims 2 and 3, including enhanced data security and better user-friendliness.

Michalson, ¶¶248-250; Ex-1005, ¶¶[0043], [0045], Fig. 10.



Ex-1005, Fig. 10 (annotated).

Further, *Fish* in view of *Ziv* also teaches using *Ziv*'s biometric verification techniques to identify a user and selectively decrypt data. Ex-1005, ¶[0006];

Michalson, ¶248. In an example, a user provides “a clear, un-hashed password or biometric signature.” Ex-1005, ¶[0026]; Michalson, ¶251. For this, *Ziv* teaches using “a biometric reader such as a fingerprint reader.” Ex-1005, ¶[0031]; Michalson, ¶251. *Ziv* also teaches using biometric parameters as an alternative to a password for verifying a user’s identity. Ex-1005, ¶¶[0033], [0037]-[0038]; Michalson, ¶251.

A POSITA would have been motivated to use *Ziv*’s password techniques for verifying a user’s identity as discussed above. Michalson, ¶251. Further, using *Ziv*’s biometric-based techniques for user verification would have been beneficial and obvious for other reasons, such as accepting biometric input (e.g., a fingerprint or retina scan) instead of a password, obviating the need for a manually typed password—especially helpful in a vehicle lacking a full keyboard. Michalson, ¶251. Further, using a biometric identifier in lieu of a password, per *Ziv*, would strengthen security for *Fish* because it is harder to misappropriate or copy biometric details than a password. Michalson, ¶251. A POSITA thus would have found it obvious and helpful to use *Ziv*’s biometric user verification in *Fish*. Michalson, ¶251.

E. Claim 15

1. **[15] The device as in claim 14, further comprising an input module disposed on the housing configured for receiving a code string input by a user, wherein [t]he user inputted code string is used for encrypting and decrypted the location information stored in the storage module.**

Fish discloses and renders obvious claim 15. *See supra* claim 2. Unlike claim 2, claim 15 does not recite that its storage module is “removable.” Claim 15 is thus broader than claim 2 and taught by *Fish* as explained above regarding claim 2. Michalson, ¶252.

F. Claim 16

1. **[16] The device as in claim 14, further comprising a user verification module for verifying the identity of [the] user of the device, wherein the processing module selectively decrypts the location information stored in the storage module based on the identity of the user.**

Fish discloses and renders obvious claim 16. *See supra* claim 3. Unlike claim 3, claim 16 does not recite that its storage module is “removable.” Claim 16 is thus broader than claim 3 and taught by *Fish* as explained above regarding claim 3. Michalson, ¶253.

G. Claim 17

1. **[17] The device as in claim 16, wherein [t]he user verification module executes a password protection algorithm for verifying the identity of the user of the device.**

Fish discloses and renders obvious claim 17. *See supra* claim 4. Michalson, ¶254.

IX. Ground 3: *Fish* In View of *Ziv* and *Gehlot* (Claims 5-8, 18)

Claims 5-8 and 18 are unpatentable under § 103 in view of *Fish*, *Ziv*, and *Gehlot*, alone or with the knowledge of a POSITA.

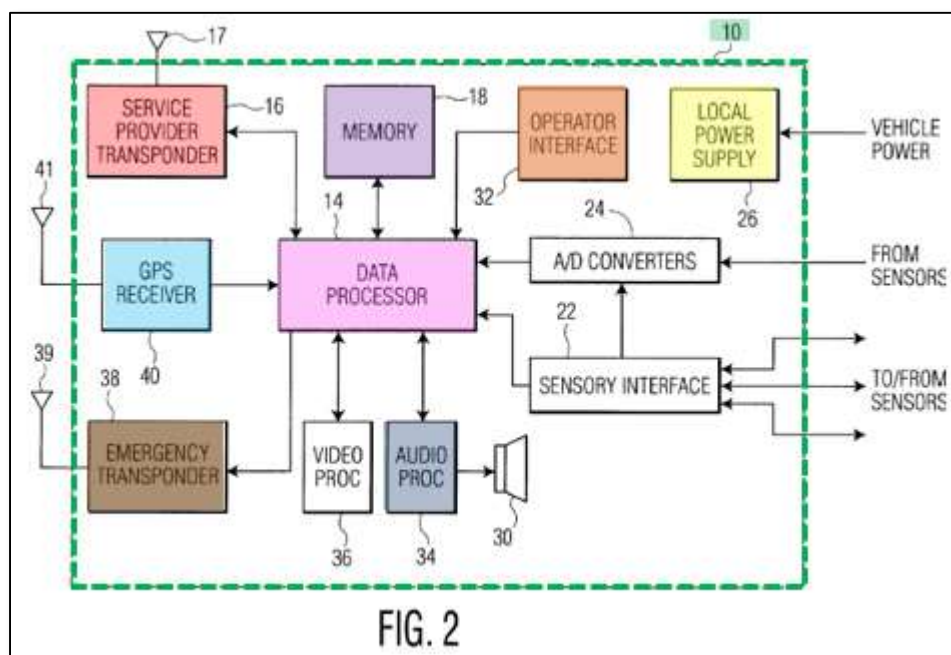
A. Motivation to Combine *Fish*, *Ziv*, and *Gehlot*

A POSITA would have been motivated to use *Gehlot*'s identity capture device and biometric authentication methods to identify users for restricting access to encrypted data on *Fish*'s data archive 10. Michalson, ¶256. *Fish* and *Gehlot* have similar goals and techniques—*Gehlot* uses vehicle-based processing unit 3 to capture vehicle data from vehicle components, including a GPS module 14, Ex-1006, 2:14-16, 3:43-55, 4:37-47, 6:51-58, Figs. 1 & 4, while *Fish* uses vehicle-based data archive 10 including data processor 14, Ex-1004, 4:22-29, 4:51-57, 6:18-29, 6:63-7:5, Figs. 1 & 2; Michalson, ¶257. *Gehlot*'s collected data may be stored at the vehicle (e.g., storage device 7) or transmitted to external entities (e.g., central database 16, D.O.T. or toll collectors 40, car manufacturer 43, law enforcement 42, vehicle insurance 44, DMV 45, or hospital 46), Ex-1006, 4:48-52, 4:64-5:25, Figs. 1 & 4, while *Fish*'s data archive 10 likewise gathers data from a variety of vehicle-based electronic units, including GPS receiver 40, which may be stored locally (e.g., in memory 18) or transmitted to external entities (e.g., service provider 13 or trusted third party 15), Ex-1004, 3:10-27, 4:22-29, 4:43-65, 5:16-26, 5:39-44, 7:6-41, Figs. 1 & 2; Michalson, ¶257. A POSITA would thus have

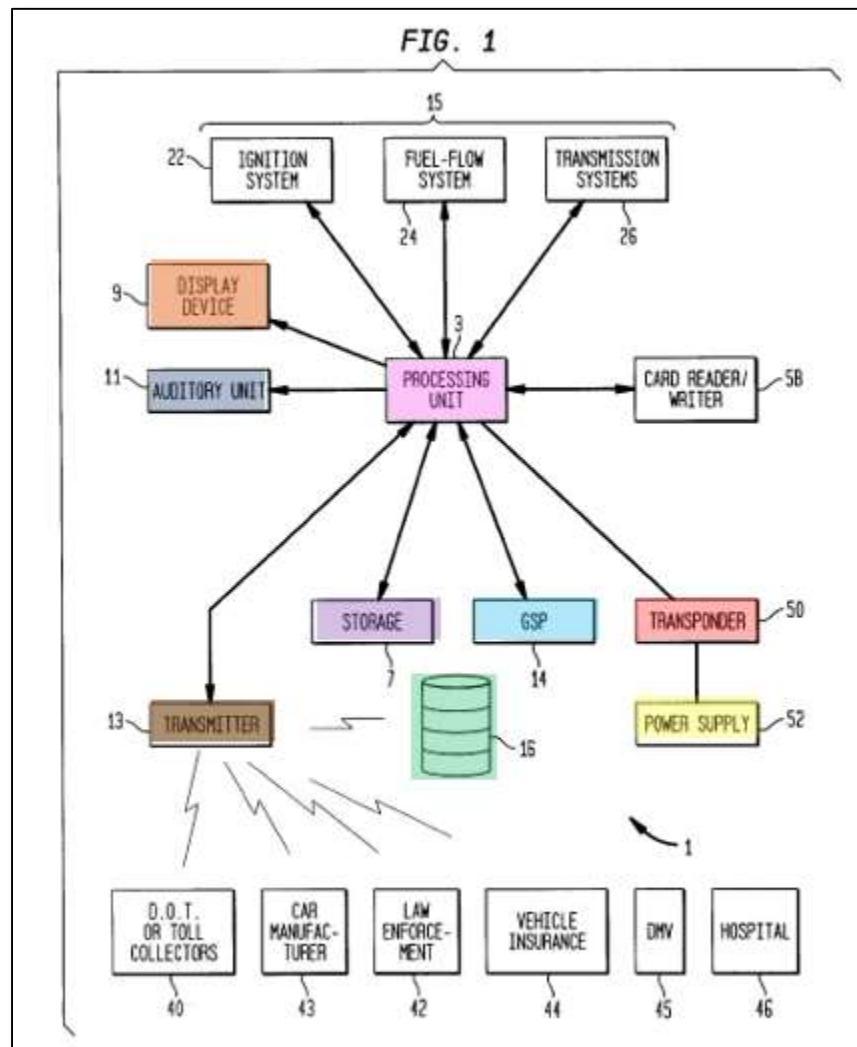
appreciated that *Fish* and *Gehlot* are in the same field of endeavor and relate to similar techniques. Michalson, ¶257.

A POSITA in possession of *Fish* and *Ziv* would have looked to *Gehlot* for additional known techniques to enhance security and privacy of data on *Fish*'s data archive 10. Michalson, ¶258. *Fish* and *Gehlot* are directed to securely storing vehicle location (and other) data. Ex-1004, 4:22-29, 5:27-32, 7:30-52, Figs. 1-2; Ex-1006, 2:1-46, 3:5-42, 4:37-53; Michalson, ¶258. *Gehlot* stores vehicle tracking information so location information can be shared, as with *Fish*'s methods. Ex-1006, 2:14-16, 4:64-5:19, 5:34-67; Michalson, ¶258. Both describe assisting third parties, e.g., law enforcement and insurers, following accidents or theft. Ex-1004, 1:6-33, 2:16-24, 7:23-29, 10:67-11:29; Ex-1006, 1:38-58, 2:1-46, 4:64-5:19; Michalson, ¶258.

Further, *Fish* and *Gehlot* disclose the same basic hardware, and a POSITA would have been familiar with *Gehlot*'s system and related software, which were common by the time of *Fish*. Michalson, ¶259. Both contain a **data processor**, **memory**, **transponder**, **emergency transmitter**, and **GPS**.



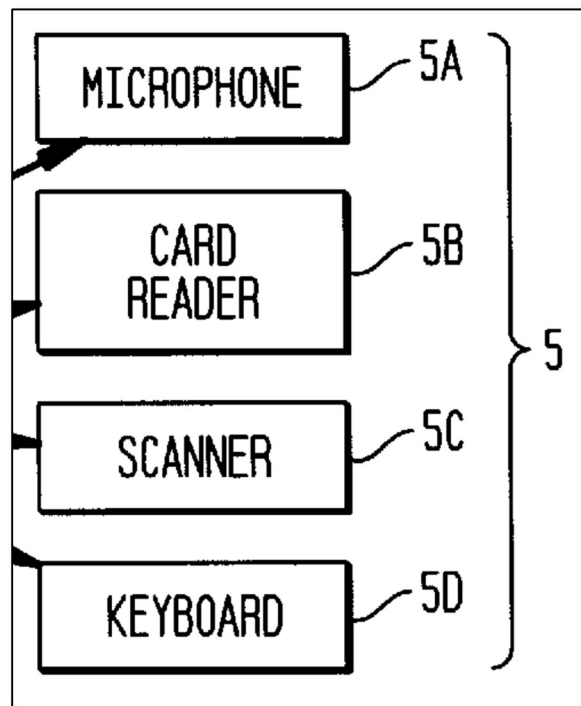
Ex-1004, Fig. 2; Michalson, ¶259.



Ex-1006, Fig. 1; Michalson, ¶259. Both also disclose collecting and storing data on removable storage devices, including location data. Ex-1004, 4:22-29, 5:27-32, 7:6-29 (SD cards); Ex-1006, 3:5-42 (“vehicle data system collects vehicle data and writes the collected data onto removable information cards 28-34.”), 4:64-5:19, 6:51-58 (gathering GPS data). Michalson, ¶260.

While *Ziv* discloses capturing a user’s biometric identification data for identification purposes, Ex-1005, ¶¶[0006], [0026], [0031], [0037], [0038], a

POSITA would have looked to *Gehlot* for more implementation details on such a biometric identity capture device. Michalson, ¶261. *Gehlot* teaches how “the user is prompted by the VDS to input some form of physical data, i.e. retinal scan, fingerprint, voice recognition, and to insert a driver and/or vehicle information card into a card reader/writer that is designed to work in conjunction with the VDP.” Ex-1006, 2:16-21. Michalson, ¶261. VDS 1 includes “a vehicle data processing unit (‘VDP’) 3 for communicating and collecting data from various vehicle systems 15 and physical input devices 5, e.g., a microphone 5A for voice recognition, a card reader/writer 5B, and a scanner 5C such as a hand or retinal scanner.” Ex-1006, 3:6-12; Michalson, ¶261.



Ex-1006, Fig. 4.

Implementing *Gehlot*'s biometric user identification components and/or methods in the combination of *Fish* and *Ziv* would have been advantageous and obvious. Michalson, ¶262. This would enhance flexibility and convenience with different options for accessing encrypted data. Michalson, ¶262. This would amount to simply substituting *Gehlot*'s known biometric authentication to achieve predictable results, enhanced security, in *Fish* and *Ziv*'s system. Michalson, ¶262. Indeed, *Gehlot*, like *Ziv*, teaches that its biometric methods are interchangeable with password-based authentication. Ex-1006, 6:6-8 ("physical data may include the entry of a password via a keyboard, a driver's voice, a driver's retinal scan, a driver's hand-print, or the like."); Michalson, ¶262.

B. Claim 5

- 1. [5] The device as in claim 3, wherein the user verification module further comprises an identity capture device for verifying the identity of the user of the device.**

Fish in view of *Ziv* and *Gehlot*, alone or with the knowledge of a POSITA, discloses and renders obvious the device as in claim 3, wherein the user verification module further comprises an identity capture device for verifying the identity of the user of the device, as claimed. Michalson, ¶263.

The claimed "identity capture device" may be a "biometric device, such as a retinal scanning device, finger print reader, facial recognition reader or another type of user identity verification input device which will collect information on the

user to be compared to information that has previously been stored in the device's memory." Ex-1001, 5:54-59; Michalson, ¶264. *Gehlot* discloses the same types of identity capture devices.

Gehlot securely stores vehicle data during operation, including location information. *E.g.*, Ex-1006, 3:5-42 ("vehicle data system collects vehicle data and writes the collected data onto removable information cards 28-34."), 4:64-5:1, 6:51-58 (gathering GPS data); Michalson, ¶265. *Gehlot*'s VDS includes a GPS system for tracking the vehicle and sharing location information. Ex-1006, 2:1-16; Michalson, ¶265. *Gehlot* uses biometric safeguards for access to VDS 1.

Michalson, ¶266. "In a preferred embodiment, the user is prompted by the VDS [vehicle data system] to input some form of physical data, i.e. **retinal scan, fingerprint, voice recognition**, and to insert a **driver and/or vehicle information card** into a card reader/writer that is designed to work in conjunction with the VDP." Ex-1006, 2:17-21; Michalson, ¶266. *Gehlot* matches this information to stored data and uses it to grant authorization. Ex-1006, 2:21-23; Michalson, ¶266.

As discussed above, a POSITA would have been motivated to use *Gehlot*'s biometric authentication methods for restricting access to encrypted data on *Fish*'s data archive 10. Michalson, ¶267. While *Ziv* uses biometric techniques to verify a user's identity, *Gehlot* discloses components, implementation examples, and prompts for such biometric identification devices. Michalson, ¶267. A POSITA

would have thus been motivated to implement *Fish* and *Ziv*'s biometric identification techniques with *Gehlot*'s more specific components and techniques of biometric identification. Michalson, ¶267.

C. Claim 6

1. [6] The device as in claim 5, wherein the identity capture device is a biometric device.

Fish in view of *Ziv* and *Gehlot*, alone or with the knowledge of a POSITA, discloses and renders obvious the device as in claim 5, wherein the identity capture device is a biometric device, as claimed. Michalson, ¶268. As discussed regarding claim 5, a POSITA would have been motivated to implement *Gehlot*'s biometric authentication components and techniques (e.g., **retinal scan, fingerprint, voice recognition** with accompanying input devices) in the system of *Fish* and *Ziv*. See *supra* claim 5; Ex-1006, 2:1-23, 3:5-42, 4:64-5:1, 6:51-58; Michalson, ¶¶265-68. In such a system, as discussed regarding claim 5, *Gehlot*'s more specific biometric components, techniques, and prompts would accomplish the biometric-based security techniques of *Fish* and *Ziv*. Michalson, ¶268.

D. Claim 7

- 1. [7] The device as in claim 5, wherein the identity capture device is a retinal scanning device.**

Fish in view of *Ziv* and *Gehlot*, alone or with the knowledge of a POSITA, discloses and renders obvious the device as in claim 5, wherein the identity capture device is a retinal scanning device, as claimed. Michalson, ¶269.

As discussed regarding claim 5, a POSITA would have been motivated to implement *Gehlot*'s biometric authentication, including the use of a “**retinal scanner**.” Ex-1006, 3:6-12; *see also id.*, 2:16-20 (“[T]he user is prompted by the VDS to input some form of physical data, i.e. **retinal scan**, fingerprint, voice recognition, and to insert a driver and/or vehicle information card into a card reader/writer that is designed to work in conjunction with the VDP.”), 6:6-11 (“Such physical data may include the entry of a password via a keyboard, a driver’s voice, a driver’s **retinal scan**, a driver’s hand-print, or the like. The physical data may be retrieved from the driver/owner by the use of a keyboard, a microphone, a **retinal scanner** or a hand-scanner.”), 6:28-33 (“[P]rocessing unit 3 can also request the driver to provide the input of a hand-print using a scanner 5C, which may be a hand-scanner, or a **retinal scan using a retinal scanner**, and compare these inputs in a manner similar to the voice comparison discussed above.”); Michalson, ¶269. A POSITA would have been motivated to use a retinal

scan for biometric verification procedures, as retinal scans are difficult to falsify and would efficiently use the confined space within vehicles, especially absent a full keyboard. Michalson, ¶269.

E. Claim 8

1. [8] The device as in claim 5, wherein the identity capture device is a finger print reader.

Fish in view of *Ziv* and *Gehlot*, alone or with the knowledge of a POSITA, discloses and renders obvious the device as in claim 5, wherein the identity capture device is a fingerprint reader, as claimed. Michalson, ¶270. As discussed regarding claim 5, a POSITA would have been motivated to implement *Gehlot*'s biometric authentication, including fingerprint methods. Ex-1006, 2:16-20 (“[T]he user is prompted by the VDS to input some form of physical data, i.e. retinal scan, **fingerprint**, voice recognition, and to insert a driver and/or vehicle information card into a card reader/writer that is designed to work in conjunction with the VDP.”), claims 28-29; Michalson, ¶270. Indeed, *Ziv* itself teaches using “a **fingerprint reader**” to verify a user’s identity. Ex-1005, ¶31; Michalson, ¶270.

A POSITA would have been motivated by this teaching to utilize *Gehlot*'s more specific and complete implementation (e.g., with user prompts) of a fingerprint reader, as taught in *Ziv*. Ex-1006, 2:16-20, 3:10-12, 6:28-33; Michalson, ¶270. For example, a POSITA would have understood that fingerprints

cannot easily be falsified and can be quick for a user to provide, especially in a vehicle without a full keyboard. Michalson, ¶271. These security and user-friendliness benefits would have motivated a POSITA to use fingerprint verification for identity capture in *Fish-Ziv. Id.*

F. Claim 18

1. [18] The device as in claim 16, wherein the user verification module further comprising an identity capture device for verifying the identity of the user of the device.

Fish in view of *Ziv* and *Gehlot*, alone or with the knowledge of a POSITA, discloses and renders obvious claim 18. *See supra* claim 5; Michalson, ¶272.

X. Ground 4: *Fish, Ziv, Gehlot, and Stevenson* (Claims 9-10)

Claims 9-10 are unpatentable under § 103 in view of *Fish, Ziv, Gehlot*, and *Stevenson*, alone or with the knowledge of a POSITA.

A. Motivation to Combine *Fish, Ziv, Gehlot, and Stevenson*

A POSITA practicing *Fish, Ziv*, and *Gehlot* would have looked to *Stevenson* for ways to further enhance data security and secure access to *Fish*'s data archive 10. Michalson, ¶274.

Like *Fish* and *Gehlot*, *Stevenson* generally relates to security for vehicle systems, and, like *Ziv*, *Stevenson* relates to portable device data encryption and retrieval. *E.g.*, Ex-1004, 1:6-33, 2:16-24; Ex-1006, 1:5-59, 2:1-46, 3:5-42; Ex-1007, Abstract, ¶¶[0001]-[0007], [0018]-[0020]; Michalson, ¶275. *Stevenson* is

in the same field of endeavor as *Fish*, as well as *Fish* as combined with *Ziv* and *Gehlot*. Michalson, ¶275. Like *Fish*, *Stevenson* describes a vehicle-based control system 10. Ex-1007, Abstract, ¶¶[0010], [0011], [0016], Fig. 1; Michalson, ¶275. Also, like *Fish*, *Stevenson* discloses user authentication or authorization. Ex-1007, Abstract, ¶¶[0005], [0006], [0008], [0010], [0012]-[0020], Fig. 1; Michalson, ¶275.

Combining *Fish-Ziv-Gehlot* with *Stevenson* would have been beneficial and obvious because both *Gehlot* and *Stevenson* disclose eye scanning (iris or retinal), fingerprints, palm (hand) prints, and voice patterns to enhance security in a vehicle, Ex-1006, 2:17-26, 3:5-12, 6:1-35; Ex-1007, Abstract, ¶¶[0007], [0018]-[0020], and *Stevenson* discloses **additional** types of such user verification (e.g., **facial recognition** and **DNA recognition**), Ex-1007, Abstract, ¶¶[0005], [0007], [0010], [0020]; Michalson, ¶276. These additional security techniques would further enhance security and provide greater user flexibility to one implementing *Gehlot*'s biometric techniques in *Fish-Ziv*'s system. Michalson, ¶¶276-277. *Stevenson*'s techniques could be used instead of, or in addition to, *Gehlot*'s, which would enhance flexibility, simplify the user experience, and offer convenience by enabling different options for accessing encrypted data. *Id.* Some users may be limited in their ability or preference for using *Stevenson*'s facial or DNA recognition as opposed to *Gehlot*'s techniques, or vice versa. *Id.*

B. Claim 9

1. [9] The device as in claim 5, wherein the identity capture device is a facial recognition reader.

Fish-Ziv, in view of *Gehlot* and *Stevenson*, discloses and renders obvious the device as in claim 5, wherein the identity capture device is a facial recognition reader, as claimed. Michalson, ¶278. As discussed regarding claim 5, a POSITA would have been motivated to implement *Gehlot*'s biometric authentication techniques in combination with *Fish-Ziv-Gehlot*. Michalson, ¶278.

Stevenson enhances security with facial recognition and DNA-based authentication for vehicle entry and exit systems. Ex-1007, Abstract; Michalson, ¶279. *Stevenson*'s authentication methods include **facial recognition**, iris recognition, palm prints, fingerprints, or “means for examining the DNA of a driver, such as from a sample of saliva.” Ex-1007, Abstract, ¶¶[0007], [0018]-[0020]; Michalson, ¶279. For facial recognition, *Stevenson* positions a camera to recognize a user's face and compares images to stored images for driver authentication. Ex-1007, Abstract, ¶[0007]; Michalson, ¶279. A POSITA would have found it obvious and advantageous to use such facial recognition or DNA techniques in *Fish-Ziv-Gehlot* to enhance security and provide more user-friendly options for authentication and authorization. Michalson, ¶¶279-280.

C. Claim 10

1. [10] The device as in claim 5, wherein the identity capture device is a DNA detection device.

Fish-Ziv, in view of *Gehlot* and *Stevenson*, discloses and renders the device as in claim 5, wherein the identity capture device is a DNA detection device, as claimed. Michalson, ¶281.

As discussed regarding claim 9, a POSITA would have used *Stevenson*'s biometric authentication methods in *Fish-Ziv-Gehlot*'s system. *See supra* claim 9; Michalson, ¶282. *Stevenson* also uses **DNA-based authentication** for drivers. Ex-1007, ¶¶Abstract (“**DNA analysis**”), [0007] & [0020] (“**DNA** of the driver”); Michalson, ¶282. A POSITA would have been motivated to implement *Stevenson*'s DNA-based user authentication methods in *Fish-Ziv-Gehlot* to provide further enhanced user authentication and identification, user flexibility, and rapidity of identification. Michalson, ¶282.

XI. Discretionary Denial Is Not Warranted

A. 35 U.S.C. § 325(d) Denial Is Improper

The factors in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 at 17-18 (P.T.A.B. Dec. 15, 2017) favor institution. *See also Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 8-11 (P.T.A.B. Feb. 13, 2020) (precedential).

Advanced Bionics, step 1, and *Becton, Dickinson* factors (a), (b), and (d), favor institution, because none of the references used in this Petition were considered during prosecution. Ex-1003 at 48-54, 88-96; *see Microsoft Corp. v. Parallel Networks Licensing LLC*, IPR2015-00486, Paper 10 at 15-20 (P.T.A.B. July 15, 2015) (granting institution when “there [was] no evidence that the Examiner considered the particular disclosures cited”). The *Becton Dickinson* “analysis ends at this point, and [the Board] need not proceed to part two of the *Advanced Bionics* framework.” *See Amazon.com, Inc. v. Nokia Techs. Oy*, IPR2024-00799, Paper 9 at 17-18 (P.T.A.B. Jan. 8, 2025).

B. *Fintiv* Denial Is Improper

The Office’s Memorandum of March 26, 2025, titled “Interim Process for PTAB Workload Management,” describes a procedure where Petitioner can respond to any discretionary denial arguments Patent Owner may raise in bifurcated briefing. Petitioner believes discretionary denial is unwarranted here and, at the appropriate time, plans to rebut any claims by Patent Owner to the contrary.

Petitioner identifies below several nonlimiting considerations that weigh against discretionary denial:

- The complaint in the parallel district court case was served January 28, 2025, less than three months before this Petition was filed. No discovery or other substantive work has occurred in the litigation. *See*

Apple Inc. v. Fintiv, Inc., IPR2020-00019, Paper 11, at 11 (P.T.A.B. Mar. 20, 2020) (expeditious filing weighs against denial); *SharkNinja v. iRobot Corp.*, IPR2021-00545, Paper 11, at 8 (P.T.A.B. Sept. 8, 2021) (petitioner’s diligence and remaining work in litigation weigh against denial).

- Petitioner promptly brought this challenge less than one month after infringement contentions (and notice of the asserted claims) were served, on April 4, 2025. *CoolIT Sys., Inc. v. Asetek Danmark A/S*, IPR2021-01195, Paper 10 at 11-14 (P.T.A.B. Dec. 28, 2021).
- No other forum has adjudicated these claims.
- This Petition challenges three claims (7, 8, and 10) not asserted in the parallel litigation.
- The merits of this Petition are strong. Indeed, as noted above, the claims were allowed based on the doubly erroneous premise that “removable” storage was present in all claims and was patentable.
- Petitioner stipulates that, if this Petition is instituted, it will not pursue in district court the grounds identified in this Petition or grounds that could reasonably have been raised in this IPR.

The *Fintiv* factors thus weigh strongly in favor of institution.

XII. Mandatory Notices Under 37 C.F.R. § 42.8

A. Real Parties-in-Interest

The real parties-in-interest are Volkswagen Group of America, Inc., Volkswagen AG, and Audi AG.

B. Related Matters

To the best of Petitioner's knowledge, the '192 patent is involved in only *Longhorn Automotive Group LLC v. Volkswagen AG*, 2:24-cv-00933 (E.D. Tex.).

C. Lead and Back-Up Counsel

Lead Counsel	Back-up Counsel
Elliot C. Cook (Reg. No. 61,769) elliot.cook@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel.: 571-203-2700 Fax: 202-408-4400	Alexander Boyer (Reg. No. 66,599) alexander.boyer@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel.: 571-203-2700 Fax: 202-408-4400 Daniel Jordan (Reg. No. 78,038) daniel.jordan@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel.: 571-203-2700 Fax: 202-408-4400 Luke MacDonald (Reg. No. 79,064) luke.macdonald@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800

	Reston, VA 20190-6023 Tel.: 571-203-2700 Fax: 202-408-4400
--	--

Petitioner consents to electronic service at the following email address:

Finnegan-Longhorn-192IPR@finnegan.com.

XIII. Standing

The '192 patent is available for IPR. Petitioner is not barred or estopped.

XIV. Conclusion

Petitioner requests institution and cancellation of challenged claims 1-22.

Respectfully submitted,

Dated: April 24, 2025

By: /Elliot C. Cook/
Elliot C. Cook (Reg. No. 61,769)
Lead Counsel

CLAIM APPENDIX

- [1.pre] 1. A location information device with secure data storage comprising:
- [1.a] a housing;
- [1.b] a locational information module for determining location information of the device, the determined location information being at least one route traveled by the device;
- [1.c] an encryption module for encrypting the determined location information;
- [1.d] a removable storage module for storing the encrypted location information, the removable storage module being removably disposed in the housing; and
- [1.e] a processing module for sending the encrypted location information to the removable storage module removably disposed in the housing and retrieving the encrypted location information from the removable storage module.
- [2] 2. The device as in claim 1, further comprising an input module disposed on the housing configured for receiving a code string input

by a user, wherein the user inputted code string is used for encrypting and decrypting the location information stored in the removable storage module.

[3] 3. The device as in claim 1, further comprising a user verification module for verifying the identity of user of the device, wherein the processing module selectively decrypts the location information stored in the removable storage module based on the identity of the user.

[4] 4. The device as in claim 3, wherein the user verification module executes a password protection algorithm for verifying the identity of the user of the device.

[5] 5. The device as in claim 3, wherein the user verification module further comprises an identity capture device for verifying the identity of the user of the device.

[6] 6. The device as in claim 5, wherein the identity capture device is a biometric device.

[7] 7. The device as in claim 5, wherein the identity capture device is a retinal scanning device.

- [8] 8. The device as in claim 5, wherein the identity capture device is a finger print reader.
- [9] 9. The device as in claim 5, wherein the identity capture device is a facial recognition reader.
- [10] 10. The device as in claim 5, wherein the identity capture device is a DNA detection device.
- [11] 11. The device as in claim 1, wherein the location information further includes at least one of a home address, destination addresses and velocity of the device at predetermined times.
- [12] 12. The device as in claim 1, further comprising a transmission module for transmitting the encrypted location information to an external computing device.
- [13.pre] A location information device with secure data storage comprising:
- [13.a] a housing;
- [13.b] a locational information module for determining location information of the device, the determined location information being at least one route traveled by the device;

- [13.c] an encryption module for encrypting the determined location information;
- [13.d] a storage module for storing the encrypted location information; and
- [13.e] a processing module for sending the encrypted location information to the storage module and retrieving the encrypted location information from the storage module.
- [14] 14. The device as in claim 13, further comprising a transmission module for transmitting the encrypted location information from the storage module to an external computing device.
- [15] 15. The device as in claim 14, further comprising an input module disposed on the housing configured for receiving a code string input by a user, wherein the user inputted code string is used for encrypting and decrypting the location information stored in the storage module.
- [16] 16. The device as in claim 14, further comprising a user verification module for verifying the identity of user of the device, wherein the processing module selectively decrypts the location information stored in the storage module based on the identity of the user.

- [17] 17. The device as in claim 16, wherein the user verification module executes a password protection algorithm for verifying the identity of the user of the device.
- [18] 18. The device as in claim 16, wherein the user verification module further comprising an identity capture device for verifying the identity of the user of the device.
- [19.pre] 19. A system for controlling and storing location information comprising:
- [19.a] a location information device with secure data storage comprising:
- [19.b] a housing;
- [19.c] a locational information module for determining location information of the location information device, the determined location information being at least one route traveled by the location information device;
- [19.d] an encryption module for encrypting the determined location information;

- [19.e] a removable storage module for storing the encrypted location information, the removable storage module being removably disposed in the housing; and
- [19.f] a processing module for sending the encrypted location information to the removable storage module removably disposed in the housing and retrieving the encrypted location information from the removable storage module; and
- [19.g] a computing device comprising:
- [19.h] a reader configured for reading the removable storage module of the location information device when the removable storage module is removably disposed in the reader; and
- [19.i] a processor configured to execute a decryption program for decrypting the encrypted location information on the removable storage module removably disposed in the reader.
- [20] 20. The system as in claim 19, wherein the location information further includes at least one of a home address, destination addresses and velocity of the device at predetermined times.

- [21] 21. The system as in claim 19, wherein the computing device further comprises a memory for storing a plurality of geographical maps and the processor is configured to overlay the location information on at least one of the plurality of geographical maps.
- [22.pre] 22. A system for controlling and storing location information comprising:
- [22.a] a location information device with secure data storage comprising:
- [22.b] a housing;
- [22.c] locational information module for determining location information of the location information device, the determined location information being at least one route traveled by the location information device;
- [22.d] an encryption module for encrypting the determined location information;
- [22.e] a storage module for storing the encrypted location information;
- [22.f] a processing module for sending the encrypted location information to the storage module and retrieving the encrypted location information from the storage module;
- and

[22.g] a transmission module for transmitting the encrypted location information from the storage module to an external computing device; and

[22.h] the external computing device comprising:

[22.i] a connectivity device configured for receiving the encrypted location information from the location information device; and

[22.j] a processor configured to execute a decryption program for decrypting the encrypted location information received from the location information device.

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing **Petition for *Inter Partes* Review** contains 13,628 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.

Dated: April 24, 2025

/Elliot C. Cook/
Elliot C. Cook (Reg. No. 61,769)
Lead Counsel

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 8,085,192, the associated Power of Attorney, and Exhibits 1001 through 1026 were served on April 24, 2025, by FedEx Priority Overnight® on the correspondence address of record indicated in the Patent Office's Patent Center system for U.S. Patent No. 8,085,192.

COJK PLLC
1201 Third Avenue, Suite 3600
Seattle, WA 98101-3029

A courtesy copy is also being sent via FedEx Priority Overnight® to
litigation counsel at:

Alfred R. Fabricant, Esq.
FABRICANT LLP
411 Theodore Fremd Ave., Suite 206 South
Rye, New York 10580

Dated: April 24, 2025

/Mark A. Rosenberger/

Mark A. Rosenberger
Case Manager
Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP