

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

DECLARATION OF WILLIAM R. MICHALSON, PH.D.

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. SUMMARY OF OPINIONS	2
III. QUALIFICATIONS AND BACKGROUND	2
IV. MATERIALS CONSIDERED	7
V. LEGAL STANDARDS	9
A. Level of Ordinary Skill in the Art	11
B. Anticipation	11
C. Obviousness	11
D. Means-Plus-Function Terms	16
VI. OVERVIEW OF THE '192 PATENT	17
VII. TECHNOLOGICAL BACKGROUND	22
A. The Global Positioning System (GPS)	22
B. Navigation in Vehicles	27
C. Data Encryption	29
VIII. LEVEL OF ORDINARY SKILL	31
IX. CLAIM CONSTRUCTION	32
A. Means-Plus-Function Terms	34
1. “a locational information module for determining” (Claims 1, 13, 19, 22)	34
2. “an encryption module for encrypting” (Claims 1, 13, 19, 22)	36

3.	“a storage module for storing” (Claims 13, 22).....	37
4.	“a removable storage module for storing” (Claims 1, 19).....	38
5.	“a processing module for sending” (Claims 1, 13, 19, 22) and “the processing module selectively decrypts” (Claims 3, 16).....	40
6.	“an input module disposed on the housing configured for receiving” (Claims 2, 15).....	42
7.	“a user verification module for verifying the identity of [the] user” (Claims 3-5, 16-18).....	45
8.	“a transmission module for transmitting” (Claims 12, 14, 22)	47
X.	THE PRIOR ART	48
A.	Overview of <i>Fish</i> (Ex-1004, U.S. 6,490,513).....	49
B.	Overview of <i>Ziv</i> (Ex-1005, U.S. 2004/0103288 A1).....	51
C.	Overview of <i>Gehlot</i> (Ex-1006, U.S. 6,310,542)	54
D.	Overview of <i>Stevenson</i> (Ex-1007, European Patent Pub. EP0962894A2)	56
XI.	OVERVIEW OF THE GROUNDS.....	58
XII.	GROUND 1: <i>FISH</i> (CLAIMS 1, 11-14, 19-22).....	58
A.	Claim 1	58
1.	[1pre] A location information device with secure data storage comprising:	58
2.	[1a] a housing;.....	60
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;	62

4.	[1c] an encryption module for encrypting the determined location information;.....	69
5.	[1d] a removable storage module for storing the encrypted location information, the removable storage module being removably disposed in the housing; and.....	71
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.	73
B.	Claim 11	76
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.	76
C.	Claim 12	78
1.	[12] The device as in claim 1, further comprising a transmission module for transmitting the encrypted location information to an external computing device.	78
D.	Claim 13	81
1.	[13pre] A location information device with secure data storage comprising:	81
2.	[13a] a housing;.....	82
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;	82
4.	[13c] an encryption module for encrypting the determined location information;.....	82

5.	[13d] a storage module for storing the encrypted location information; and.....	82
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.....	82
E.	Claim 14	82
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.	82
F.	Claim 19	83
1.	[19pre] A system for controlling and storing location information comprising:.....	83
2.	[19a] a location information device with secure data storage comprising:	83
3.	[19b] a housing;	83
4.	[19c] a locational information module for determining location information of the location information device, the determined [19d] location information being at least one route traveled by the location information device;	83
5.	[19d] an encryption module for encrypting the determined location information;.....	84
6.	[19e] a removable storage module for storing the encrypted location information, the removable storage module being removably disposed in the housing; and.....	84
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	84

8.	[19g] a computing device comprising:	84
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.....	85
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.....	86
G.	Claim 20	87
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.	87
H.	Claim 21	87
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.....	87
I.	Claim 22	89
1.	[22pre] A system for controlling and storing location information comprising:.....	89
2.	[22a] a location information device with secure data storage comprising:	89
3.	[22b] a housing;	89
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;	89

5.	[22d] an encryption module for encrypting the determined location information;.....	90
6.	[22e] a storage module for storing the encrypted location information;.....	90
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.....	90
8.	[22g] a transmission module for transmitting the encrypted location information from the storage module to an external computing device; and	90
9.	[22h] the external computing device comprising: a connectivity device configured for receiving the encrypted location information form [sic] the location information device; and	90
10.	[22i] a processor configured to execute a decryption program for decrypting the encrypted location information received from the location information device.	93
XIII.	GROUND 2: <i>FISH</i> IN VIEW OF <i>ZIV</i> (CLAIMS 2-4, 15-17).....	94
A.	Motivation to Combine <i>Fish</i> and <i>Ziv</i>	94
B.	Claim 2	99
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.....	99
C.	Claim 3	106
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.....	106
D.	Claim 4	110
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.	110
E.	Claim 15	115
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.	115
F.	Claim 16	115
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.	115
G.	Claim 17	116
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.	116
XIV.	GROUND 3: <i>FISH</i> IN VIEW OF <i>ZIV</i> AND <i>GEHLOT</i> (CLAIMS 5-8, 18)	116
A.	Motivation to Combine <i>Fish</i> , <i>Ziv</i> , and <i>Gehlot</i>	116
B.	Claim 5	122

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.	122
C.	Claim 6	124
1.	[6] The device as in claim 5, wherein the identity capture device is a biometric device.....	124
D.	Claim 7	124
1.	[7] The device as in claim 5, wherein the identity capture device is a retinal scanning device.....	124
E.	Claim 8	126
1.	[8] The device as in claim 5, wherein the identity capture device is a finger print reader.....	126
F.	Claim 18	128
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.	128
XV.	GROUND 4: <i>FISH, ZIV, GEHLOT, AND STEVENSON</i> (CLAIMS 9-10)	128
A.	Motivation to Combine <i>Fish, Ziv, Gehlot, and Stevenson</i>	128
B.	Claim 9	130
1.	[9] The device as in claim 5, wherein the identity capture device is a facial recognition reader.	130
C.	Claim 10	131
1.	[10] The device as in claim 5, wherein the identity capture device is a DNA detection device.	131
XVI.	CONCLUSION.....	132

I. INTRODUCTION

[001] I have been retained by Volkswagen Group of America, Inc. as an independent expert for the above-identified *inter partes* review proceeding involving U.S. Patent No. 8,085,192 (“the ’192 patent”).

[002] I am over 21 years of age and, if I am called upon to do so, I would be competent to testify as to the matters set forth herein.

[003] Although I am being compensated for my time in connection with this proceeding at my standard hourly consulting rate and reimbursed for reasonable out-of-pocket expenses, no part of my compensation depends on the outcome of this proceeding, and I have no other interest in this proceeding.

[004] I have been asked to provide my opinions concerning whether the claims of the ’192 patent would have been obvious to a person of ordinary skill in the art at the time of the earliest claimed priority date of the ’192 patent. In performing my analysis, I have been asked to assume that the priority date is September 6, 2005. My opinions are set forth below.

[005] Throughout this declaration, I refer to specific pages, figures, and/or line numbers of various exhibits. These citations are illustrative and are not intended to suggest that they are the only support for the propositions for which they are cited.

II. SUMMARY OF OPINIONS

[006] This declaration addresses claims 1-22 of the '192 patent. Below, I set forth the opinions I have formed, the conclusions I have reached, and the bases for my opinions and conclusions. I believe the statements contained in this declaration to be true and correct to the best of my knowledge.

[007] Based on my experience and knowledge of the art at the time of the applicable priority date (I was told to assume a priority date of September 6, 2005), it is my opinion that claims 1-22 of the '192 patent would have been obvious based on the asserted grounds discussed below.

III. QUALIFICATIONS AND BACKGROUND

[008] I believe that I am well qualified to serve as a technical expert in this matter based upon my qualifications, discussed in detail below.

[009] I am competent to write this Declaration.

[010] This is a summary of my background and qualifications. I set forth my background in more detail in my Curriculum Vitae, which is attached as Ex-1026 herewith.

[011] I am currently a tenured Professor in Robotics Engineering in the Robotics Engineering Department of Worcester Polytechnic Institute (WPI). Additionally, I have appointments as a Professor of Computer Science, Electrical and Computer Engineering, and Mechanical Engineering at WPI. As part of my

appointments, I perform research and teach in the areas of navigation, communications, and computer system design. I supervised the WPI Center for Advanced Integrated Radio Navigation (CAIRN), where I was developing a Public Safety Integration Center focused on the integration of communications, navigation, and information technologies for public safety applications. Currently, I direct the Robot Communication and Navigation Laboratory where my research focuses on the development, testing, and evaluation of communication and navigation systems for both civilian and military applications with a special emphasis on techniques focused on indoor, underground, or otherwise GPS-deprived situations. My interests in communication, navigation, and computing have led me to play an active role in the development of the Robotics Program at WPI, where I teach robotics courses at the graduate and undergraduate levels.

[012] Prior to joining the faculty of WPI, I worked at the Raytheon Company from 1981-1991, with a leave of absence between 1985-1988 to complete my Doctoral Degree (Ph.D.) in Electrical Engineering from the Worcester Polytechnic Institute. Prior to my leave of absence, I worked as an Engineer in the Cursive Displays Department and VLSI Design Department of the Computer and Displays Laboratory within Raytheon's Equipment Division. After receiving my Ph.D., I returned to the Equipment Division of the Raytheon Company where I was promoted to the title of Engineer, Design and Development.

I was subsequently selected to sit on the engineering staff of the newly formed System Engineering Department of the Division's Computer and Displays Laboratory. In this capacity, I acted primarily as a consultant to other departments within the laboratory, and my responsibilities ranged from leading the hardware and software development of supercomputer-class computer systems to performing applied research into the exploitation of new technology.

[013] I earned a B.S. from the Syracuse University in 1981, and an M.S. and a Ph.D. in Electrical Engineering from WPI in 1985 and 1989, respectively.

[014] I have more than 40 years of experience in the field of computer technology, specifically in the specialized field of signal and data processing. I have consulted and served, including being qualified by courts, as an expert for numerous patent cases, including in patent cases involving motion sensing, positioning, map navigation technologies, and wireless communications, a listing of which is set forth in my current curriculum vitae, which is attached as Ex-1026. I hold a commercial General Radio Operator's license (with Ship RADAR Endorsement), an Extra Class Amateur Radio operator's license, and have held a Commercial Radiotelegraph Operators license. I was first licensed as a Radio Amateur in 1974 and have been involved in the design, implementation, and repair of radio systems, including radio-controlled systems, since that time.

[015] I have been involved with numerous projects involving remote objects which require wireless tracking, control, and telemetry. These objects include land vehicles, sea vehicles, and air vehicles. Starting with my work at the Raytheon Company, I was involved with the tracking of aircraft in both military and civilian air traffic control systems. I have worked on the guidance and control systems for multiple missile systems, as well as the guidance and tracking systems for fire control systems and on spaceborne systems for tracking ballistic missiles. In my work at WPI, I have been involved with numerous projects related to tracking land, sea, and air vehicles using the GPS and/or inertial guidance systems. Some of this work has involved the use and control of rotorcraft for applications, such as firefighting and landmine detection and destruction. All of these projects involve interacting with these systems remotely via wireless communications.

[016] GPS and GPS-related technologies have dominated the bulk of my research since 1992. I have been involved in numerous academic and consulting projects involving navigation technologies and their association with geographic information system technologies. Examples of academic projects include (1) a container tracking system in 2003, which explored the application of tracking and communications technologies to track shipping containers, (2) an automotive-based system in 2000, which combined GPS and map data in an automotive environment, (3) a remote hazard detection system in 1996 that combined GPS and

radio communications to remotely identify hazards to the engineer operating a freight train, and (4) a differential GPS system in 1995 that combined GPS and radio technologies to allow determining the precise path of vehicles operating off-road during forest operations. As a consultant, I have worked with the combination of GPS and radio communications in the context of space shuttle docking operations, transfer of traffic information to GPS devices in a vehicle, combinations of GPS and cellular communications for the tracking of individuals, and map-based handheld tracking devices.

[017] I am a named inventor on nine patents, including patents on map navigation devices, geolocation systems, and high resolution and precision location systems. I have authored, or co-authored, over 100 journal papers and conference publications, including papers and publications regarding positioning and navigation systems and methods. I am also the co-author of a chapter entitled “An Approach for Implementing a Reconfigurable Optical Interconnection Network for Massively Parallel Computers” in Optical Interconnection – Foundations and Approaches by C. Tocci and H. J. Caulfield Eds., Artech House, 1994. I am currently under contract to write a book tentatively entitled “Radionavigation and the Global Positioning System,” which covers the physical principles upon which radionavigation system are based as well as the hardware and software required to perform navigation. At WPI, I have taught courses in Sensors, Circuits, and

Systems, Digital Circuit Design, Embedded Computing, Computer Architecture, Computer, and Navigation. In addition, I have advised projects involving computers, navigation, and communications for a large variety of applications in the air, on land, and on the sea.

[018] I have received several awards and recognition for my work, including becoming an Elected Senior Member of the IEEE. In addition, I was awarded the Joseph Samuel Satin Distinguished Fellowship for the 1994-1995 academic year, and the Aldo Miccioli Fellowship from the Raytheon Company's Equipment Division. I am also a member of the Institute of Navigation, the Royal Institute of Navigation, the American Society of Engineering Educators, The Society of Automotive Engineers, the National Marine Electronics Association, and the National Academy of Inventors.

[019] My curriculum vitae, attached as Ex-1026, includes a list of publications on which I am a named author. It contains further details regarding my experience, education, publications, and other qualifications pertinent to an expert opinion in connection with this proceeding.

IV. MATERIALS CONSIDERED

[020] In forming my opinions, I have read and considered the '192 patent and its prosecution history, the exhibits listed in the Exhibit List filed with the

petition for inter partes review of the '192 patent, as well as any other materials referenced herein. I have reviewed at least the following documents:

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. 2004/103288 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> ”)
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.

[032] I reserve the right to supplement and amend any of my opinions in this declaration based on documents, testimony, and other information that becomes available to me after the date of this declaration.

V. LEGAL STANDARDS

[033] I am not a lawyer. My understanding of the legal standards that apply in reaching the conclusions of this declaration are based on discussions with counsel for Petitioner, my experience applying similar standards in other patent-related matters, and my reading of the documents submitted in this proceeding. In preparing this declaration, I have tried faithfully to apply these legal standards to the challenged claims.

[034] I have been informed that there are two ways in which prior art may render a patent claim unpatentable. First, I have been informed that the prior art can “anticipate” a claim. Second, I have been informed that the prior art can render a claim “obvious” to a person of ordinary skill in the art. I understand that a claim is patentable if it was not, *inter alia*, anticipated and would not have been obvious by the prior art at the effective filing date of the patent.

[035] I have been informed that a dependent claim is a patent claim that refers to a previous patent claim. I have been informed that a dependent claim includes all the limitations of the claim to which it refers.

[036] I have been asked to provide my opinions as to whether the cited prior art teaches or renders obvious claims 1-22 of the '192 patent from the perspective of a person of ordinary skill in the art at the '192 patent's earliest claimed priority date of September 6, 2005, as described in more detail below.

[037] I have been informed that in *inter partes* review proceedings, such as this one, the party challenging the patent bears the burden of proving unpatentability by a preponderance of the evidence. I understand that a preponderance of the evidence means “more likely than not.”

[038] For purposes of this declaration, I have been asked to provide my opinions on issues regarding unpatentability. I have been informed of the following legal standards, which I have applied in forming my opinions.

A. Level of Ordinary Skill in the Art

[039] I have been informed a person of ordinary skill in the art is determined by considering several factors, including the (i) type of problems encountered in the art; (ii) prior art solutions to those problems; (iii) rapidity with which innovations are made; (iv) sophistication of the technology; and (v) educational level of active workers in the field.

[040] I have been instructed to assume a person of ordinary skill in the art is not a specific real individual, but rather a hypothetical individual having the qualities reflected by the factors discussed above.

B. Anticipation

[041] I have been informed that under 35 U.S.C. § 102, a patent claim is unpatentable for anticipation if the claimed subject matter was patented or described in a printed publication before the effective filing date of the claimed invention. I have been informed that a patent claim is anticipated under § 102 if a single prior art reference discloses all limitations of the claimed invention.

C. Obviousness

[042] I have been informed that for obviousness under 35 U.S.C. § 103, a patent claim is unpatentable if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have

been obvious to a person having ordinary skill in the art to which said subject matter pertains at the time the invention was made.

[043] I have been informed that a proper obviousness analysis includes the following:

- a. Determining the scope and content of the prior art;
- b. Ascertaining the differences between the prior art and the claims at issue;
- c. Resolving the level of ordinary skill in the pertinent art; and
- d. Considering evidence of secondary indicia of non-obviousness (if available).

[044] I have been informed that the relevant time for considering whether a claim would have been obvious to a person of ordinary skill in the art is the time of invention. For my obviousness analysis, counsel for Petitioner instructed me to assume that the date of invention for the challenged claims is September 6, 2005. My opinions would not change if I assumed a later date of invention.

[045] I have been informed that a reference may be modified or combined with other references or with a person of ordinary skill in the art's own knowledge if the person would have found the modification or combination obvious. I have also been informed that a person of ordinary skill in the art is presumed to know all

the relevant prior art, and the obviousness analysis may consider the inferences and creative steps that a person of ordinary skill in the art would employ.

[046] I have been informed that whether a prior art reference renders a patent claim obvious is determined from the perspective of a person of ordinary skill in the art. I have also been informed that, while there is no requirement that the prior art contain an express suggestion to combine known elements to achieve the claimed invention, and while a suggestion to combine known elements to achieve the claimed invention may come from the prior art as a whole or individually and may consider the inferences and creative steps a person of ordinary skill in the art would employ, as filtered through the knowledge of one skilled in the art, obviousness grounds cannot be sustained by mere conclusory statements and must include some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.

[047] In determining whether a prior art reference could have been combined with another prior art reference or other information known to a person having ordinary skill in the art, I have been informed that the following principles may be considered:

- a. A combination of familiar elements according to known methods is likely to be obvious if it yields predictable results;

- b. The substitution of one known element for another is likely to be obvious if it yields predictable results;
- c. The use of a known technique to improve similar items or methods in the same way is likely to be obvious if it yields predictable results;
- d. The application of a known technique to a prior art reference that is ready for improvement to yield predictable results;
- e. Any need or problem known in the field and addressed by the reference can provide a reason for combining the elements in the manner claimed;
- f. A person of ordinary skill often will be able to fit the teachings of multiple references together like a puzzle; and
- g. The proper analysis of obviousness requires a determination of whether a person of ordinary skill in the art would have a “reasonable expectation of success”—but not “absolute predictability” of success—in achieving the claimed invention by combining prior art references.

[048] I have been informed that, when a work is available in one field, design alternatives and other market forces can prompt variations of it, either in the same field or in another. I have been informed that, if a person of ordinary skill in

the art could have implemented a predictable variation, and would have seen the benefit of doing so, that variation is likely to have been obvious. I have been informed that, in many fields, there may be little discussion of obvious combinations, and in these fields, market demand—not scientific literature—may drive design trends. I have been informed that, when there was a design need or market pressure and there are a finite number of predictable solutions, a person of ordinary skill in the art would have had a good reason to pursue those known options.

[049] I have been informed that the law permits the application of “common sense” in examining whether a claimed invention would have been obvious to a person skilled in the art. For example, I have been informed that combining familiar elements according to known methods and in a predictable way may suggest obviousness when such a combination would yield nothing more than predictable results. I understand, however, that a claim is not obvious merely because every claim element is disclosed in the prior art and that a party asserting obviousness must still provide a specific motivation to combine or modify the references as recited in the claims and explain why one skilled in the art would have reasonably expected to succeed in doing so.

[050] I have been informed that there is no rigid rule that a reference or combination of references must contain a “teaching, suggestion, or motivation” to

combine references. But I also understand that the “teaching, suggestion, or motivation” test can be a useful guide in establishing a rationale for combining elements of the prior art. I have been informed that this test poses the question as to whether there is an express or implied teaching, suggestion, or motivation to combine prior art elements in a way that realizes the claimed invention, and that it seeks to counter impermissible hindsight analysis.

[051] I am not aware of any evidence of secondary considerations (such as commercial success, long-felt needs, failure of others, unexpected results, copying, or industry praise) that would support a determination of non-obviousness of the claimed subject matter in the '192 patent.

[052] I have been informed that, in an obviousness analysis, prior art must be analogous prior art to the patent being considered. I have been informed that a prior art reference is considered to be analogous, or in the same field of art, if the reference is either (1) in the same field of endeavor as the challenged patent, regardless of the problems the challenged patent and the prior art address, or (2) reasonably pertinent to the particular problem being solved by the challenged patent.

D. Means-Plus-Function Terms

[053] I understand that certain claims include what are referred to as “means-plus-function” terms, which recite a structural component solely in terms

of the function it performs. In other words, a patent claim may recite a structural term that is essentially a placeholder word (for example, the word “module”), presented in terms of the function it performs (e.g., “[function] module”). I have been told that construing a means-plus-function term involves two steps: (1) identifying the claimed function, and (2) determining what structure, if any, disclosed in the specification corresponds to that claimed function. The claimed function and the corresponding structure are identified below in my detailed opinions. For every identified structure, the claim terms encompass equivalents of the identified structure as well. 35 U.S.C. § 112 ¶ 6.

VI. OVERVIEW OF THE '192 PATENT

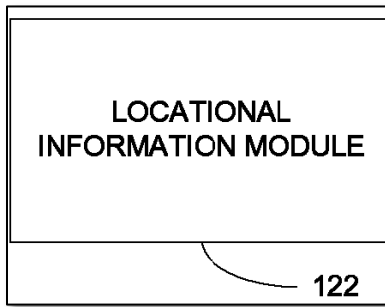
[054] The '192 patent is directed to a “system and method for controlling and storing sensitive information on a global positioning system (GPS) device.” Ex-1001, Abstract. According to the specification, the '192 patent addressed a need for “techniques for controlling and storing sensitive information on a GPS device and only allowing access to designated parties.” *Id.*, 1:53-55. However, as discussed below, techniques for controlling and storing sensitive information on an internal memory and in removable memory were already well-known at the time of the '192 patent.

[055] The application that issued as the '192 patent was filed on April 5, 2010. *Id.*, Cover. It claims priority to U.S. Application Number 11/220,233, filed

September 6, 2005, now U.S. Patent Number 7,692,580. *Id.* The '192 patent issued on December 27, 2011, with 22 claims, including independent claims 1, 13, 19, and 22. *Id.*, Cover, 8:1-10:40. The patent lists one inventor, Leigh M. Rothschild.

[056] Many aspects of the claimed embodiments are disclosed in the specification as known in the art prior to the filing of the '192 patent, including in the field of automobiles.

[057] The '192 patent specification correctly concedes that GPS devices were ubiquitous at the time of the patent (“GPS (Global Positioning System) devices are everywhere”) and were particularly useful in vehicles. *Id.*, 1:21-25. The '192 patent specification discloses multiple “conventional locational information processing technolog[ies] such as Global Positioning Satellite (GPS) Technology, Loran Technology, or any other available locational technology, to indicate the exact location, e.g., latitude, longitude and altitude” of a device. *Id.*, 3:56-62. Consistent with this prior-art description of GPS, the '192 patent describes its locational information module 122 as merely a black box—a conventional GPS module:



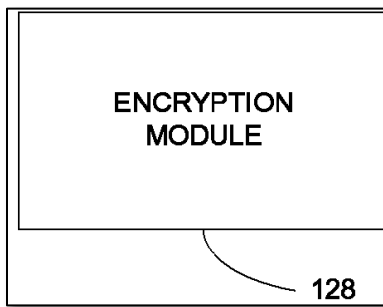
Id., Fig. 2.

[058] The '192 patent specification discloses as known that GPS devices provide a user with location information such as latitude and longitude, as well as “accurate time, heading, velocity, etc.” which can be used to continuously calculate a user’s location or route. *Id.*, 1:22-23.

[059] The '192 patent concedes that “most [GPS] devices will allow a user to store information such as address points” and information “regarding the time and location of the vehicle during usage” in the memory of the GPS device, including in internal memory or on removeable memory. *Id.*, 1:26-29, 1:42-44. The '192 patent discloses that this stored information can be used “to see where a [] car was driven during a particular day” and “where the car was taken.” *Id.*, 1:45-49. The '192 patent provides known exemplary memory storage modules. *Id.*, 1:66-2:07, 4:47-54.

[060] The '192 patent also discloses multiple prior art forms of encryption, including “conventional code encryption algorithms currently in use or that will be

in use in the future such as symmetric-key algorithms, e.g., DES, Triple-DES, Blowfish, RC2, RC4, RC5, etc., and asymmetric-key algorithms, e.g., Diffie-Hellman, RSA, ElGamal, etc. to encrypt the data information that comes into the input module 126 and/or that is stored in the storage module 110.” *Id.*, 4:60-66, 5:11-16. Given the admitted prior art status of such encryption techniques, the ’192 patent describes its encryption module 128 as a generic black box:

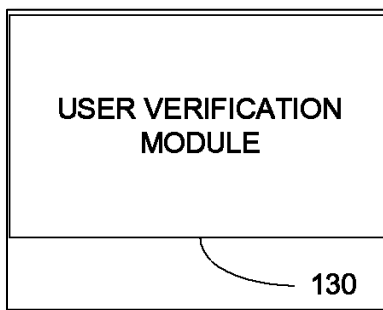


Id., Fig. 2.

[061] The ’192 patent discloses “small code (decryption) program (CEP)” that “may be distributed on optical media, or other computer media, or may also be downloaded from a website on a server 214 that the manufacturer provides the user.” *Id.*, 7:01-06. The ’192 patent explicitly discloses that “[s]uch encryption/decryption programs are standard in the industry and include such programs as PGP (Pretty Good Privacy).” *Id.*, 7:06-08.

[062] The ’192 patent also discloses prior art user identity capture devices including “biometric device[s], such as a retinal scanning device, finger print

reader, facial recognition reader.” *Id.*, 5:54-61. The ’192 patent explicitly states, “[i]t is to be noted that identity detection devices such as biometric devices are common and are currently widely in use.” *Id.*, 5:62-64. These admitted prior art techniques are performed via the nondescript user verification module 130 of the ’192 patent:



Id., Fig. 2.

[063] As a POSITA would readily have understood, the ’192 patent teaches merely “using” these prior art technologies for their known and conventional purposes. The patent does not improve the technologies themselves. For example, claim 1 generically recites a “location information device” and “locational information module” (e.g., conventional GPS device), conventional “housing,” conventional “encryption module,” conventional “removable storage,” and conventional “processing module.” Nowhere does the claim, or any of its dependent claims, recite any technical improvements to these known, prior art components. The components are simply used for their known, prior art functions,

in the claims. Similarly, independent claims 13, 19, and 22 recite these and other conventional components (e.g., “computing device,” “reader,” and “processor” in claim 19, and “transmission module,” “external computing device,” “connectivity device,” and “processor” in claim 22). Nowhere do these claims, or their dependents, recite any technical improvements in the areas of GPS, encryption, computing, data storage, navigation, or any other field.

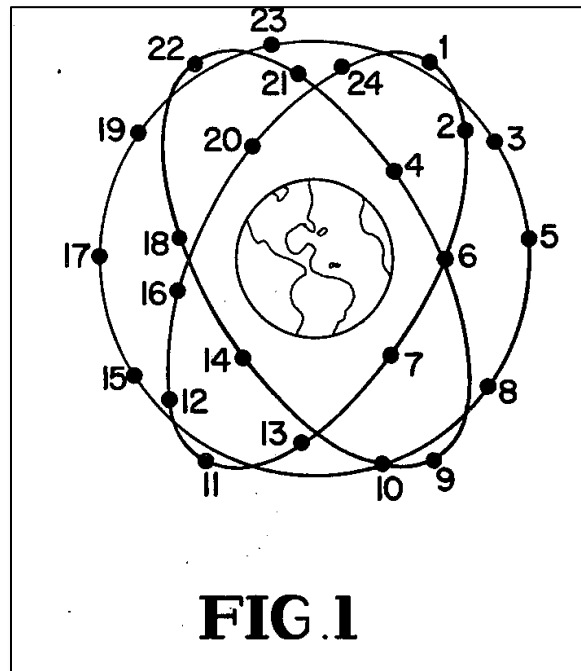
VII. TECHNOLOGICAL BACKGROUND

[064] At the time the '192 patent was filed, both vehicle navigation technologies and encryption technologies were well understood, known, and conventional. As detailed below, the combinations of navigation and encryption technologies proposed by the '192 patent were well-known in the prior art and a matter of routine implementation. Before providing an invalidity analysis, I provide a brief background of both navigation and data encryption technologies as of the purported priority date of the '192 patent.

A. The Global Positioning System (GPS)

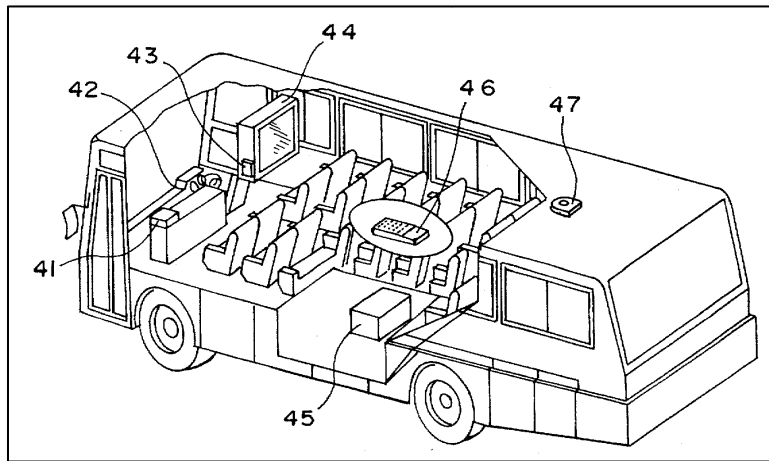
[065] The Global Positioning System, or GPS, is a United States government-maintained satellite-based positioning system that was developed and deployed for both civilian and military uses. GPS is part of a satellite navigation system developed by the United States Department of Defense under its NAVSTAR satellite program in the early 1970s. By December 1993, 24 GPS

satellites had become operational. The basic schematic view of an early GPS system is shown below, with 24 spacecraft in a medium-Earth orbit (MEO).

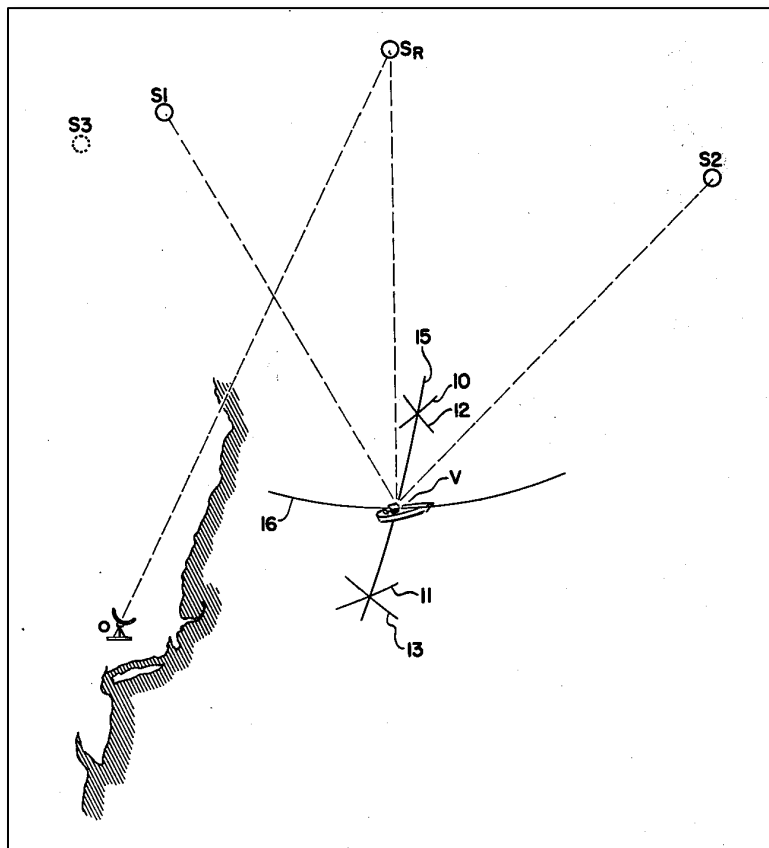


Ex-1008, *Raab*, Fig. 1.

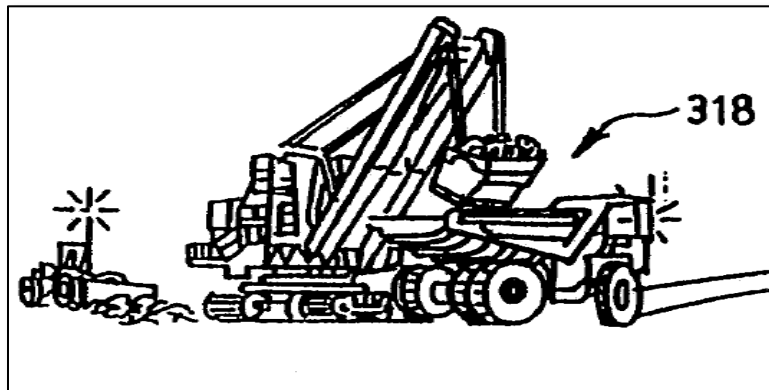
[066] GPS was quickly adopted in a variety of fields, including, especially, transportation. Examples include buses:

Ex-1009, *Kamiya*, Fig. 16.

[067] Further examples include ships:

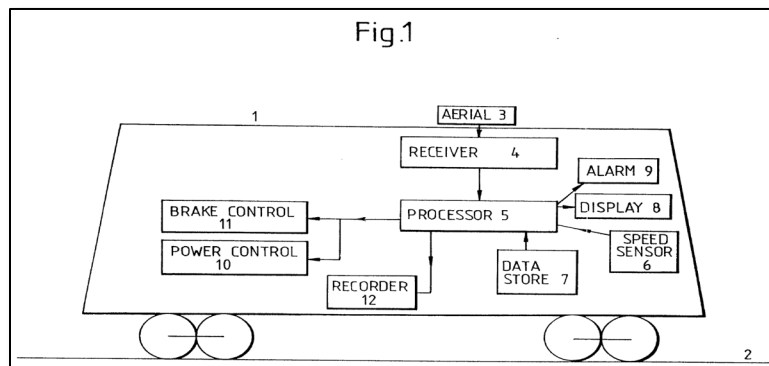
Ex-1010, *Anderson*, Fig. 1.

[068] Additional examples include heavy machinery:



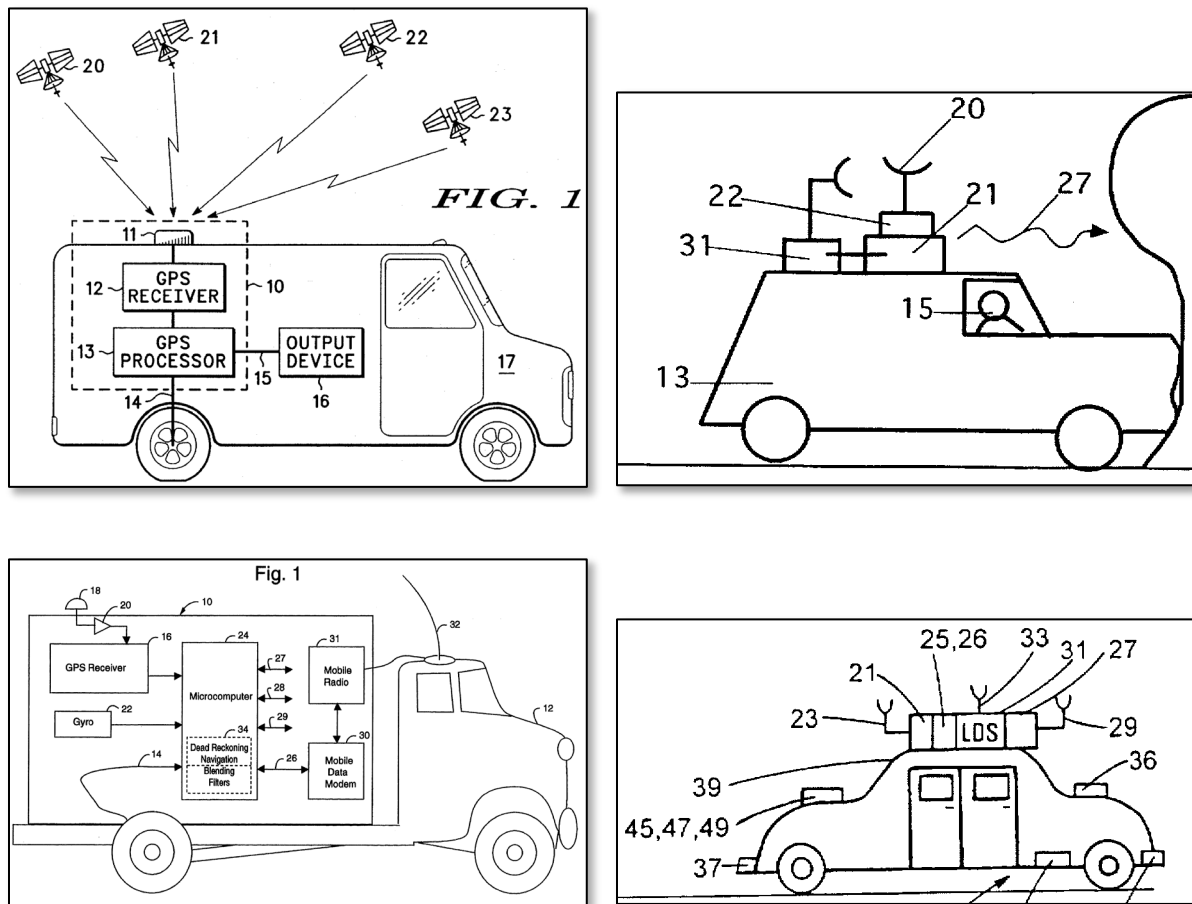
Ex-1011, *Kyrtsos*, Fig. 3.

[069] Further examples include locomotives:



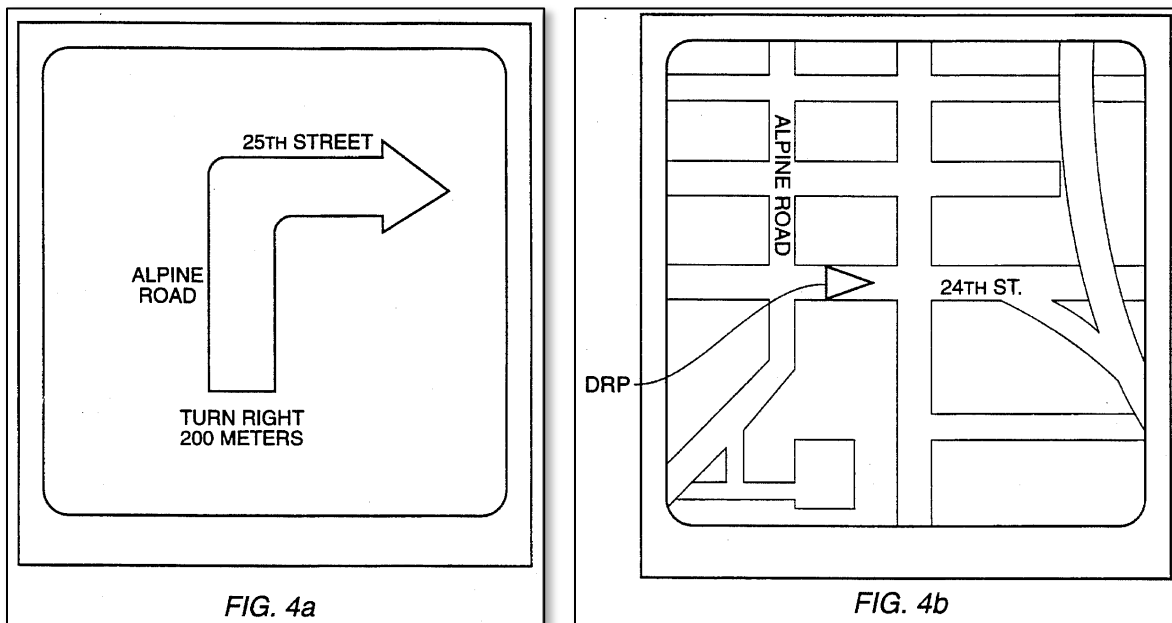
Ex-1012, *Whyntie*, Fig. 1.

[070] Of course, many other examples of GPS in vehicles address use in automobiles:



Ex-1013, *Geier*, Fig. 1; Ex-1014, *Sorden*, Fig. 1; Ex-1015, *Geier II*, Fig. 1;
Ex-1016, *Janky*, Fig. 1.

[071] In addition to integrating GPS into vehicles, prior to the '192 patent GPS was utilized to provide user-friendly displays of navigation guidance. Such systems tracked the position of the vehicle with reference to its route to a destination. Examples of such display modules described in 1992 include the following:



Ex-1017, *Snider*, Figs. 4a, 4b.

[072] As disclosed in the '192 patent, by the time of the patent, GPS devices were “everywhere,” including in vehicles. Ex-1001, 1:21-34. By the time of the '192 patent, GPS systems were “well known” and “navigational purposes were prime motivators for the creation of these systems.” Ex-1018, *Hoffberg*, 8:24-27, 9:14-24, 10:1-18:14. Systems including GPS devices were able to provide location information with a typical accuracy of 100 meters and known to include “memory to record location, time, and event type, and some systems may be integrated with global information systems, to track path, speed, etc.” *Id.*, 1:17-27, 2:18-22.

B. Navigation in Vehicles

[073] By the 1990s, navigation systems existed in commercial vehicles. These navigation systems made use of stored map displays, where the maps of a

predetermined area were stored in the in-vehicle computer and displayed to the vehicle operator or driver. Ex-1018, *Hoffberg*, 7:13-17. The maps, combined with information describing the location where the vehicle started and where it was to go, resulted in a readable display that allowed a driver to follow a route. *Id.*, 7:17-20. *See supra* § VII.A.

[074] For instance, the General Motors 1994 Oldsmobile included such a system, which allowed the driver to enter details of the desired destination into an on-board or in-vehicle computer in the form of specific address, a road intersection, etc. Ex-1018, *Hoffberg*, 7:13-33. The stored map was then displayed, allowing the operator to pinpoint the desired destination, and the on-board computer then calculated the most efficient route, displaying the distance to, and the direction of, each turn using graphics and a voice prompt. *Id.* By the time of the '192 patent, it was common to use an external data source, such as a CD, to provide updates to the stored maps. Ex-1019, Acura User, Manual, 98. Removable storage was necessary at the time due to space limitations in internal memory.

[075] Before the '192 patent, users were able to store destinations, including current GPS locations and points of interest like home addresses, in the navigation system for easy access. *Id.*, 4, 19, 24, 29, 59, 77. Users were also able to save a list of destinations or trips taken during a single day, whereby the user could follow the same itinerary at a later date. *Id.*, 43. Users were also able to secure their personal

and business data stored on a navigation system with a self-selected PIN or password. *Id.*, 29, 43, 76, 79, 118.

[076] By the time of the '192 patent, numerous manufacturers, including OnStar, Alpine, Clarion, Philips, Pioneer, Visteon, and Delphi, were producing in-vehicle navigation systems, including memory and processing capabilities, in addition to handheld electronic navigation device manufacturers, like Garmin International. Ex-1020, *Walters*, 1:55-2:9; Ex-1019, Acura User Manual, 7.

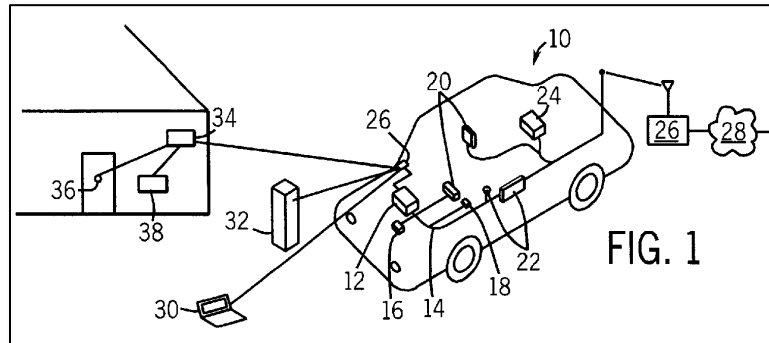
[077] Also, before the '192 patent, navigation systems storing location data derived from a GPS system including locations of interest were also known. Ex-1018, *Hoffberg*, 18:66-19:17.

C. Data Encryption

[078] By the time of the '192 patent, data encryption and decryption were also well-known, including the field of vehicles. Ex-1001, 4:60-66 (disclosing “conventional code encryption algorithms”); Ex-1018, *Hoffberg*, 9:25-45.

[079] For example, *Madau* in 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, *Madau*, Abstract. “The data may be encrypted by the key code to be secure even if the memory system is removed from the vehicle or the vehicle is stolen.” *Id.* This is illustrated in Figure 1, for

example, which shows vehicle 10 including a mobile computing module 12 and communicating with external network elements 30, 32, 34, 36, 38.



Id., 4:7-15, 4:49-5:4. Madau’s “encryption engine 82” is described in much the same way as the encryption module 128 of the ’192 patent. *Id.*, 6:23-28, 6:65-7:2, Fig. 3.

[080] Further, Taniguchi in 1997 described “[e]ncrypted route information and the like” that are stored in a “vehicle-mounted apparatus 30.” Ex-1022, *Taniguchi*, Abstract. In this system, “encryption information” is stored locally in the vehicle and used for communications external to the vehicle. *Id.*, 2:47-6:23. Further, Maeda in 1995 described encryption in vehicles in connection with payment of tolls. Ex-1023, *Maeda*, Abstract. Maeda’s “vehicle-mounted communication device” would “encrypt data to be transmitted, perform communication in a small communication area for a short period of time and prevent illegal interception of the communication data” for use with a “toll charging system that uses this vehicle-mounted communication device.”

Id., 3:6-14. In addition, Scaman in 1998 described techniques for secure and encrypted data storage in vehicles for purposes of incident verification. Ex-1024, *Scaman*, Abstract. Such techniques called for a vehicle-based device that would store encrypted and unencrypted information for later retrieval. *Id.*, 4:27-30, 5:61-6:26. Further, storing data on removable media was also well known before the '192 patent. Examples included diskettes or floppy disks (Ex-1018, 2:39; Ex-1022, 22:28-46), CDs or DVDs (Ex-1018, 27:42-43; Ex-1020, 18:3; Ex-1022, 22:48-53), and SD memory (Ex-1004, 7:10), among various others. Each of these was well known, commonplace, and conventional before the '192 patent.

VIII. LEVEL OF ORDINARY SKILL

[081] In rendering the opinions set forth in this declaration, I have been asked to consider the '192 patent's claims and the prior art through the eyes of a person of ordinary skill in the art (which I may also refer to as "one skilled in the art," "skilled artisan," "POSITA," "POSA," or similar variation). I have considered factors such as the educational level and years of experience of those working in the pertinent art, the types of problems encountered in the art, the teachings of the prior art, patents and publications of other persons or companies, and the sophistication of the technology.

[082] Taking the factors described in the Legal Standards – Level of Ordinary Skill in the Art section into consideration, and the above technology

background, it is my opinion that a person of ordinary skill in the art with respect to the '192 patent 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.

[083] Based on my educational background and experience, I was at least a person of ordinary skill in the art at the earliest priority date of the '192 patent.

IX. CLAIM CONSTRUCTION

[084] I am not an attorney. However, I have been informed by counsel of certain legal standards that apply with respect to claim construction and indefiniteness, and I have used those standards, described below, in formulating my opinions.

[085] I have been instructed that the “intrinsic record” includes the patent itself, including the claims, description, and figures (Ex-1001), and the patent’s prosecution history—i.e., the record of proceedings at the U.S. Patent and Trademark Office (“Patent Office”) concerning the patent (Ex-1003). I understand that, like the claims and written description, the prosecution history provides evidence to a person of ordinary skill in the art of how the inventor intended his patent to be understood and how the Patent Office understood the patent. I

understand that the inventor is permitted to apply a special definition to the terms or to limit the scope of claim terms in his patent claims, which may differ from the terms' plain and ordinary meanings. Such a special definition or limitation on scope may be provided in the patent's written description, the patent's prosecution history, or both.

[086] I understand that claim interpretation may also be informed by “extrinsic evidence” (that is, evidence outside of the patent record itself). I have been informed that extrinsic evidence may include dictionaries, technical treatises, and other materials evidencing the meaning of a claim term and the understanding held by a person of ordinary skill in the relevant time period.

[087] I was also informed by counsel that a patent applicant can act as their own lexicographer to set forth a definition of a claim term in the specification. The definition provided by the applicant can differ from the claim term's plain and ordinary meaning. I have also been informed by counsel that, when a patent claim uses the term “comprises” as a transitional statement after the preamble, there is a presumption that the claim is open-ended and not limited to the recited elements.

[088] Other than the terms identified below, I have been asked to assume that the claim terms otherwise have their plain and ordinary meaning to a person skilled in the art in light of the specification and the prosecution history.

A. Means-Plus-Function Terms

[089] As discussed above, I understand that there is a special category of claim terms, known as “means-plus-function” terms, that recite a structural component solely in terms of the function it performs. I understand that these terms recite functions but lack sufficient structure in the claims themselves, and that corresponding structure must be found in the specification as known to a person of ordinary skill in the art (or else the claim is indefinite). I have tried my best to identify a corresponding structure for each of the recited functions, to the extent they can be discerned from the ’192 patent’s specification. Because indefiniteness is not at issue in this proceeding, I express no opinion here about whether the structure identified below is sufficient for purposes of indefiniteness.

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

[090] A POSITA would have understood that the claimed “locational information module for determining,” in the full context in which it is recited, does not connote specific structure. Indeed, the phrase “locational information” does not add specific structure to the claimed “module.” Locational information, to a POSITA, would have suggested a type of location data, not any particular structure. This language, to a POSITA, would appear as a black box or nonce description of a function but not a specific structure for performing the function.

Accordingly, in my opinion and in accordance with the views of a POSITA, this language invokes pre-AIA § 112, ¶ 6 as a means-plus function term.

[091] 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.

[092] Structure: The specification describes that 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 location, e.g., latitude, longitude and altitude, of the device 100.” Ex-1001, 3:56-62. The corresponding structure also includes equivalents of these disclosed devices.

[093] A POSITA would have understood a locational module to include a receiver and antenna to employ conventional locational information techniques, consistent with GPS systems and vehicle navigation technology known at the time of the ’192 patent, as discussed above. *See supra* §§ VII.A and VII.B.

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

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

[094] A POSITA would have understood that the claimed “encryption module for encrypting,” in the full context in which it is recited, does not connote specific structure. Indeed, the phrase “encryption” does not add specific structure to the claimed “module.” Rather than serve as structure, a POSITA would have understood “encryption” to be a function or action—encrypting. To a POSITA, this recitation would appear as a black box or nonce description of a function but not a specific structure for performing the function. Accordingly, in my opinion and in accordance with the views of a POSITA, this language invokes pre-AIA § 112, ¶ 6 as a means-plus function term.

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

[096] Structure: A POSITA would have understood that the “encryption module” is an encryption technique, such as the techniques referenced in the specification—i.e., symmetric-key techniques, including DES, Triple-DES, Blowfish, RC2, RC4, and RC5, and asymmetric-key techniques, including Diffie-Hellman, RSA, and ElGamal. *See, e.g.*, Ex-1001, 4:60-66. The corresponding structure also includes equivalents of these techniques.

[097] A POSITA would have understood an encryption module to be an encryption technique, which were widely available and well known at the time of the '192 patent as described above. *See supra* § VII.C.

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

[098] A POSITA would have understood that the claimed “storage module for storing,” in the full context in which it is recited, does not connote specific structure. Indeed, the phrase “storage” does not add specific structure to the claimed “module.” A POSITA would have understood that “storage” is an action or function—i.e., the action or function of storing. This language, to a POSITA, would appear as a black box or nonce description of a function but not a specific structure for performing the function. Accordingly, in my opinion and in accordance with the views of a POSITA, this language invokes pre-AIA § 112, ¶ 6 as a means-plus function term.

[099] Function: Claims 13 and 22 recite the following function for the claimed “storage module”: “storing the encrypted location information.”

[100] Structure: The specification states “the storage module may be [an] internal memory.” Ex-1001, 2:4-5; *see also id.*, 2:21-22. The specification further provides “[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.

[101] A POSITA would have understood the structure of the “storage module” to include the removable and non-removable forms of memory described above. By contrast, the “removable storage module,” which is separately recited in other claims of the ’192 patent, is limited to the removable forms of memory from the above listing. Indeed, a POSITA would have appreciated the patentee’s delineation in the claims between these two different forms of storage. The corresponding structure also includes equivalents of this disclosed structure.

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

[102] A POSITA would have understood that the claimed “removable storage module for storing,” in the full context in which it is recited, does not connote specific structure. Indeed, the phrase “removable storage” does not add specific structure to the claimed “module.” Instead, “removable storage” would connote two actions to a POSITA—removing and storing. As a POSITA would view this claim, the “module” is recited as a black box or nonce description of a function but not a specific structure for performing the function. Accordingly, in

my opinion and in accordance with the views of a POSITA, this language invokes pre-AIA § 112, ¶ 6 as a means-plus function term.

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

[104] Structure: Claims 1 and 19 describe the “removable storage module” as being “removably disposed in the housing.” Claim 19 also discloses a circumstance where the “removable storage module” is “removably disposed in the reader.”

[105] The specification states “[i]n another aspect, the storage module is removable storage memory.” Ex-1001, 2:18-19. Therefore, a POSITA would have understood the structure of a “removable storage module” to be a “removable storage memory” including in the form of structures described above in § IX.A.3 for the term “a 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”). The corresponding structure also includes equivalents of these disclosed removable memories.

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

[106] A POSITA would have understood that the claimed “processing module,” in the full context in which it is recited, does not connote specific structure. Indeed, the phrase “processing” does not add specific structure to the claimed “module.” This language, to a POSITA, would appear as a black box or nonce description of a function but not a specific structure for performing the function. Accordingly, in my opinion and in accordance with the views of a POSITA, this language invokes pre-AIA § 112, ¶ 6 as a means-plus function term.

[107] Function: The “processing module” serves 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.

[108] 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.” Claim 3, unlike

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

claim 16, is directed to location information stored in the **removable** storage module.

[109] Structure: The specification describes the structure of the processing module as “a computer processing module 120, e.g., a microprocessor. The computer processing module 120 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. It is to be understood that the present disclosure may be implemented in various forms of hardware, software, firmware, special purpose processors, or a combination thereof.” Ex-1001, 3:26-34. The specification later abbreviates “the computer processing module” 120 to “the processing module.” *E.g., id.*, 4:5, 5:4, 5:10. The corresponding structure also includes equivalents of this disclosed structure.

[110] The structure of the processing module is supported by the '192 patent file history. In a September 9, 2010, non-final rejection, claims 1, 13, 19 and 22 were rejected under 35 U.S.C. § 112 as failing to comply with the enablement requirement because the phrase “[a] processing module for sending the encrypted location information to the removable storage module . . .” was found not to be described in the specification. Ex-1003, 48-50. On December 8, 2010, the Applicant amended the specification and the claims, and submitted remarks in

support of allowing the claims. *Id.*, 67-84. In its remarks, the Applicant described the processing module as interacting with and organizing the traffic flow. The Applicant stated:

The computer processing module 120 is configured to “organize the traffic flow between the various other modules” (paragraph 0028). The encryption module 128 encrypts addresses and route points and this information is stored in the storage module 110 (paragraph 0036). One skilled in the art would clearly understand that a processing module that is configured to organize traffic flow between modules will at least assist in sending the encrypted information from the encryption module to the storage module.

Id., 76.

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

[111] A POSITA would have understood that the claimed “input module disposed on the housing configured for receiving,” in the full context in which it is recited, does not connote specific structure. Indeed, the phrase “input” does not add specific structure to the claimed “module.” Rather, a POSITA would have understood “input” to connote the function or action of inputting, not specific structure. This language, to a POSITA, would appear as a black box or nonce description of a function but not a specific structure for performing the function. Accordingly, in my opinion and in accordance with the views of a POSITA, this language invokes pre-AIA § 112, ¶ 6 as a means-plus function term.

[112] Function: Claims 2 and 15 recite the following function for the claimed “input module”: “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.” Claim 2, unlike claim 15, is directed to encrypting and decrypting the location information stored in the **removable** storage module.

[113] Structure: Claims 2 and 15 describe that the “input module” is “disposed on the housing.” 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. The corresponding structure also includes equivalents of this disclosed structure.

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

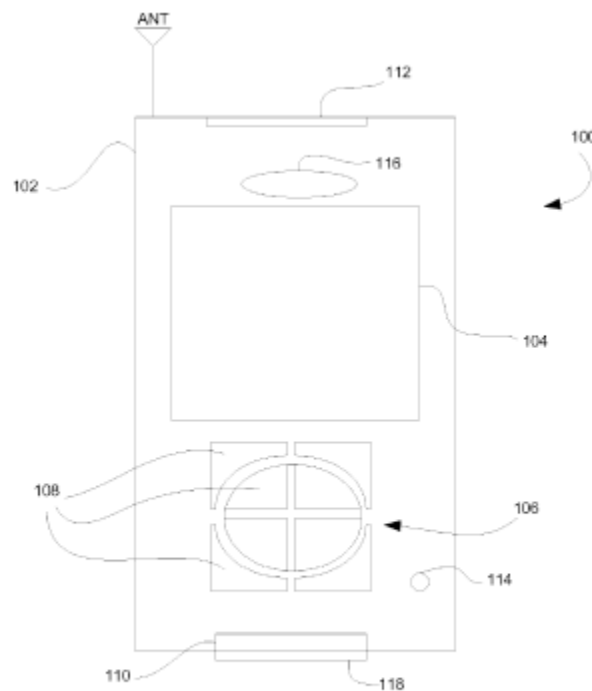


FIG. 1

[114] The specification further provides “[t]he device 100 of the present disclosure will contain a user input module 126 to either 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. Preferably, the character recognition device is a touch screen which overlays the display module 104 and text is entered via a pen-like stylus. Such input devices are standard and currently available on many electronic devices including portable digital assistants (PDAs) and cellular telephones. Optionally, microphone 114 may be further coupled to the input module 126 for capturing any audio information spoken by the user and the input

module will further include an analog-to-digital (A/D) converter for converting the spoken audio information into a digital format. Furthermore, the input module may include a voice recognition processor that translates the digital human voice into alpha numeric characters for user input. The user will utilize the user input module 126 to enter various data, for example, a plurality of destination addresses, waypoints, etc.” *Id.*, 4:27-46.

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

[115] A POSITA would have understood that the claimed “user verification module for verifying the identity of [the] user,” in the full context in which it is recited, does not connote specific structure. Indeed, the phrase “user verification” does not add specific structure to the claimed “module.” As a POSITA would have appreciated, “user verification” is itself a function or action, not a definite structure. This language, to a POSITA, would appear as a black box or nonce description of a function but not a specific structure for performing the function. Accordingly, in my opinion and in accordance with the views of a POSITA, this language invokes pre-AIA § 112, ¶ 6 as a means-plus function term.

[116] Function: Claims 3 and 16 recite the following function for the claimed “user verification module”: “verifying the identity of user of the device.”

[117] Claims 4 and 17 recite the same function for the claimed “user verification module,” and further recite that the “user verification module” **“executes a password protection algorithm** for verifying the identity of the user of the device.” 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.”

[118] Structure: The specification describes a “user verification module 130” that “will indicate and verify the identity of the user of the device 100.” Ex-1001, 5:49-51. “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.” *Id.*, 5:51-54. If the user verification module includes an identity capture device, such 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.” *Id.*, 5:54-59. The corresponding structure also includes equivalents of this disclosed structure.

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

[119] A POSITA would have understood that the claimed “transmission module for transmitting,” in the full context in which it is recited, does not connote specific structure. Indeed, the phrase “transmission” does not add specific structure to the claimed “module.” To the contrary, a POSITA would interpret the “transmission” recitation as referring to the function or action of transmitting. This language, to a POSITA, would appear as a black box or nonce description of a function but not a specific structure for performing the function. Accordingly, in my opinion and in accordance with the views of a POSITA, this language invokes pre-AIA § 112, ¶ 6 as a means-plus function term.

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

[121] Structure: The specification describes that “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. The specification describes: “[i]f the information is stored in internal memory instead of removable

memory, the transfer will be done by transmission module 112 including hardwired and/or wireless connectivity. The hardwire connection may include but is not limited to hard wire cabling e.g., parallel or serial cables, USB cable, Firewire (1394 connectivity) cables, and the appropriate port. The wireless connection will operate under any of the 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.” *Id.*, 6:26-40. The corresponding structure also includes equivalents of this disclosed structure.

X. THE PRIOR ART

[122] In forming my opinions, I found the following prior art relevant when considering whether the claims of the '192 patent would have been obvious to a person of ordinary skill in the art:

- Ex-1004, U.S. Patent No. 6,490,513 to Fish et al. (“*Fish*”)
- Ex-1005, U.S. 2004/0103288 A1 to Ziv et al. (“*Ziv*”)
- Ex-1006, U.S. Patent No. 6,310,542 to Gehlot (“*Gehlot*”)
- Ex-1007, European Patent Publication No. EP0962894A2 to Stevenson (“*Stevenson*”)

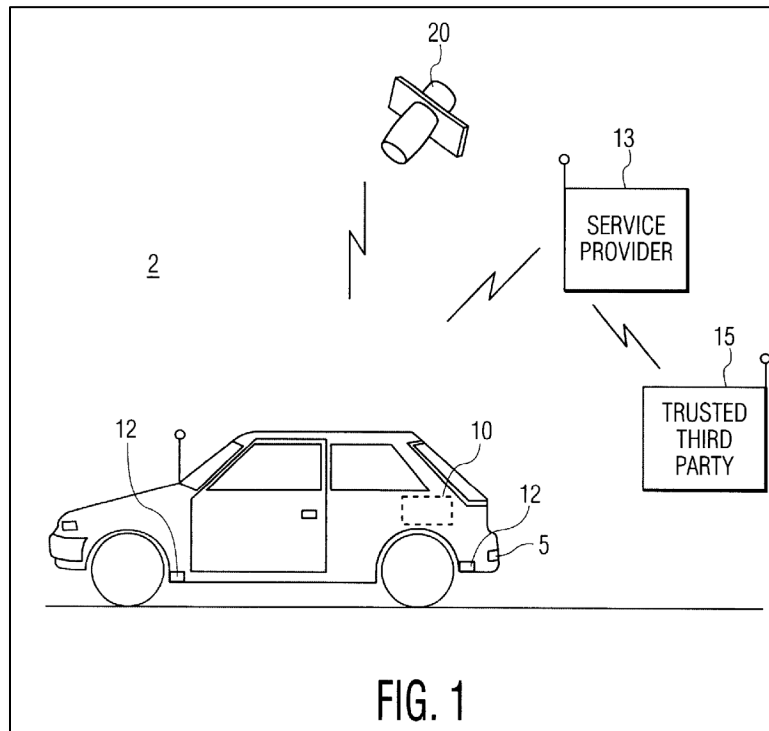
[123] None of these references were cited during prosecution of the '192 patent or considered by the Examiner. Ex-1003; Ex-1001, Cover. However, I understand that the '192 patent has a single child application, a continuation filed on December 14, 2011, as U.S. Patent Application Number 13/326,214 (“the '214 application”) and published on April 12, 2012, as US 2012/0089324 A1. Ex-1025, 64. *Fish* was cited and applied by the Examiner during the prosecution of the child '214 application. *Id.*, 257. Despite amending the claims and arguing against multiple rejections in view of *Fish*, the Applicant failed to provide arguments that were persuasive to the Examiner with respect to overcoming *Fish* and thereafter abandoned the child '214 application. *Id.*, 309-25, 334-49, 352-53, 383-98, 402-16, 420-21.

A. Overview of *Fish* (Ex-1004, U.S. 6,490,513)

[124] *Fish* is a U.S. patent issued December 3, 2002, directed to a “vehicle data archive system” using encryption. Ex-1004, Abstract. The corresponding application was filed August 22, 2001. *Id.*, Cover. I understand that *Fish* is accordingly a prior art reference under pre-AIA 35 U.S.C. § 102(b).

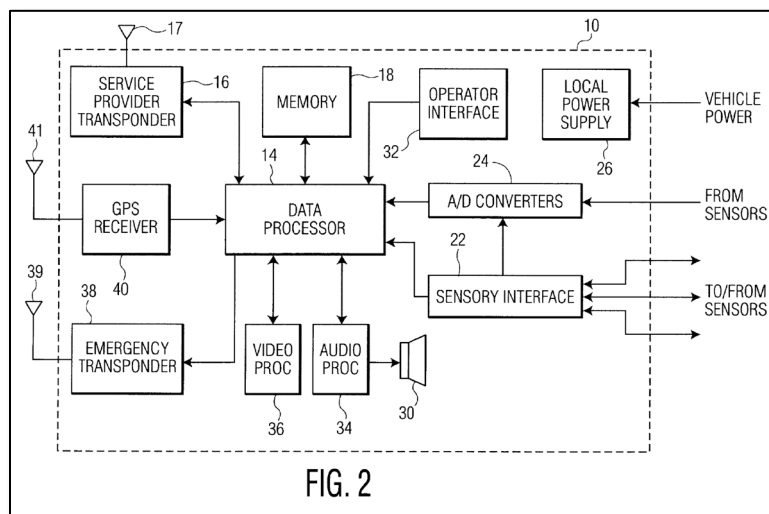
[125] Like the '192 patent, *Fish* discloses controlling and storing sensitive data from a vehicle securely, including location information and information derived from a GPS unit. Ex-1004, Abstract, 1:5-9, 4:22-29, 5:27-32, 7:6-52,

Figs. 1 and 2. As *Fish* describes, a vehicle data archive system (VDAS) 2 may be included in a vehicle 5 having a data archive 10.



Id., 2:45-52, Fig. 1.

[126] *Fish*'s data archive 10 is shown in more detail in Figure 2, below:



Id., 4:22-29, Fig. 2.

[127] Like the '192 patent, *Fish* teaches the conventionality of encrypting data relating to a vehicle, including its location information, whereby the encryption enables the vehicle data to be accessible by authorized personnel. *Id.*, 4:8-21, 5:26-38, 11:8-29. Also, like the '192 patent, *Fish* teaches the conventionality of including “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.” *Id.*, 7:8-14.

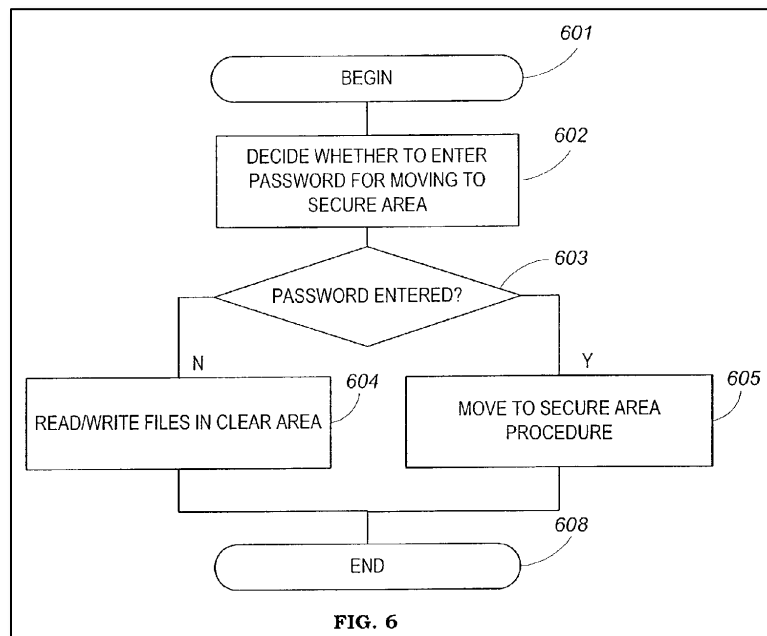
B. Overview of *Ziv* (Ex-1005, U.S. 2004/0103288 A1)

[128] *Ziv* is a U.S. Patent Publication published May 27, 2004, directed to a “portable storage device including a microprocessor.” Ex-1005, Abstract. The corresponding application was filed November 27, 2002. *Id.*, Cover. I understand that *Ziv* is accordingly a prior art reference under pre-AIA 35 U.S.C. § 102(b).

[129] *Ziv* discloses “[a] portable storage device including a microprocessor and a secure user data area, the microprocessor operable to perform on-the-fly encryption/decryption of secure data stored on the storage device under a user password, the microprocessor also operable to exclude access to the secure user data area unless the user password is provided.” *Id.*, Abstract.

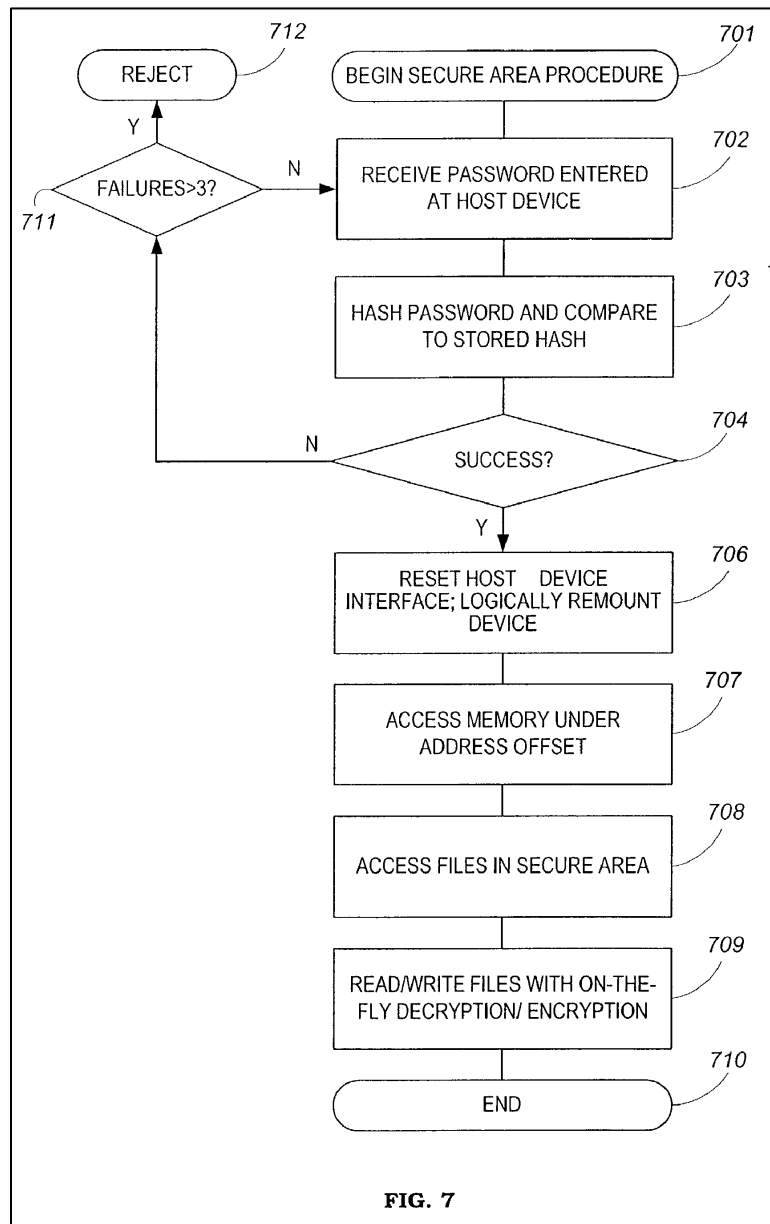
[130] *Ziv* discloses various techniques for using a password to selectively encrypt or decrypt data. For example, as shown in Figure 6, a user may enter a

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.

[131] Further, in Figure 7, *Ziv* describes a process of a user entering a password and, if the password is verified, the device performs encryption or decryption operations in step 709.



Id., ¶¶ [0038]-[0040], Fig. 7.

[132] Like the '192 patent and *Fish*, *Ziv* discloses the use of a removable storage device to store personal confidential information. *Id.*, Abstract, ¶¶ [0001], [0025]. For example, *Fish* discloses use of removable storage media such as secure digital (SD) memory and the like, Ex-1004, 7:6-29, and *Ziv* teaches the same types

of memory, Ex-1005, ¶ [0025]. Indeed, *Ziv* confirms that its storage medium 113 may be “detachable from portable storage device 110” and may include “a ZIP drive or a portable unit accommodating a Compact Flash or Secure Digital memory module.” Ex-1005, ¶ [0025]. 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 to provide further enhanced security. *Id.*, Abstract, ¶¶ [0026], [0031], [0033], [0037]-[0045].

C. Overview of *Gehlot* (Ex-1006, U.S. 6,310,542)

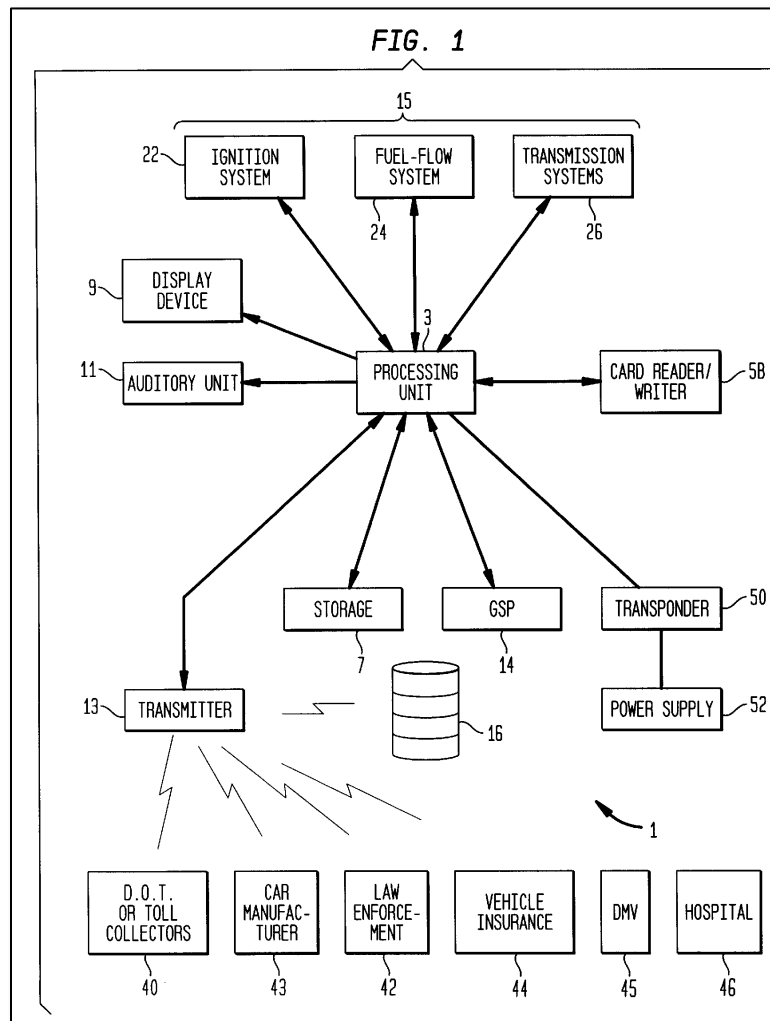
[133] *Gehlot* is a U.S. Patent issued October 30, 2001, directed to “a system for receiving, processing, and storing real-time data from various types of input, including but not limited to information from a vehicle’s micro-processing systems, a driver information card, a vehicle information card, and physical attributes of the driver/owner.” Ex-1006, Abstract. The corresponding application was filed August 19, 1999. *Id.*, Cover. I understand that *Gehlot* is accordingly a prior art reference under pre-AIA 35 U.S.C. § 102(b).

[134] *Gehlot* discloses “a system for collecting vehicle data and preventing unauthorized vehicle use, and, in particular, a system for collecting data from various vehicle systems, information cards, and other external data sources and transmitting the collected data to external data receivers.” *Id.*, 1:5-9.

[135] *Gehlot* discloses a “vehicle data processor” prompting the vehicle 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. *Id.*, 2:3-8, 2:17-31, 6:1-12. The input may alternatively be a “password via a keyboard.” *Id.* “During the trip, the [vehicle data system] constantly monitors the vehicle’s systems and provides data regarding operation of such systems.” *Id.* Said data can also be shared with third parties. *Id.*

[136] Like the ’192 patent and *Fish*, *Gehlot* also discloses the use of removable storage cards for the storage of vehicle-related information, as well as the 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.” *Id.*, 4:24-5:33. The information stored on the data storage device further has the ability to be transmitted to external entities and devices. *Id.*, 5:34-66.

[137] Further, the system in *Gehlot* preferably includes a GPS unit, and “data from the GPS unit can also be routed by the processor unit 3 to transmitter 13 to be sent to law enforcement.” *Id.*, 6:51-54. *Gehlot* discloses “[t]he use and operation of GPS systems are well-known in the art and, therefore, these systems require no further discussion.” *Id.*, 6:55-58.



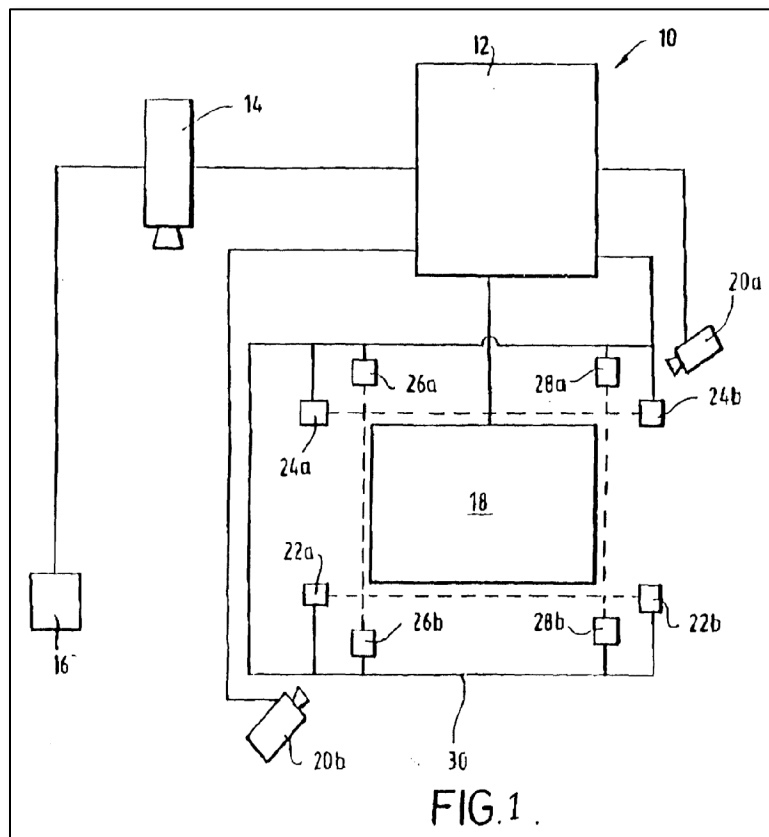
Id., Fig. 1.

D. Overview of *Stevenson* (Ex-1007, European Patent Pub. EP0962894A2)

[138] *Stevenson* is a European Patent Publication which published December 8, 1999, directed to “a vehicle entry/exit control system.” Ex-1007, Cover. The corresponding application was filed May 28, 1999. *Id.* I understand that *Stevenson* is accordingly a prior art reference under pre-AIA 35 U.S.C. § 102(b).

[139] *Stevenson* describes the use of biometric sensing methods to confirm the identity of a driver in order to control the entry and exit of vehicles within a restricted area. *Id.*, Abstract, ¶¶ [0001], [0004]-[0007]. The described biometric sensing methods include iris recognition, fingerprint, palm print, voice pattern and DNA, such as saliva. *Id.*, ¶¶ [0007], [0019]-[0020].

[140] For example, *Stevenson's* 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.



Id., ¶¶ [0007]-[0010], Fig. 1.

XI. OVERVIEW OF THE GROUNDS

Grounds	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 Ziv
Ground 3	5-8, 18	§ 103	<i>Fish</i> in view of Ziv and Gehlot
Ground 4	9-10	§ 103	<i>Fish</i> in view of Ziv, Gehlot, and Stevenson

XII. GROUND 1: *FISH* (CLAIMS 1, 11-14, 19-22)

[141] Claims 1, 11-14, 19-22 of the '192 patent are unpatentable as obvious in view of *Fish*, alone or in view of the knowledge of a POSITA.

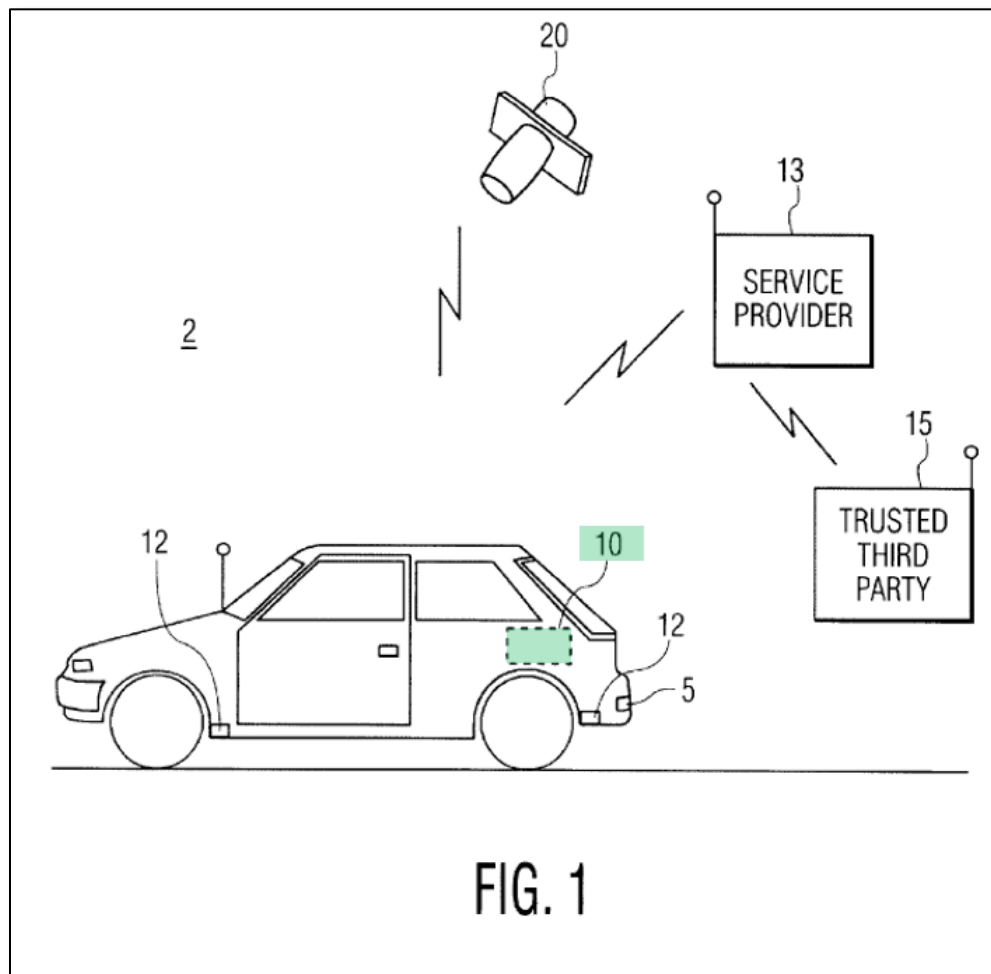
A. Claim 1

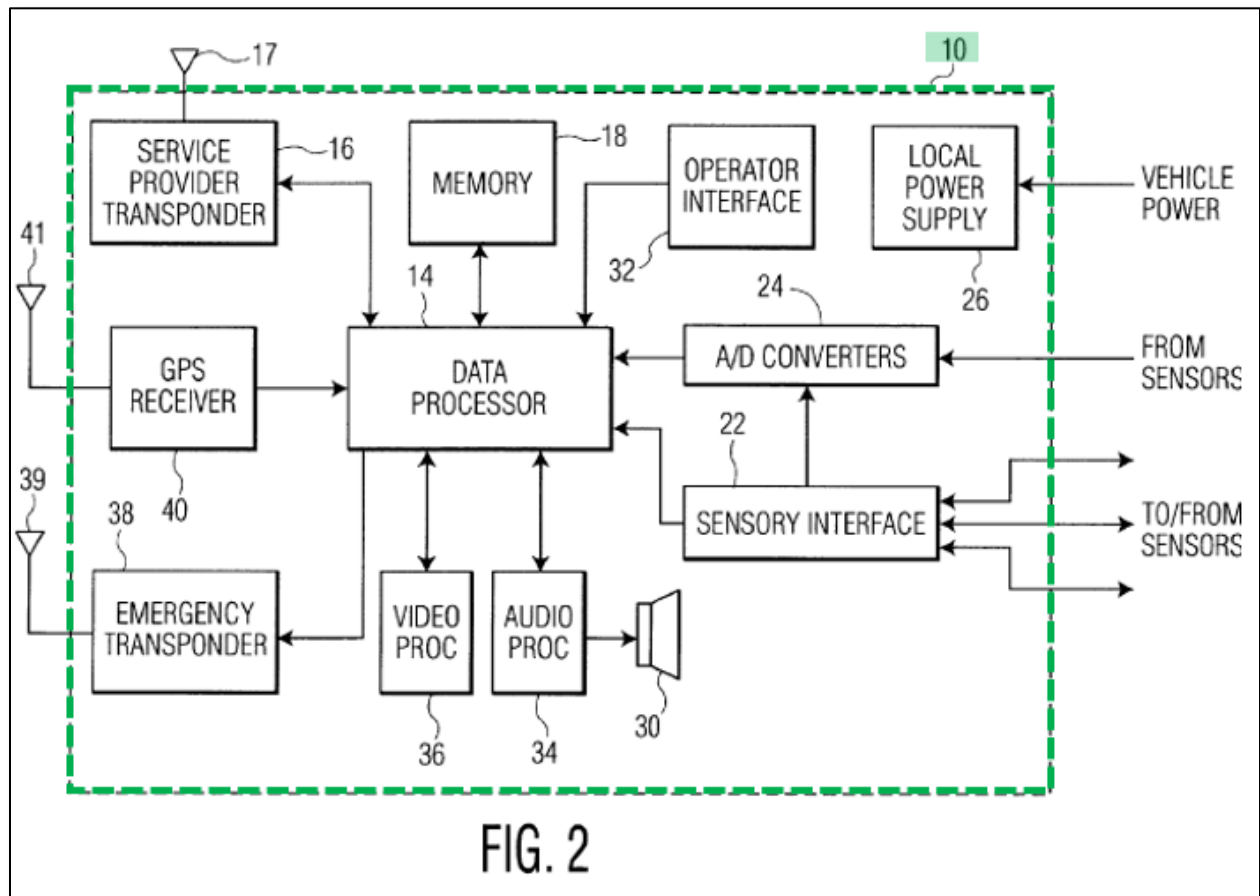
1. [1pre] A location information device with secure data storage comprising:

[142] I understand that the beginning portion of a claim is called the “preamble.” I also understand that, for the purposes of this proceeding, the preamble is not considered as a requirement of the claim. In my view, even if the preamble of claim 1 was considered a requirement, *Fish* describes the preamble of claim 1.

[143] *Fish* teaches a location information device with secure data storage, as recited in [1pre]. *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.

[144] *Fish*'s Abstract 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. *Id.*, Abstract. The information may be encrypted (i.e., "secure," as claimed). *Id.* Indeed, *Fish* discloses that "[t]he present invention relates to a data archive system for securely archiving signals," including "situational data concerning a vehicle." *Id.*, 1:6-9, 1:36-54, 2:16-43. *Fish* teaches storing and encrypting received information in "data archive 10 located in a vehicle." *Id.*, 2:45-57, Fig. 1.



Id., Fig. 1 (annotated)*Id.*, Fig. 2 (annotated)

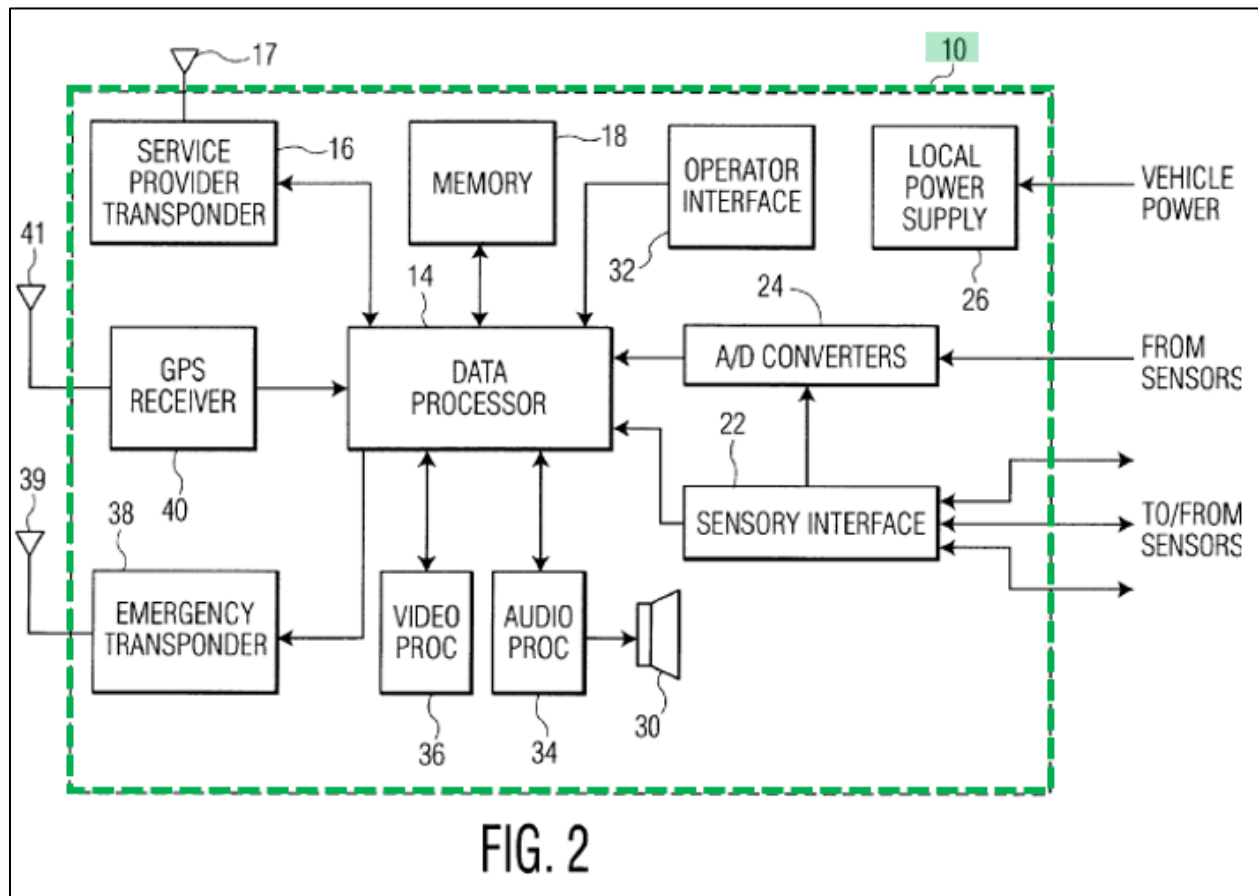
[145] *Fish* discloses storing encrypted “location” information, including GPS information, in “**data archive 10**,” e.g., in memory 18, which is a “location information device with secure data storage” as claimed. *Id.*, 3:10-27, 4:8-15, 4:22-29, 4:57-59, 7:30-56, 8:41-53, 11:8-14, Fig. 1.

2. [1a] a housing;

[146] *Fish* discloses a housing, as recited in [1a], for the location information device. Ex-1004, 2:66-3:9.

[147] *Fish* discloses “[t]he data archive 10 of the exemplary embodiment is preferably **housed in a sealed cabinet** (not shown).” *Id.*, 3:2-4 (emphasis added). *Fish* explains this housing “is desirably fire and water resistant and designed to offer significant resistance to crush forces typically encountered in catastrophic vehicle wrecks.” *Id.*, 3:6-9.

[148] A POSITA would have readily and obviously understood that *Fish*’s housing or sealed cabinet discloses the “housing” of claim 1. Indeed, no unique physical or functional attributes of such a “housing,” are recited in claim 1. The specification of the ’192 patent likewise imposes no unique structural or functional requirements for the “housing,” other than it being “rectangular” in some embodiments. Ex-1001, 3:7-9; *see also id.*, Fig. 1. The same characteristics are present in *Fish*’s data archive 10, which may have a housing or sealed cabinet, and is illustrated with a rectangular shape. Ex-1004, 3:2-6, Fig. 2. A POSITA would have understood that it was very common for electronics to exist in an enclosure and that the most common shape of an enclosure was a box-type shape. Indeed, a POSITA would have recognized that the claimed “housing” is not itself inventive or nonobvious (either alone or in combination with the remainder of the claim), and is not described in the ’192 patent as new or inventive.



Id., Fig. 2.

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;

[149] *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, as recited in [1b]. *E.g.*, Ex-1004, 4:22-29, 5:27-32, 7:23-51, Figs. 1-2.

[150] As discussed above in § IX.A.1, the claimed “locational information module” in claims 1, 13, 19, and 22 should be construed as a means-plus-function

term. The function of this term is determining location information of the device, and the corresponding structure is 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 location, e.g., latitude, longitude and altitude, of the device 100.” Ex-1001, 3:56-62. As discussed below, *Fish* discloses this same function and corresponding structure. In particular, *Fish*’s GPS receiver 40 and antenna 41 serve as a structure for performing the function of determining routes traveled.

[151] *Fish* discloses that **data archive 10** may include **GPS receiver 40** that determines location information. Ex-1004, 4:22-29, Fig. 2. The **GPS receiver 40** also records temporal data corresponding to the location information. *Id.*, 4:22-29, 5:27-32. **GPS receiver 40** has an associated **antenna 41**, as indicated using the standard antenna symbol well-known to a POSITA. *Id.*, Fig. 2. Indeed, *Fish* uses the same symbol for “antenna 17.” *See id.*, 4:43-51, Fig. 2. Therefore, a POSITA would readily have understood that *Fish* also includes a GPS and an antenna.

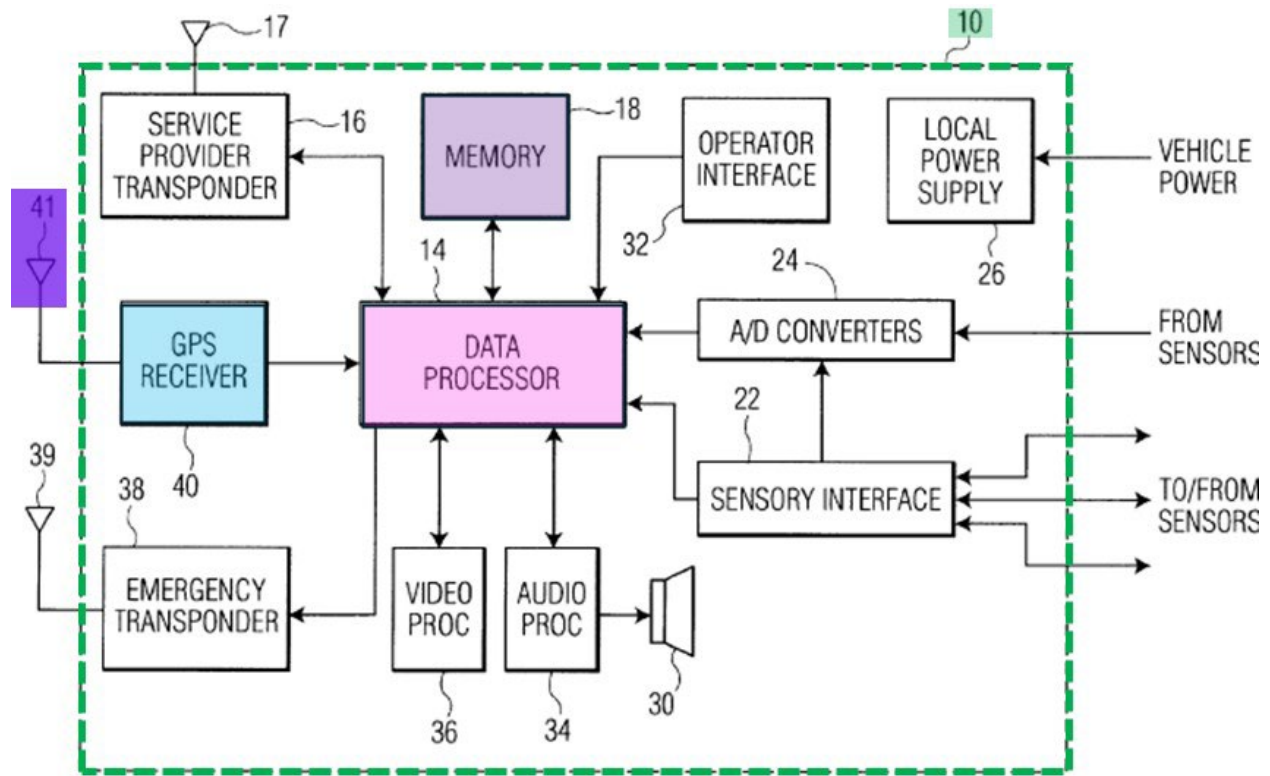


FIG. 2

Id., Fig. 2 (annotated)

[152] Data may be stored at a “predetermined interval (e.g., 15 seconds)” to better ensure relevant data exists at the time of an accident. *Id.*, 7:23-29. A POSITA would have understood that by storing location data collected at predetermined time intervals, the resulting stored data provides the route traveled by the device. A POSITA would have known that primitive GPS models displayed the path traveled as a series of dots, or “breadcrumbs,” on a screen in-line with navigational practices dating back at least to the 1400s. A POSITA would understand that storing route information as raw latitude and longitude data or as a

function of predetermined intervals would be advantageous where data storage capacity is limited in comparison to storing route information superimposed on cartographic information, which may require additional storage space.

[153] For example, as a POSITA would understand, storing location data every 15 seconds would produce route information such as the following:

Time	Location
0 seconds	GPS location #1
15 seconds	GPS location #2
30 seconds	GPS location #3
45 seconds	GPS location #4
...	...
X seconds	GPS location #Y

[154] A POSITA would have understood that, if given a sequence of location points over time, in addition to other characteristics of a route, such as speed and heading, a location on a map can be determined. A POSITA would have understood that such a series of points (or, in navigation terms, “waypoints”) would be understood to form a route. Indeed, it would have been obvious to a POSITA that such route data would represent various types of routes traveled by a vehicle (i.e., any route actually traveled).

[155] *Fish* thus discloses and renders obvious the determined location information being at least one route traveled by the device, as recited in [1b]. Ex-1004, 5:27-32, 7:30-52, 11:8-26.

[156] *Fish* also provides an example in which “a vehicle is traveling” a particular route and 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.

Id., 11:8-26 (emphasis added).

[157] *Fish* further explains:

In an alternative embodiment, the data archive 10 may not send a digital signature to the service provider 13 but may encrypt and record the sensory data signals as composite sensory data signals, **concatenated with temporal and/or cartographic reference data from the GPS signal** using a secure encryption key.

Id., 5:27-32 (emphasis added).

[158] *Fish* thus discloses and renders obvious, again in these examples, the determined location information being at least one *route* traveled by the device, as recited in [1b]. Such a route would be the time, location, direction, and/or cartographic data of the vehicle over time. *Id.*, 11:8-26, 5:27-32.

[159] Indeed, *Fish* further discloses the **data processor 14** uses a portion of **secure memory 18** with preloaded cartographic content to use in conjunction with GPS information to identify a cartographic location, i.e., the location on a map:

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**.

Id., 7:30-41 (emphases added).

[160] In addition, claim 21 of *Fish* recites a GPS communication module “responsive to global positioning signals for identifying a cartographic location of the modular data archive.” *Id.*, 14:23-27 (claim 21).

[161] *Fish* additionally emphasizes that “location and temporal signals” from **GPS receiver 40** are “widely available,” 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.” *Id.*, 7:42-49 (emphasis added). Alternatively, latitude and longitude “may simply be recorded” without translation into cartographic location in other embodiments. *Id.*, 7:49-51. *Fish* thereby discloses cartographic locations are more than mere GPS coordinates—a POSITA would have understood *Fish*’s cartographic locations to be locations traveled on a map, including a route traveled.

[162] Accordingly, a POSITA would also have understood that the “conjunction” of cartographic content (i.e., map information) with GPS data and temporal data would have included “at least one route travelled by the device.” *Fish*’s temporal location data stored in conjunction with cartographic (map) locations constitute “route travelled” data. It would have been obvious to a POSITA that the cartographic locations determined by *Fish*’s data processor would have included a route traveled by the vehicle.

[163] Further, a POSITA would have found storing a “route travelled” obvious given *Fish*’s disclosure of storing GPS coordinates, times, directions, speeds, and cartographic locations in light of *Fish*’s stated goals to record “situational data concerning a vehicle” to assist with enforcement of driving rules by law enforcement and resolve disputes between insurance companies, including after accidents. *Id.*, 1:6-33, 2:16-24, 7:23-27, 11:8-29.

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

[164] *Fish* discloses an encryption module for encrypting the determined location information, as recited in [1c]. *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.

[165] As discussed above in § IX.A.2, the encryption module of claims 1, 13, 19, and 22 would be construed as a means-plus-function term. The function of this term is encrypting the determined location information, and the corresponding structure is an encryption technique, such as the techniques disclosed in the specification—i.e., symmetric-key techniques, including DES, Triple-DES, Blowfish, RC2, RC4, and RC5, and asymmetric-key techniques, including Diffie-Hellman, RSA, and ElGamal. *See, e.g.*, Ex-1001, 4:60-66. As discussed below, *Fish* discloses this function and structure. In particular, *Fish*'s **data processor 14** or **data archive 10** perform the same conventional types of data encryption disclosed in the '192 patent for the claimed encryption module. *E.g.*, Ex-1004, 4:43-5:3, 9:18-28, 10:16-30, 12:1-12.

[166] *Fish* discloses storing data on its data archive system using a “secret encryption key.” *Id.*, 1:35-54, 2:16-24. The encryption key may be generated by a service provider. *E.g.*, *Id.*, 2:25-42, 3:10-37, 4:8-21 (encrypting GPS data), 5:27-38 (encrypting and storing composite data, including GPS data), Figs. 2-3. In some

embodiments, the **data processor 14** of the **data archive 10** receives keys from the service provider to encrypt and store information in **memory 18**. *E.g., Id.*, 4:43-54, 13:9-22 (claim 10, reciting “data processor which encrypts the . . . data signal”), Figs. 1-2.

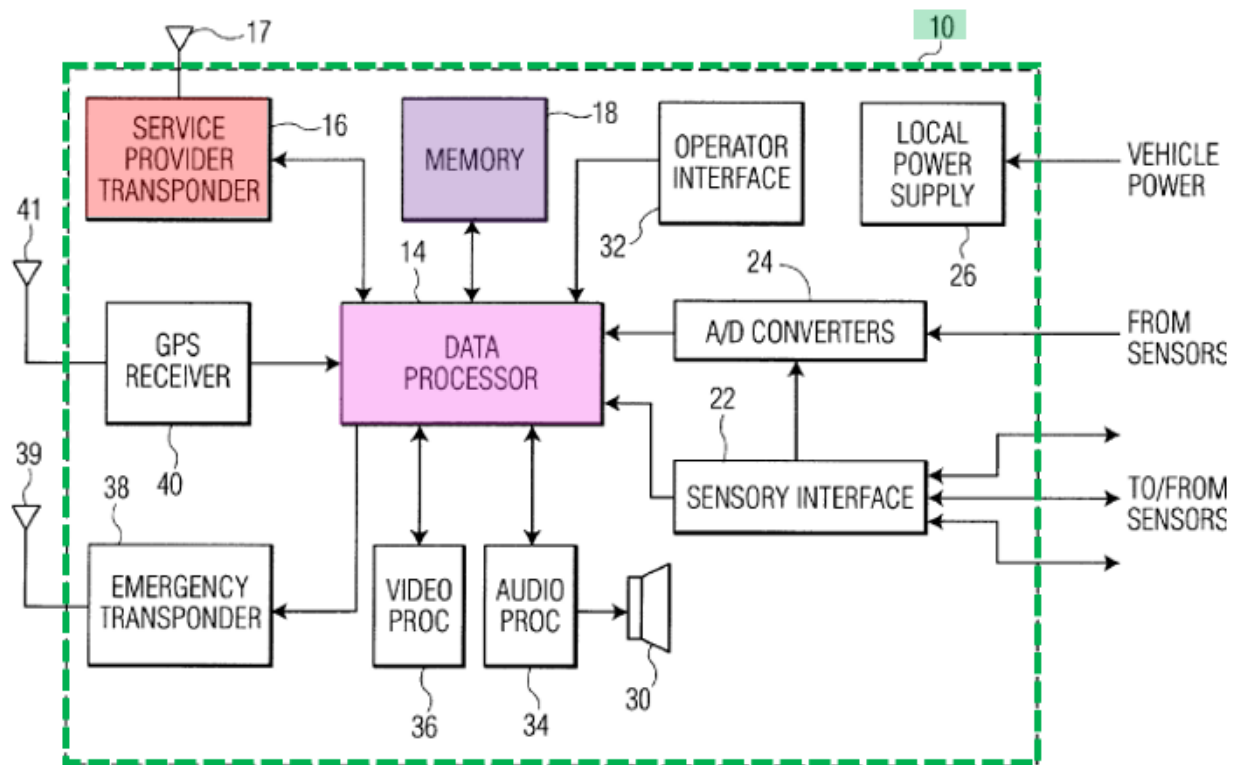


FIG. 2

Id., Fig. 2 (annotated)

[167] Encrypted data includes GPS information and “cartographic information.” *Id.*, 4:8-22 (GPS data “may be combined . . . with the sensory signal data prior to encryption.”), 5:27-32 (data archive may encrypt temporal, cartographic, GPS, and sensory data), 7:30-49 (storing longitude, latitude, and

cartographic data in **secure memory 18**), 14:23-27 (claim 21). The conventional encryption techniques disclosed in *Fish*—similar to the '192 patent itself—include Diffie-Hellman key exchange, and the like. *Id.*, 4:66-5:4, 9:25-31, 10:5-11, 10:26-30, 12:1-5; *see also* Ex-1001, 4:60-5:3 (discussing conventional encryption techniques such as “DES, Triple-DES, Blowfish, RC2, RC4, RC5, etc.,” and “Diffie-Hellman, RSA, ElGamal, etc.”).

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

[168] *Fish* discloses a removable storage module for storing the encrypted location information, the removable storage module being removably disposed in the housing, as recited in [1d]. *E.g.*, Ex-1004, 7:6-29.

[169] As discussed above in § IX.A.4, the removable storage module of claims 1 and 19 would be construed as a means-plus-function term. The function of this term is storing the encrypted location information, and the corresponding structure is storage removably disposed in the housing, e.g., 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), or SD (Secure Digital) memory.

[170] *Fish* discloses that its “secure memory 18 is a **removable** non-volatile memory device such as a secure digital (SD) memory device.” Ex-1004, 7:6-29

(emphasis added). *Fish* explains “secure memory 18 is **removable** to allow for easy access to the data after an accident.” *Id.* (emphasis added). Consistent with the discussion above in § XII.A.2, *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. *Id.*, 3:2-9. According to such disclosure, *Fish*’s removable “**secure memory 18**” (e.g., SD memory, or the like) would be removably disposed in the housing. This **secure memory 18** stores *Fish*’s encrypted location data. Ex-1004, 11:44-51, 3:32-36, 3:61-66, 1:46-50, 3:10-4:7, 4:45-5:38, 5:39-44, 5:55-57, 7:6-29, Abstract, Figs. 2, 4, claims 2, 10, 11.

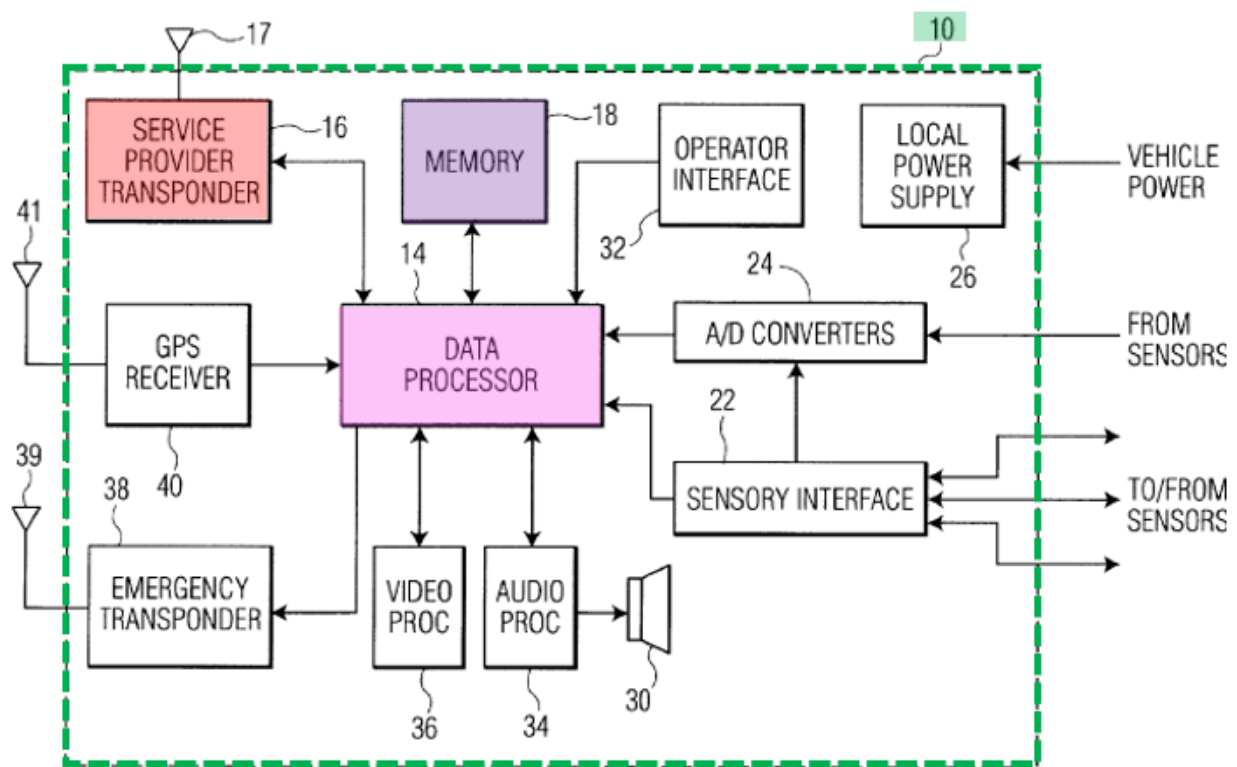


FIG. 2

Id., Fig. 2.

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.**

[171] *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 recited in [1e]. *E.g.*, Ex-1004, 4:8-22, 4:51-54, 5:27-32, 6:63-7:5, 7:30-49, Fig. 2.

[172] As discussed above in § IX.A.5, the processing module of claims 1, 13, 19, and 22 would be construed as a means-plus-function term. The recited function for the claimed processing module is “sending the encrypted location information to the [] storage module [] . . . and retrieving the encrypted location information from⁴ 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. The corresponding structure is a computer processing module 120, e.g., a microprocessor. The computer processing module 120 will use computer software instructions that have been programmed into the module and conventional computer processing power to interact with and organize the traffic

⁴ Claim 19 mistakenly recites “form” instead of “from.”

flow between the various other modules. Ex-1001, 3:26-34. *Fish* discloses this function and structure, as discussed below.

[173] According to *Fish*, **data processor 14** 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. **Data processor 14** encrypts data and stores encrypted data, including location information. *E.g., id.*, 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.

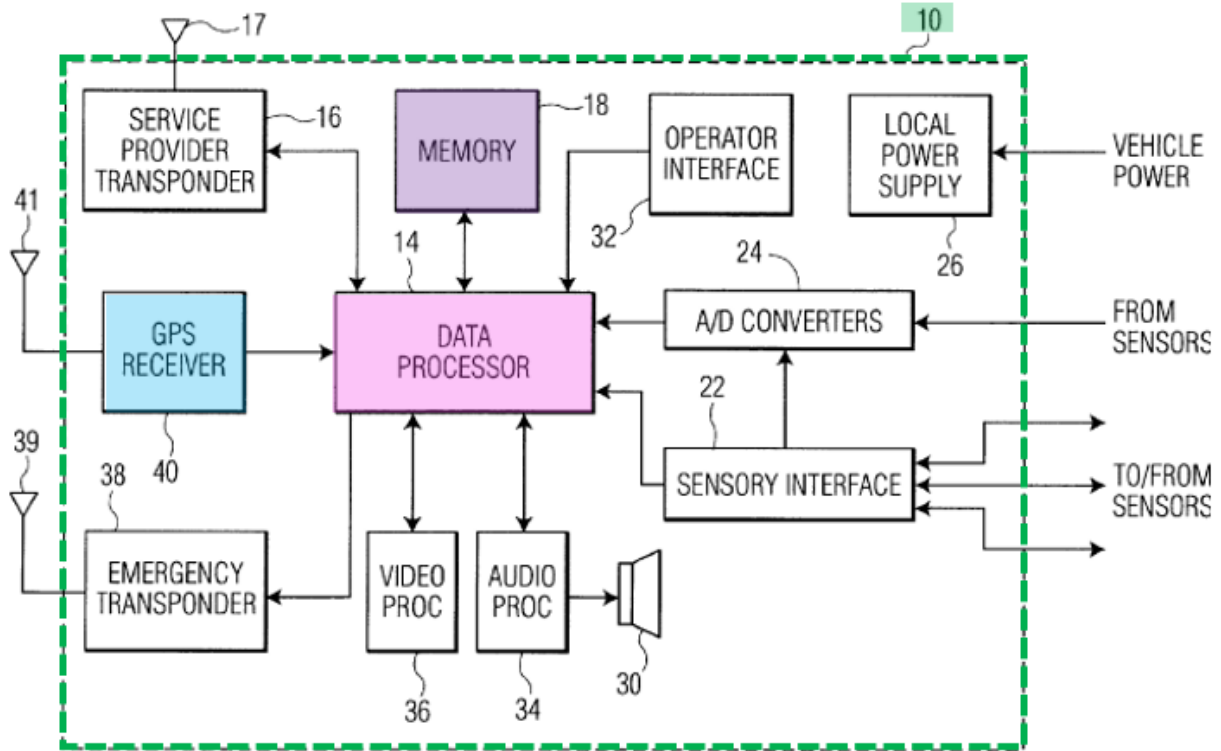


FIG. 2

Id., Fig. 2 (annotated).

[174] *Fish* also discloses that, once encrypted location data is stored on **secure memory 18**, it may be retrieved by **data processor 14**. See *id.*, 7:6-29. Indeed, retrieving this data from *Fish*'s data "archive" 10 is the purpose of the data archive 10—to allow for later access to and inspection of the stored data. *Id.*, Abstract, 1:36-45, 5:51-54, 7:12-17, 10:16-30, 11:24-26.

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.

[175] *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, as recited in claim 11. Indeed, *Fish* discloses and renders obvious each of these three types of location data.

[176] *Fish* discloses storing location information as described above in [1b]. See [1b], above. According to *Fish*, its system identifies and stores “**cartographic locations.**” *E.g.*, Ex-1004, 7:30-41 (emphasis added). In particular, *Fish* describes identifying and storing in the data archive 10 a “**cartographic location** corresponding to latitude and longitude coordinates derived from the GPS signal.” *Id.*, 7:30-41 (emphasis added), 14:23-27 (claim 21, reciting a GPS communication module “responsive to global positioning signals for identifying a **cartographic location** of the modular data archive.”). *Fish* emphasizes 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.” *Id.*, 7:42-49 (emphasis added). *Fish* distinguishes “simply [] record[ing]” latitude and longitude without translation into cartographic location in other embodiments, thereby discloses cartographic locations can be more than mere GPS coordinates. *Id.*, 7:49-51. A POSITA would have understood *Fish*’s cartographic locations to include a home address, destination addresses, or any other address, as was common at the time in commercial devices. Indeed, when a vehicle containing data archive 10 was positioned at a user’s home or a chosen destination, *Fish*’s stored cartographic or GPS data would be their home address or destination address. As a POSITA would readily have known, it would have been beyond obvious for a user to position their vehicle (including data archive 10) at their home (e.g., in their driveway or garage), at their destination (e.g., a place being driven to), or any other location.

[177] In addition, *Fish* also discloses storing velocity data, which a POSITA would understand to mean the speed and direction of motion of an object, as recited in claim 11. First, *Fish* discloses storing acceleration data which a POSITA would understand is the rate at which velocity changes over time. *Id.*, 2:58-65, 11:8-29.

[178] *Fish* also describes storing and encrypting “speed data” and multiple types of direction data, along with time, to the data archive 10:

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. . . . [sic] 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.

Id., 11:8-26 (emphases added), 2:61-65. Further, *Fish* discloses the storing of latitudinal and longitudinal information over time, which a POSITA would understand provide the direction motion of the vehicle. *Id.*, 4:8-14, 7:30-55. It would have been obvious to a POSITA that the stored speed and directional data over time constitute velocity data.

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.**

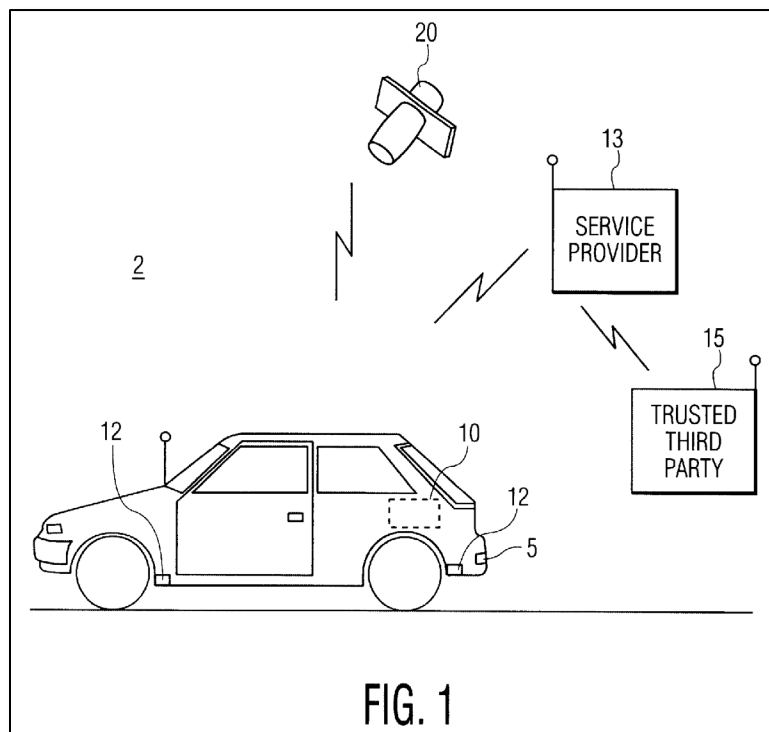
[179] *Fish* discloses the device as in claim 1, further comprising a transmission module for transmitting the encrypted location information to an external computing device, as recited in claim 12.

[180] As discussed above in § IX.A.8, a POSITA would have construed the claimed “transmission module” as a means-plus-function term. The recited

function is “transmitting the encrypted location information to an external computing device.” Claims 14 and 22 recite that the location information is transmitted “from the storage module to an external computing device.” The corresponding structure is “a transmission module or connection, e.g., hardwire or wireless, to port the information to a computer.” Ex-1001, 2:4-7; Abstract. The specification describes: “[i]f the information is stored in internal memory instead of removable memory, the transfer will be done by transmission module 112 including hardwired and/or wireless connectivity. The hardwire connection may include but is not limited to hard wire cabling e.g., parallel or serial cables, USB cable, Firewire (1394 connectivity) cables, and the appropriate port. The wireless connection will operate under any of the 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.” *Id.*, 6:26-40. *Fish* discloses and renders obvious this claimed function and associated structure.

[181] As *Fish* describes, **service provider transponder 16** is a transmission module of the data archive 10, as recited in claim 12. *Fish* explains **service**

provider transponder 16 is a “communication module” for transmitting data to the service provider, 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. *Fish* describes sending to the service provider 13 encrypted location information. *Id.*, 5:4-38 (data archive 10 sends composite encrypted sensory and location data to service provider 13), 8:41-52, 10:16-31 (service provider 13 receives encrypted data from data archive 10). The “service provider” is an external computing device, as recited in claim 12. *Id.*, 9:51-55 (service provider 13 comprises processor and memory), Figs. 1, 3. Indeed, service provider 13 is illustrated in Figure 1 as being external to data archive 10:



Id., Fig. 1.

[182] In addition, *Fish*'s "**emergency transponder 38**" is a transmission module of the data archive for sending location information to remote computing devices, as recited in claim 12. *Id.*, 8:9-40, 9:56-65.

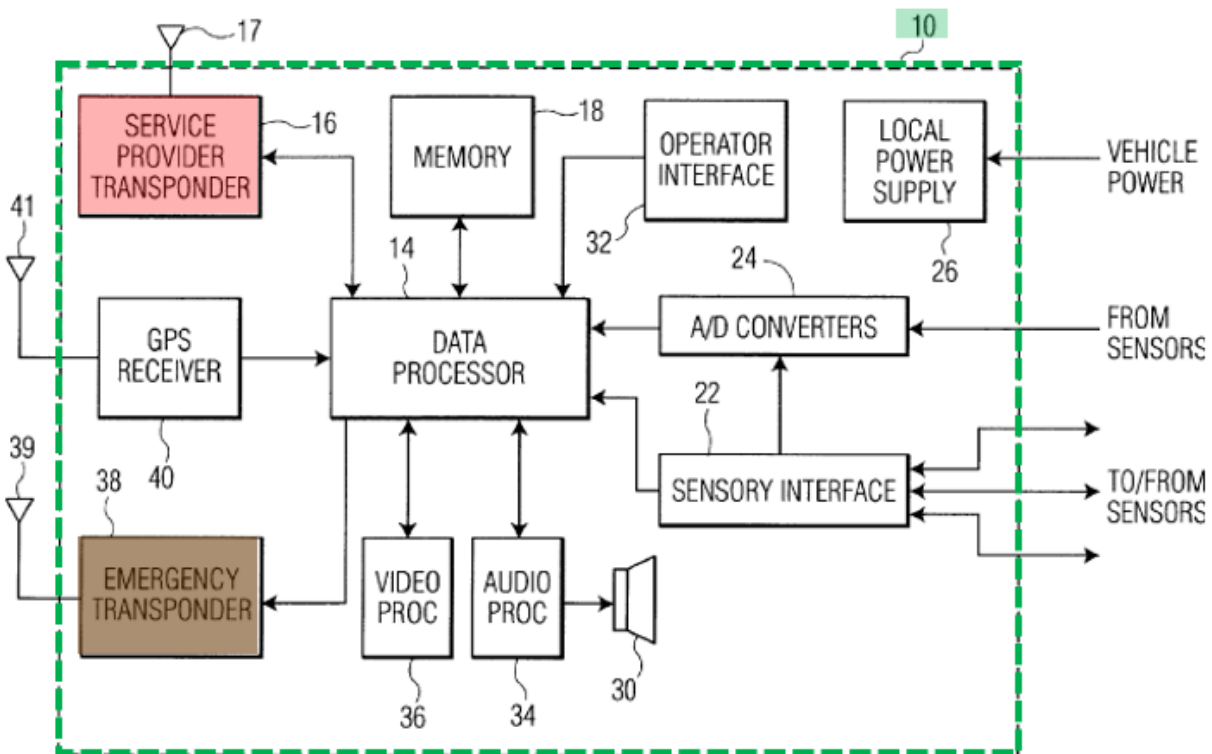


FIG. 2

Id., Fig. 2 (annotated).

D. Claim 13

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

[183] *Fish* discloses and renders obvious [13pre]. See [1pre], above.

2. **[13a] a housing;**

[184] *Fish* discloses and renders obvious [13a]. *See* [1a], above.

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;**

[185] *Fish* discloses and renders obvious [13b]. *See* [1b], above.

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

[186] *Fish* discloses and renders obvious [13c]. *See* [1c], above.

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

[187] *See* [1d], above. Unlike claim 1, claim 13 does not recite that the “storage module” is “removable.” Claim 13 is thus broader in this respect than claim 1, and therefore *Fish* teaches all of claim 13.

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.**

[188] *Fish* discloses [13e]. *See* [1e], above.

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.**

[189] *Fish* discloses claim 14. *See* claim 12, above. Unlike claim 12, claim 14 more specifically recites that the encrypted location information comes

“from the storage module.” This detail is also taught by *Fish* for the reasons discussed above regarding claim 12. Specifically, *Fish*’s encrypted location information is stored in memory 18. *See* claim [1d], above. This encrypted location information is then transmitted via *Fish*’s various transmission modules, as discussed above regarding claim 12. *See* claim 12, above.

F. Claim 19

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

[190] *Fish* discloses a system for controlling and storing location information, as recited in [19pre]. For example, data archive 10 is a system for controlling and storing location information, including GPS coordinates and identified cartographic locations. *See* [1pre], above.

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

[191] *Fish* discloses and renders obvious [19a]. *See* [1pre], above.

3. [19b] a housing;

[192] *Fish* discloses and renders obvious [19b]. *See* [1a], above.

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;

[193] *Fish* discloses and renders obvious [19c]. *See* [1b], above.

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

[194] *Fish* discloses and renders obvious [19d]. *See* [1c], above.

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

[195] *Fish* discloses and renders obvious [19e]. *See* [1d], above.

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

[196] *Fish* discloses and renders obvious [19f]. *See* [1e], above.

8. [19g] a computing device comprising:

[197] *Fish* discloses and renders obvious a computing device, as recited in [19g].

[198] *Fish* describes using “facilities” to “directly read the contents of memory.” Ex-1004, 7:6-29. A POSITA would have understood the “facilities” to be or be integrated into a computing device, as claimed. Indeed, POSITAs knew as obvious at the time that computers included ports and other components for accessing and reading memory—a core purpose of a computer. *See also id.* at 7:12-14 (“The exemplary secure memory 18 is removable to allow for easy access to the data after an accident.”). *Fish*’s disclosed computer facilities “directly read the contents of the memory.” *Id.* at 7:14-17; *see also id.* at 7:17-29.

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

[199] *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 recited in [19h].

[200] *Fish* states:

In the exemplary embodiment, the secure memory 18 is 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. The exemplary secure memory 18 is removable to allow for easy access to the data after an accident. It is contemplated, however, that a non-removable memory may be used and 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.

[201] A POSITA would have found it obvious that *Fish*'s "facilities" that "directly read the contents of memory" through a port would have been equipped to read the SD card. Standard computing devices (e.g., laptops) at the time of the '192 patent included the ability to read memory through external ports when SD cards when inserted. A POSITA would have found the inclusion of SD card reading capabilities obvious in light of this common technology and *Fish*'s goal of enabling parties (e.g., law enforcement or insurers) to identify conditions leading

up to an accident or other vehicle incident. *Id.*, 1:6-33, 2:16-24, 7:23-29, 10:22-25, 11:8-29.

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.

[202] *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 recited in [19i].

[203] *Fish* discloses decrypting stored encrypted data for analysis using shared or private keys, for example. Ex-1004, 3:50-4:7. 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 leading up to an accident. *Id.*, 1:6-33, 2:16-24, 7:23-29, 11:8-29. Indeed, this is the point of *Fish*—to make its encrypted and stored data available for later inspection. Being able to access and understand encrypted data presupposes the ability to decrypt it, as *Fish* teaches. As a POSITA would have understood, this decryption naturally and inherently requires a processor, as claimed, consistent with *Fish*'s discourse. Ex-1004, 1:6-33, 2:16-24, 3:50-4:7, 7:23-29, 11:8-29, Figs. 1-2.

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.**

[204] *Fish* discloses and renders obvious claim 20. *See* claim 11, above.

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.**

[205] *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 recited in claim 21.

[206] *Fish* discloses that the data processor 14 uses a portion of secure memory 18 with preloaded cartographic content to use in conjunction with GPS information to identify a cartographic location, i.e., a 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.

[207] It would have been obvious that a device reading *Fish*'s cartographic data would also have included preloaded cartographic maps stored in data archive 10 to facilitate *Fish*'s goals of representing and recreating vehicle travel information for later analysis. *Id.*, 1:6-33, 2:16-24, 7:23-29, 11:8-29. The utility of such maps is taught by *Fish* itself and its stated purpose of recreating and assessing vehicle movements before an accident. *Id.*; *see also id.* 3:21-27, 6:25-29, 8:2-9, 8:49-52, 10:19-25, 10:54-57. Furthermore, a POSITA would have readily known about and considered obvious such overlaying techniques, where location information is overlaid on a map. Examples of this, as discussed above, come from *Snider* in 1992 and the Acura RL in 2005, where a map is presented along with "the locality in which the vehicle is travelling" and "is displayed with the dead-reckoned position shown on the map," Ex-1017, 12:17-20, or a "Vehicle Position" icon, Ex-1019 at 18; *see also* Ex-1017, Figs. 5a-5b.

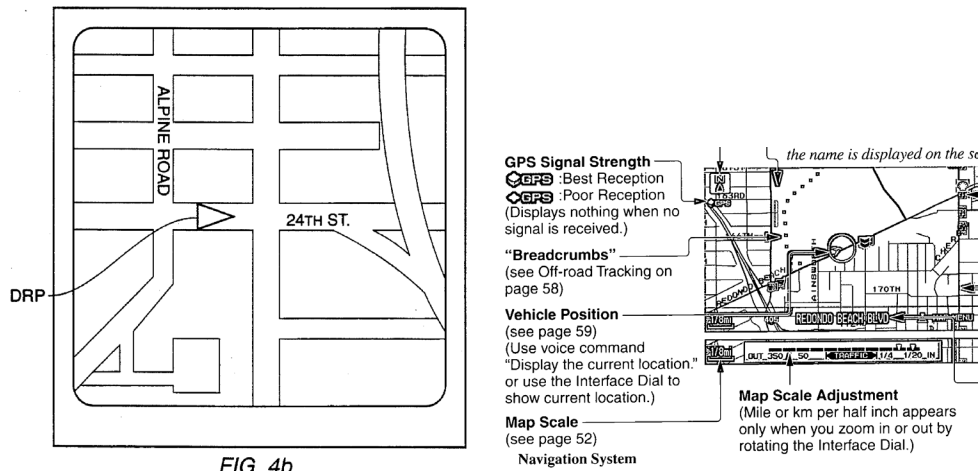


FIG. 4b

This would be obvious and conventional background information to a POSITA. As a POSITA would readily have understood, these same basic display techniques are disclosed and obvious from *Fish*'s disclosure of presenting stored map content along with position data for recreating vehicle events and motion.

I. Claim 22

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

[208] *Fish* discloses and renders obvious [22pre]. See [19pre], above.

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

[209] *Fish* discloses and renders obvious [22a]. See [1pre], above.

3. [22b] a housing;

[210] *Fish* discloses and renders obvious [22b]. See [1a], above.

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;

[211] *Fish* discloses and renders obvious [22c]. *See* [1b], above.

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

[212] *Fish* discloses and renders obvious [22d]. *See* [1c], above.

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

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

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

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

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

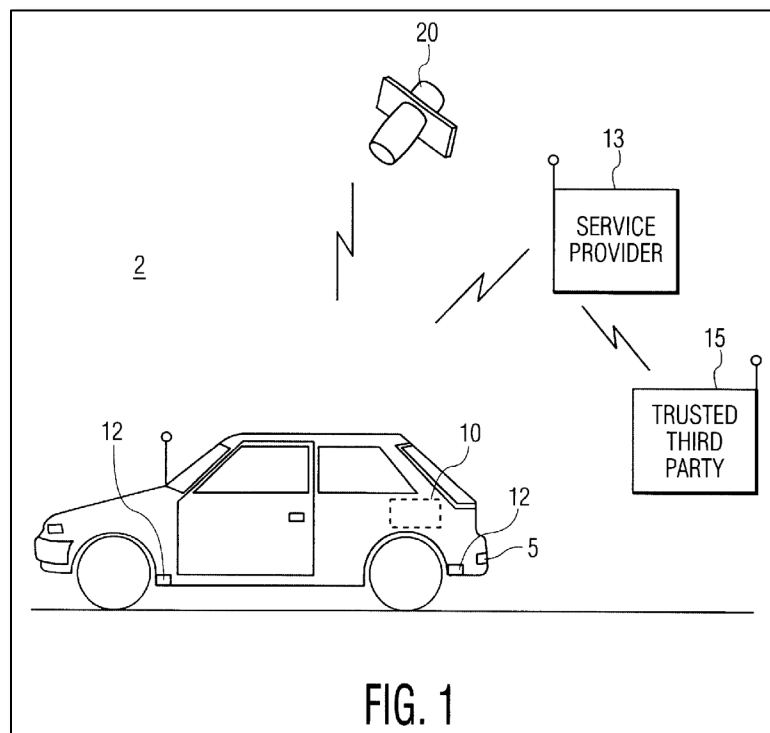
[215] *Fish* discloses and renders obvious [22g]. *See* claim 12, above.

9. [22h] the external computing device comprising: a connectivity device configured for receiving the encrypted

location information form [sic] the location information device; and

[216] *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 recited in [22h].

[217] For example, *Fish*'s "service provider" is an external computing device that includes a "data receiver," which is a "connectivity device" as claimed. Ex-1004, 9:51-55, Fig. 3. Indeed, such a connectivity device would be required for *Fish*'s external computing device to communicate with data archive 10, as disclosed. *Id.*, 4:43-65, 5:4-38 (data archive sends 10 composite encrypted sensory and location data to service provider 13), 8:41-52, 10:16-31 (service provider 13 receives encrypted data from data archive 10). The "service provider" is an external computing device, as claimed. *Id.*, 9:51-55 (service provider 13 comprises processor and memory), Figs. 1, 3. Service provider 13 is illustrated in Figure 1 as being external to data archive 10:



Id., Fig. 1.

[218] In addition, *Fish*'s "**emergency transponder 38**" is a transmission module of the data archive for sending location information to remote computing devices, as recited in claim 12. *Id.*, 8:9-40, 9:56-65. These additional external computing devices would inherently and necessarily have connectivity devices (e.g., wireless antennas and transceivers) for receiving such data from *Fish*'s data archive 10. Without such a connectivity device, they could not receive the data.

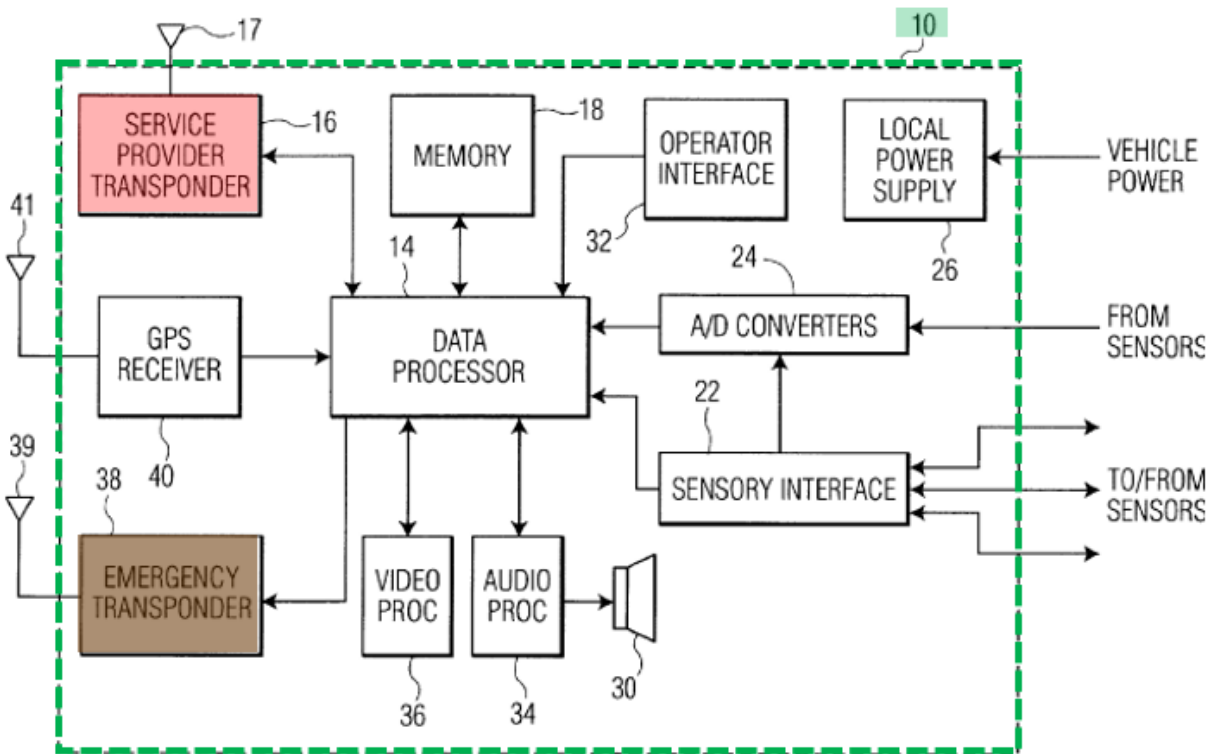


FIG. 2

Id., Fig. 2 (annotated).

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

[219] *Fish* discloses a processor configured to execute a decryption program for decrypting the encrypted location information received from the location information device, as recited in [22i].

[220] For example, *Fish*'s external computing device includes a processor, as claimed. Ex-1004, 9:51-55, Fig. 3. Data archive 10 encrypts the data according to the key received from the service provider 13, and the processor of external

service provider 13 is enabled to decrypt received encrypted data. *Id.*, 9:51-10:36, Fig. 3. As a POSITA would have immediately appreciated, if external service provider 13 received encrypted data from data archive 10, it must have a way to decrypt the data for use and analysis. Otherwise, the received encrypted data would be meaningless. It is thus disclosed, and also inherent and necessary, for *Fish*'s external service provider 13 to use a decryption program to decrypt the received encrypted location data from data archive 10.

XIII. GROUND 2: *FISH* IN VIEW OF *ZIV* (CLAIMS 2-4, 15-17)

[221] Claims 2-4 and 15-17 of the '192 patent are unpatentable as obvious in view of *Fish* and *Ziv*, alone or in view of the knowledge of a POSITA.

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

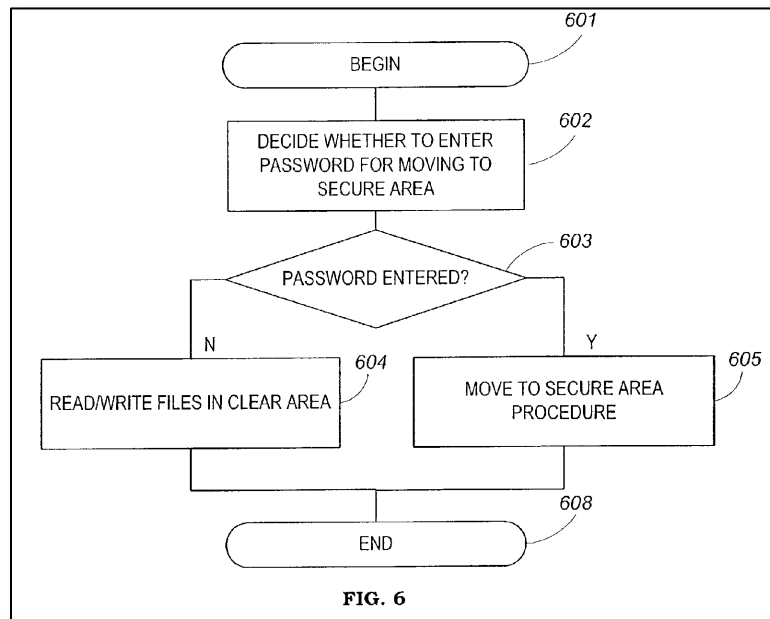
[222] In my opinion, a POSITA would have been motivated to use *Ziv*'s password protection techniques to further enhance the security techniques described in *Fish*. In particular, a POSITA would have been motivated, and found it obvious, to utilize the "password" taught in *Fish* for data deletion and other purposes as well, such as selective encryption and decryption of data as taught by *Ziv* in order to ensure that these operations were performed with proper authorization and/or authentication.

[223] Both *Ziv* and *Fish* disclose the use of removable (i.e., portable) data storage devices. Ex-1005, Abstract, ¶¶ [0001], [0025]; Ex-1004, 7:6-29. Further,

both *Ziv* and *Fish* describe techniques for ensuring data security, including through the use of encryption and a user password. Ex-1005, Abstract, ¶¶ [0026], [0031], [0033], [0037]-[0045]; Ex-1004, 3:49-4:7, 5:39-6:3. A POSITA would view both references as similar in utility, and within the same field of endeavor.

[224] To enhance security and add user-functionality, a POSITA already implementing *Fish*'s data security techniques would have found it obvious and advantageous to enhance these techniques with the additional password protection techniques disclosed in *Ziv*. The combination would also enhance flexibility and convenience by enabling different options for protecting encrypted and decrypted data.

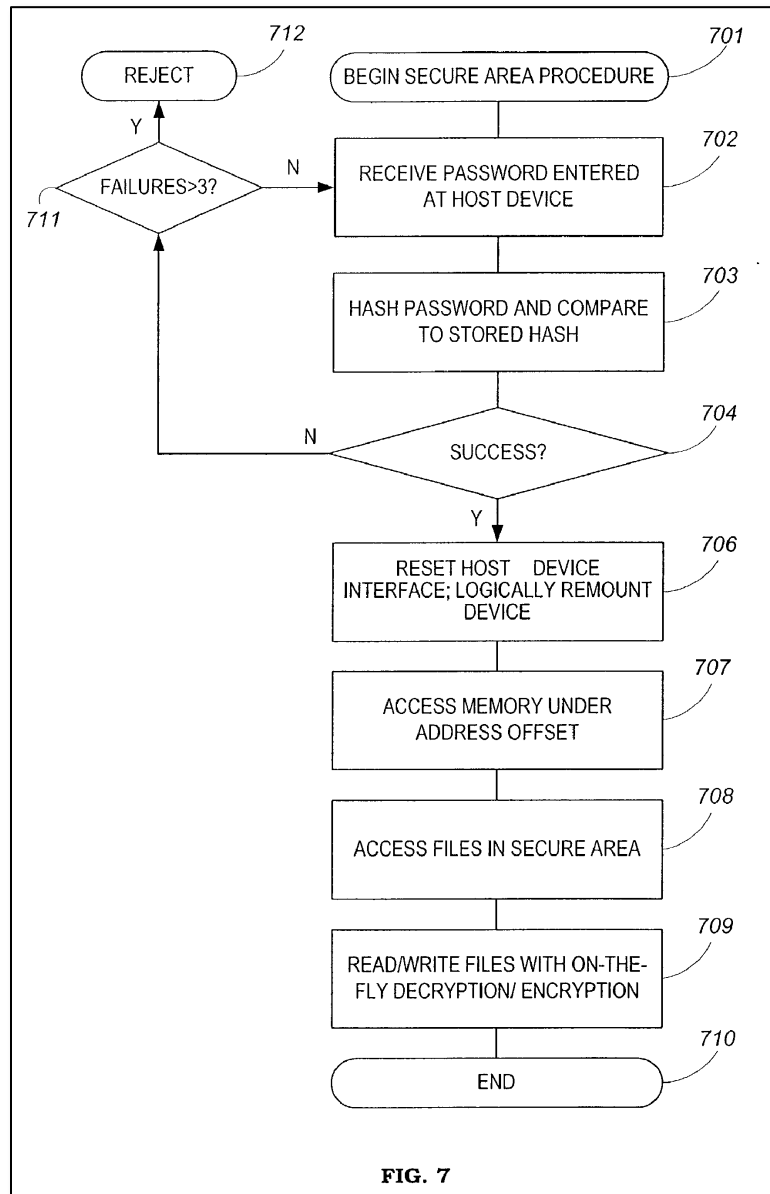
[225] Specifically, *Fish* discloses techniques where, “[t]o ensure that data is not deleted accidentally, . . . the user may be required to enter a password or personal identification number (PIN) via the operator interface 32 before being allowed to delete any data.” Ex-1004, 5:60-64. The user may thus “confirm any command to delete the data before the data is actually deleted.” *Id.*, 5:64-66. In this manner, *Fish*'s user password helps ensure the integrity and reliability of stored data. Therefore, a POSITA would have found it obvious and beneficial to combine this technique with *Ziv*'s use of a password to move data to a secure storage area. This technique in *Ziv* is shown in Figure 6:



Ziv, Fig. 6.

[226] Akin to *Fish*'s secure storage of data in its memory 18, *Ziv* discloses securely storing data in its "secure [user] area 122." Ex-1005, ¶ [0026]. Secure user area 122 stores "secure user data accessible only upon the provision of a password or biometric signature." *Id.* According to step 603 of Figure 6, a determination is made whether a user entered a valid password. *Id.*, ¶ [0037]. In particular, "if in step 603 the user has decided to work in secure user area 122 and has entered a password (or alternatively has provided his/her biometric parameters), then in step 605 he/she will move to the secure area procedure of FIG. 7." *Id.* According to Figure 7, in step 703 the user's password is hashed, *id.*, ¶ [0039], and in step 709 "all data read from or written onto memory area 410 is encrypted or decrypted on-

the-fly by microprocessor 111, as described is [sic] respect to FIGS. 8-10 below,”
id., ¶ [0040].



Id., Fig. 7.

[227] In accordance with Figure 8, the user’s password is used together with a clear key to perform encryption of stored data. *Id.*, ¶ [0043]. The user’s password

is required to retrieve the key. *Id.* Ziv's Figure 10 then "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." *Id.*, ¶ [0045].

In particular, as shown in **step 952** of Figure 10, the encrypted key is retrieved and decrypted using the user's 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.* In this way, the user's **password**—i.e., a password just as used in *Fish*—is used to selectively encrypt and **decrypt** stored data. A POSITA would have immediately and obviously seen this advantageous use of a password in view of *Fish*'s use of a password for allowing selective data deletion.

[228] Since both *Fish* and *Ziv* use similar computer hardware, a POSITA would understand that creating this combination would require nothing more than routine computer programming using algorithms and techniques that were already well-known. For these reasons, a POSITA would also have a high expectation of success in making the combination.

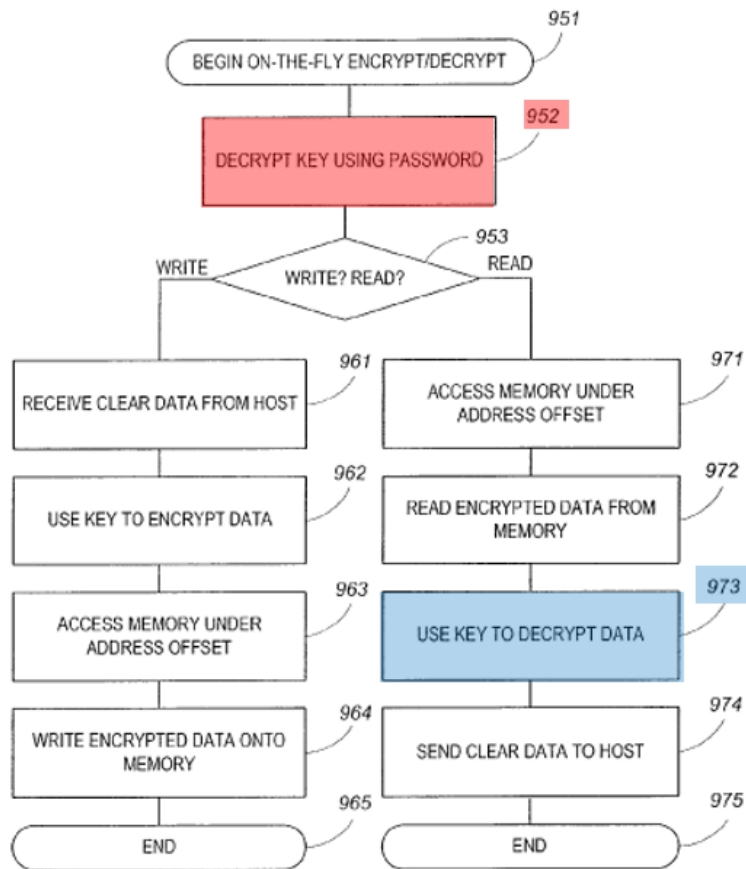


FIG. 10

Id., Fig. 10.

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.

[229] *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 recited in claim 2. *E.g.*, Ex-1004, 5:39-6:3, Fig. 2.

[230] As discussed above in § IX.A.6, the “input module” of claims 2 and 15 would be construed as a means-plus-function term. The recited function is “receiving a code string input by a user, wherein the⁵ user inputted code string is used for encrypting and decrypting the location information stored in the [] storage module.” Claim 2, unlike claim 15, is directed to encrypting and decrypting the location information stored in the removable storage module. The corresponding structure is “[i]nput 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. This function and structure are disclosed by *Fish*, as discussed below.

[231] *Fish* discloses an input module disposed on the housing configured for receiving a code string input by a user. As shown in Figure 2, **data archive 10** includes **operator interface 32**, which is an “input module,” as claimed. Ex-1004, 5:39-6:3, Fig. 2.

⁵ Claim 15 mistakenly recites “he” instead of “the.”

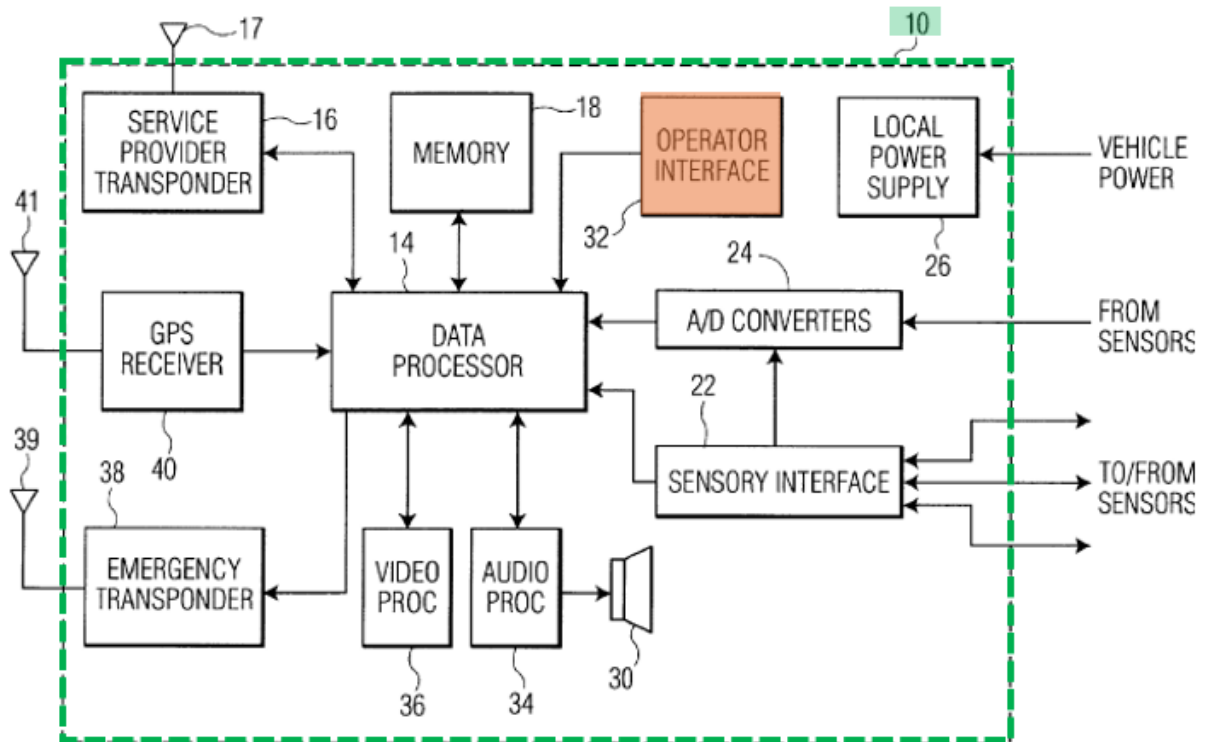
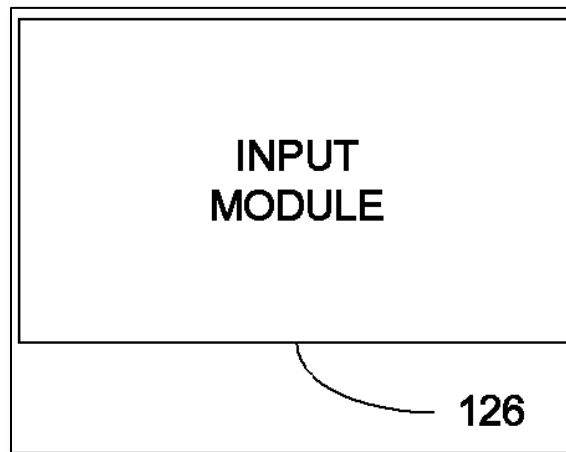


FIG. 2

Id., Fig. 2 (annotated)

[232] As discussed above, *Fish* discloses “[t]he data archive 10 of the exemplary embodiment is preferably housed in a sealed cabinet (not shown).” *Id.*, 3:2-3. *Fish* explains this housing “is desirably fire and water resistant and designed to offer significant resistance to crush forces typically encountered in catastrophic vehicle wrecks.” *Id.*, 3:6-8. Accordingly, a POSITA would have understood that *Fish* discloses that its **operator interface 32** is disposed “on the housing” in the same manner as the ’192 patent itself. The ’192 patent merely discloses that its various components are somehow “disposed in a generally rectangular housing

102,” without specifics. Ex-1001, 3:7-9, Fig. 2 (element 126). The ’192 patent’s generic input module 126 is shown below. Similarly, input module 106 of Figure 1 is generically described as having buttons, but is assigned no specific structural requirements. *Id.*, 3:14-16.



Id., Fig. 2.

[233] In like manner, *Fish* describes that its **operator interface 32** also has buttons. *See* Ex-1004, 5:46-51 (“the controls 32 are **push-button switches**, however those skilled in the art will recognize that the function of controls 32 can be performed by any number of switching technologies including a wireless communication device (not shown).”) (emphasis added). *Fish* further discloses, just like the ’192 patent but with even more detail, that the 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.” *Id.*, 5:51-54 (emphasis added).

[234] *Fish* explains **data archive 10** receives “control parameters from **operator interface 32**” to delete or deactivate data. *Id.*, 5:39-54. The **operator interface 32** “provide[s] an operator means for adjusting/controlling the operation of **data archive 10**” and further allows a “driver or owner [to] control how and when the [stored] data is used.” *Id.*, 5:39-60. *Fish* specifies these “controls may be physically located on the **data archive 10**,” i.e., disposed on the housing of the location information device, as claimed. *Id.*

[235] To control data deletion, *Fish* discloses “the user may be required to enter a password or personal identification number (PIN) via the **operator interface 32**.” *Id.*, 5:55-6:3. A POSITA would understand a password or PIN is a code string input by the user, as recited in claim 2. Indeed, the ’192 patent describes its “code string” generically as any code string a user may wish to use. *See* Ex-1001, 5:4-9 (“Upon initialization of device 100, processing module 120 and, upon verification of the identity of a user, the linked code prompts the user via display module 104 or speaker 116 to select a code string that the user wishes to use. The user selects an appropriate code string and enters the code string into the device 100 with input module 126 via buttons 108, microphone 114 or touch screen.”).

[236] As discussed above in § XIII.A, a POSITA would have found it obvious to use *Fish*’s password for other data security purposes—namely,

controlling encryption and decryption of stored data. *Ziv*'s portable storage device 110, like *Fish*'s data archive 10, may include a user interface for receiving a password. In particular, *Ziv* discloses a user entering a password using an interface such as a screen. Ex-1005, ¶ [0031]. Consistent with the above discussion, *Fish* in view of *Ziv* teaches that the password (i.e., the “user inputted code string” of claim 2) is used for encrypting and decrypting the location information stored in the removable storage module. For this purpose, *Ziv*'s techniques of selective encryption and decryption of stored data (e.g., *Fish*'s stored location information) may be performed.

[237] In particular, as discussed above in § XIII.A, *Fish*'s secure storage of data in its memory 18 is similar to how *Ziv* discloses securely storing data in its “secure [user] area 122.” Ex-1005, ¶ [0026]. In secure user area 122 is stored “secure user data accessible only upon the provision of a password or biometric signature.” *Id.* In *Ziv*'s step 603 of Figure 6, a determination is made whether a user entered a valid password. *Id.*, ¶ [0037]. In particular, “if in step 603 the user has decided to work in secure user area 122 and has entered a password (or alternatively has provided his/her biometric parameters), then in step 605 he/she will move to the secure area procedure of FIG. 7.” *Id.* According to Figure 7, in step 703, the user's password is hashed, *id.*, ¶ [0039], and in step 709 “all data read

from or written onto memory area 410 is encrypted or decrypted on-the-fly by microprocessor 111, as described is respect to FIGS. 8-10 below,” *id.*, ¶ [0040].

[238] Following *Ziv*’s Figure 8, the user’s password is used together with a clear key to perform encryption of stored data. *Id.*, ¶ [0043]. The user’s password is required to retrieve the key. *Id.* *Ziv*’s Figure 10 then “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.” *Id.*, ¶ [0045]. In particular, as shown in step 952 of Figure 10, the encrypted key is retrieved and decrypted using the user’s 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.* In this way, the user’s password—i.e., a password just as used in *Fish*—is able to selectively encrypt and decrypt stored data. For the reasons discussed above, a POSITA would have immediately and obviously seen this advantageous use of a password in view of *Fish*’s use of a password for allowing selective data deletion.

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.**

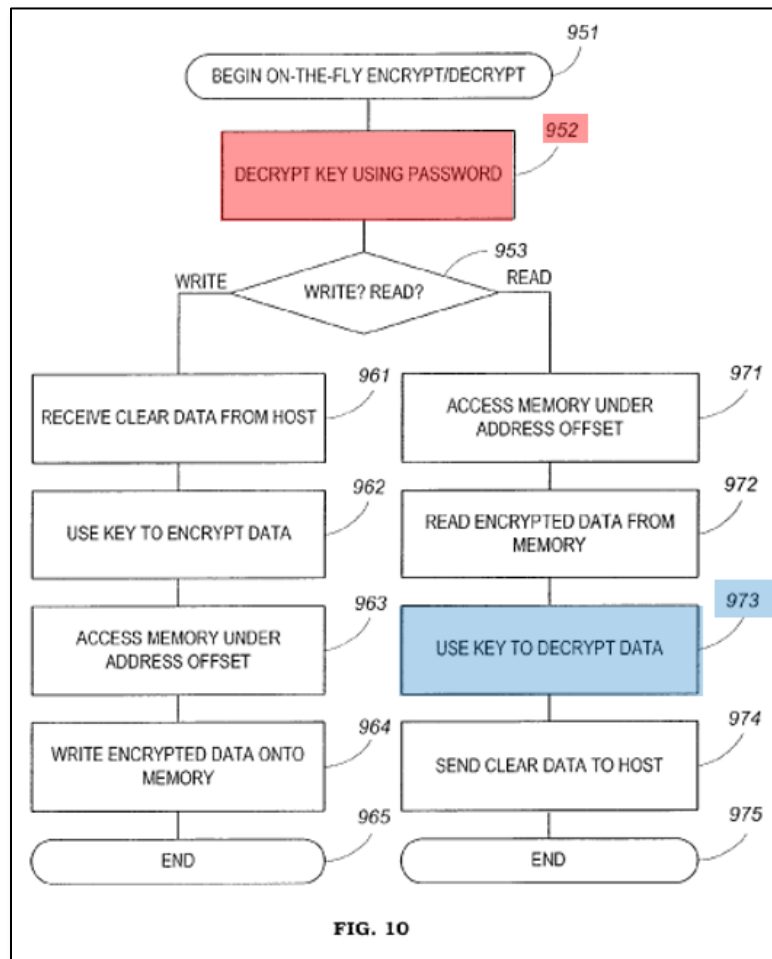
[239] *Fish* in view of *Ziv* discloses and renders obvious the device as in claim 1, further comprising a user verification module for verifying the identity of user of the device, wherein the processing module selectively decrypts the location information stored in the removable storage module based on the identity of the user, as recited in claim 3.

[240] As discussed above in § IX.A.7, a POSITA would have construed the claimed “user verification module” as a means-plus-function term. The recited function in claims 3 and 16 is verifying the identity of user of the device, and the corresponding structure is a “user verification module 130” that “will indicate and verify the identity of the user of the device 100.” Ex-1001, 5:49-51. “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.” *Id.*, 5:51-54. If the user verification module includes an identity capture device, such 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." *Id.*, 5:54-59. *Fish* in view of *Ziv* discloses this function and structure multiple ways.

[241] For example, as discussed above in relation to claim 2, operator interface 32 of *Fish* enables a user to input a password or PIN. *See* Ex-1004, 5:55-6:3 ("the user may be required to enter a password or personal identification number (PIN) via the operator interface 32."). A password or PIN is information that verifies the identity of a user, as required in claim 3. For the reasons discussed above regarding claim 2, *Fish* in view of *Ziv* teaches using this password to selectively encrypt or decrypt data, such as *Fish*'s stored location data.

[242] This selective decryption based on a user's password is taught by *Ziv*'s Figure 8, where the user's password is used together with a clear key to perform encryption of stored data. Ex-1005, ¶ [0043]. The user's password is required to retrieve the key. *Id.* *Ziv*'s Figure 10 then "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." *Id.*, ¶ [0045].



Id., Fig. 10.

[243] In particular, as shown in **step 952** of Figure 10, the encrypted key is retrieved and decrypted using the user's 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.* In this way, the user's **password**—i.e., a password just as used in *Fish*—is used to selectively encrypt and **decrypt** stored data. The combination of *Fish* and *Ziv*, as discussed above in § XIII.A, would allow for this selective decryption to decrypt stored location data

as taught in *Fish*. For the reasons discussed above, a POSITA would have appreciated as obvious this advantageous use of a password in view of *Fish*'s use of a password for allowing selective data deletion.

[244] *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.” *Id.*, ¶ [0006]. As *Ziv* explains, a user may provide “a password or biometric signature.” *Id.*, ¶ [0026]. In that technique, the user verification module of *Ziv* is “a biometric reader such as a fingerprint reader.” *Id.*, ¶ [0031]. *Ziv* then teaches using the biometric parameters as an alternative to a password—i.e., for selectively encrypting and decrypting stored data as discussed above regarding claim 2. *See also id.*, ¶¶ [0033], [0037]-[0038]. 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. A POSITA would have been motivated to use *Ziv*'s password techniques for selective encryption and decryption of *Fish*'s stored location data for all of the reasons discussed above. In addition, using *Ziv*'s biometric-based techniques for selective encryption and decryption of *Fish*'s stored location data would have been attractive, advantageous, and obvious to a POSITA for other reasons. For example, by accepting biometric input (e.g., a fingerprint or retina scan) instead of a

password, the need for a user to manually type password characters would be avoided. This would be especially advantageous in an automobile such as *Fish* discloses, where a user is typically not presented with a full QWERTY keyboard such as they would have at a personal computer. Further, using a biometric identifier as opposed to a password, as *Ziv* teaches, would add heightened security to *Fish* because it is harder to “steal” or improperly replicate a user’s biometric details than their password—while a password may be written down and copied, a fingerprint or retinal scan cannot. Further, while a password may be forgotten by a user, their fingerprint or retina cannot, and thus would be more user-friendly. For all of these reasons, a POSITA would have immediately and obviously found it beneficial to use *Ziv*’s techniques of biometric-based selective encryption and decryption of *Fish*’s stored location data.

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.**

[245] *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 recited in claim 3.

[246] First, *Fish* discloses “the user may be required to enter a password or personal identification number (PIN) via the operator interface 32.” Ex-1004,

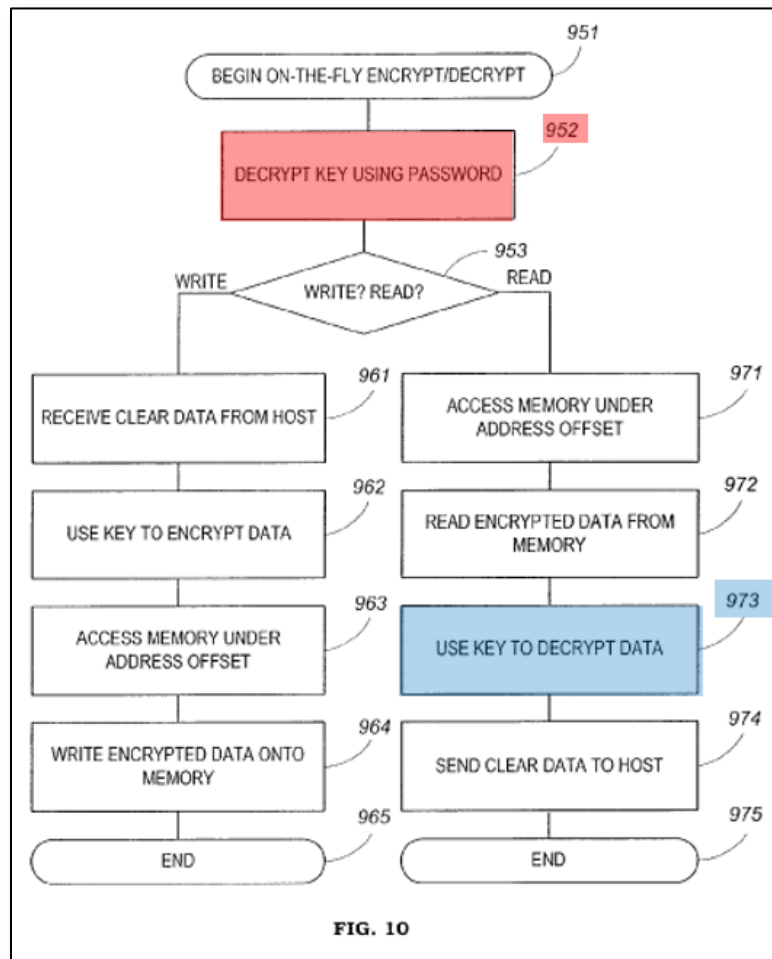
5:55-6:3. Password-based authentication is a password protection algorithm for verifying user identity, as claimed, as discussed above in connection with claims 2 and 3. Indeed, verifying a user's password or PIN to verify the user's identity is the same technique disclosed in the '192 patent itself. *See* Ex-1001, 5:49-54 ("The user verification module 130 will indicate and verify the identity of the user of the device 100. 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.").

[247] As a POSITA would have understood, *Fish*'s disclosure of verifying a password involves executing a password protection algorithm, as claimed in claim 4. The '192 patent assigns no specific requirements to the claimed algorithm, only requiring that it somehow verify the password itself. *See id.*, 5:48-6:7.

[248] 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 as recited in claim 4. *Fish* in view of *Ziv* teaches this at least two ways, as discussed above regarding claims 2 and 3. In particular, *Fish* in view of *Ziv* teaches using *Ziv*'s password verification techniques to identify a user and selectively decrypt data. Further, *Fish* in view of *Ziv* also teaches using *Ziv*'s biometric verification techniques to identify a user and selectively decrypt data. A POSITA would have been motivated to use *Ziv*'s

password protection related techniques to further enhance the password protection and encryption techniques described in *Fish* for the reasons described in connection with claims 2 and 3, including enhanced data security and better user-friendliness.

[249] *Ziv*'s password-based techniques are described in Figure 8, where the user's password is used together with a clear key to perform encryption of stored data. Ex-1005, ¶ [0043]. The user's password is required to retrieve the key. *Id.* *Ziv*'s Figure 10 then "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." *Id.*, ¶ [0045].



Ex-1005, Fig. 10 (annotated).

[250] As shown in **step 952** of Figure 10, the encrypted key is retrieved and decrypted using the user's 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.* In this way, the user's **password**—i.e., a password just as used in *Fish*—is used to selectively encrypt and **decrypt** stored data. The combination of *Fish* and *Ziv*, as discussed above, would allow for this selective decryption to decrypt stored location data as taught in *Fish*.

For the reasons discussed above, a POSITA would have appreciated as obvious this advantageous use of a password in view of *Fish*'s use of a password for allowing selective data deletion.

[251] *Ziv* further discloses alternatives to passwords, such as “biometric identification data.” *Id.*, ¶ [0006]. A user may provide “a clear, un-hashed password or biometric signature.” *Id.*, ¶ [0026]. For this, *Ziv* teaches using “a biometric reader such as a fingerprint reader.” *Id.*, ¶ [0031]. *Ziv* also teaches using biometric parameters as an alternative to a password for verifying a user's identity. *See also id.*, ¶¶ [0033], [0037]-[0038]. A POSITA would have been motivated to use *Ziv*'s password techniques for verifying a user's identity for all of the reasons discussed above. In addition, using *Ziv*'s biometric-based techniques for user verification would have been attractive, advantageous, and obvious to a POSITA for other reasons. For example, by accepting biometric input (e.g., a fingerprint or retina scan) instead of a password, the need for a user to manually type password characters would be avoided. This would be especially advantageous in an automobile such as *Fish* discloses, where a user is typically not presented with a full QWERTY keyboard such as they would have at a personal computer. Further, using a biometric identifier as opposed to a password, as *Ziv* teaches, would add heightened security to *Fish* because it is harder to “steal” or improperly replicate a user's biometric details than their password—while a password may be written

down and copied, a fingerprint or retinal scan cannot. Further, while a password may be forgotten by a user, their fingerprint or retina cannot, and thus would be more user-friendly. For all of these reasons, a POSITA would have immediately and obviously found it beneficial to use *Ziv*'s techniques of biometric-based user verification.

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.**

[252] *Fish* discloses and renders obvious claim 15. *See* claim 2, above.

Unlike claim 2, claim 15 does not recite that its storage module is “removable.”

Claim 15 is thus broader than claim 2, and is therefore fully disclosed by *Fish* for the reasons explained above regarding claim 2.

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.**

[253] *Fish* discloses and renders obvious claim 16. *See* claim 3, above.

Unlike claim 3, claim 16 does not recite that its storage module is “removable.”

Claim 16 is thus broader than claim 3, and is therefore fully disclosed by *Fish* for the reasons explained above regarding claim 3.

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.**

[254] *Fish* discloses and renders obvious claim 17. *See* claim 4, above.

XIV. GROUND 3: *FISH* IN VIEW OF *ZIV* AND *GEHLOT* (CLAIMS 5-8, 18)

[255] Claims 5-8 and 18 of the '192 patent are unpatentable as obvious in view of *Fish*, *Ziv*, and *Gehlot*, alone or in view of the knowledge of a POSITA.

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

[256] In my opinion, 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.

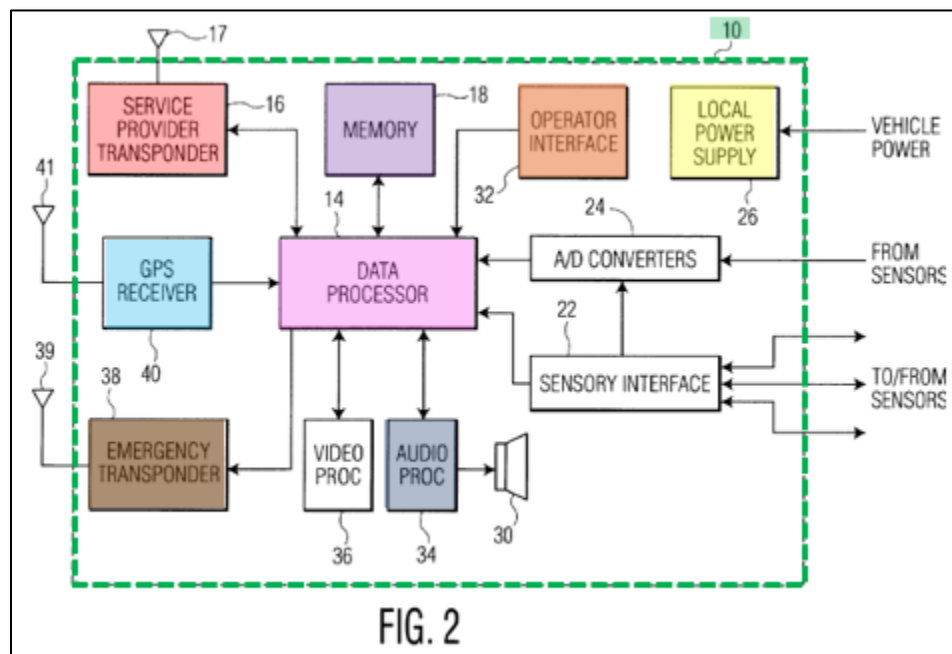
[257] Fundamentally, a POSITA would have recognized that *Fish* and *Gehlot* have very similar purposes and techniques. For example, *Gehlot* discloses use of a vehicle-based processing unit 3 to capture various types of vehicle data from vehicle electronic components, including a GPS module 14. Ex-1006, 2:14-16, 3:43-55, 4:37-47, 6:51-58, Figs. 1 & 4. This collected data may be stored at the vehicle (e.g., in storage device 7) and/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). *Id.*, 4:48-52, 4:64-5:25, Figs. 1 & 4. Similarly, *Fish* discloses use of a 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. *Fish*'s data archive 10 likewise gathers data from a variety of vehicle-based electronic units, including GPS receiver 40. *Id.*, 4:22-29, 5:16-26, 5:39-44, Figs. 1 & 2. This data may be stored locally (e.g., in memory 18) and/or transmitted to external entities (e.g., service provider 13 or trusted third party 15). *Id.*, 7:6-41, 3:10-27, 4:43-65, Figs. 1 & 2. Accordingly, a POSITA would have immediately and obviously recognized that *Fish* and *Gehlot* are in the same field of endeavor and relate to very similar techniques. For all of these reasons, a POSITA would also have recognized that the combination of *Fish* and *Ziv*, as discussed above, would also be in the same field of endeavor as *Gehlot*.

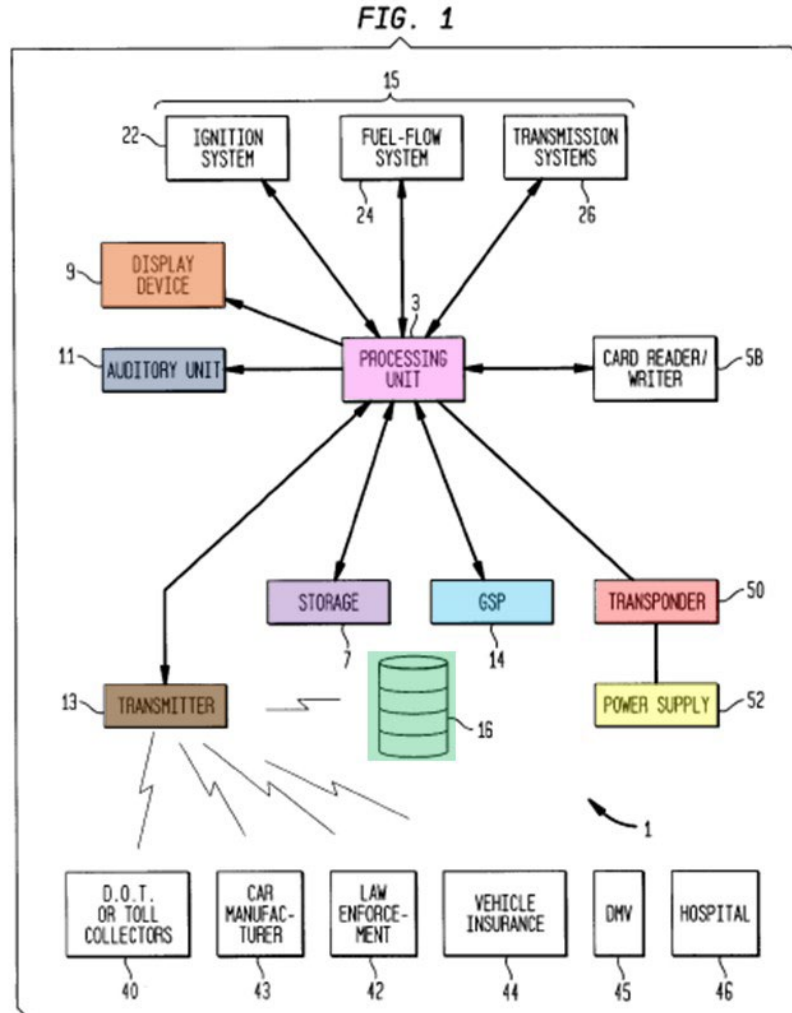
[258] A POSITA in possession of *Fish* and *Ziv* would have looked to *Gehlot* for its additional known techniques to enhance security and privacy of data on *Fish*'s data archive 10. *Fish* and *Gehlot* are both directed to securely storing vehicle data during operation, including location information. *E.g.*, 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. *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. Both references describe the goal of assisting third parties, such as law enforcement and insurers following

driving incidents or vehicle 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.

[259] Further, both *Fish* and *Gehlot* disclose the same basic hardware systems, and a POSITA would have been familiar with the system disclosed in *Gehlot* and related software designs which were common by the time *Fish* was invented. For instance, both contain a **data processor**, **memory**, a **transponder**, an **emergency transmitter** and a **GPS**.



Ex-1004, Fig. 2 (annotated).

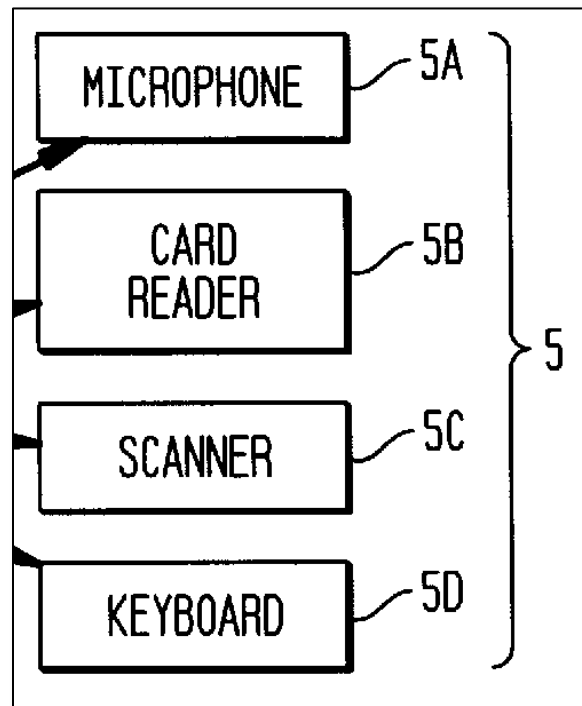


Ex-1006, Fig. 1 (annotated).

[260] Both 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). A POSITA would have understood the routine engineering

modifications necessary to implement the changes in software and hardware between *Fish* and *Gehlot*.

[261] Further, 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. In particular, *Gehlot* discloses 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. The 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." *Id.*, 3:6-12.



Id. Fig. 4.

[262] A POSITA would have found it obvious to implement *Gehlot*'s biometric user identification components and/or methods in the combination of *Fish* and *Ziv*. The combination would have enhanced flexibility and convenience by enabling different options for accessing encrypted data. The combination would have been nothing more than the simple substitution of *Gehlot*'s known method—biometric authentication—for predictable results—enhanced security—in *Fish* and *Ziv*'s system. 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.”).

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.**

[263] *Fish* in view of *Ziv* and *Gehlot* 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 recited in claim 5.

[264] In the '192 patent, 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. These are described as conventional components, with no unique requirements. As discussed above in § VI, "identity verification devices [were] common and [were] currently widely in use." *Id.*, 5:62-64.

[265] *Gehlot* discloses securely storing 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). *Gehlot* explains that its Vehicle Data System (VDS), which includes a Vehicle Data Processor (VDP), may

include a GPS system for tracking the vehicle so location information can be shared. *Id.*, 2:1-16.

[266] *Gehlot* discloses biometric access to its VDS 1. “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.” *Id.*, 2:17-21. *Gehlot* matches this information with stored data and uses it to grant authorization to the user. *Id.*, 2:21-23. As a POSITA would have obviously and readily understood, such user identification techniques involve comparing received data (e.g., a scanned image of a retina) with stored data associated with the user (e.g., a stored image of the user’s retina). A match would signify successful identification of the user. Indeed, this is the same meaning of user identification described in the ’192 patent itself. Ex-1001, 5:54-59.

[267] A POSITA would have been motivated to use *Gehlot*’s biometric authentication methods to identify users for restricting access to encrypted data on *Fish*’s data archive 10. A POSITA in possession of *Fish* and *Ziv* would have looked to *Gehlot* for the reasons described above. Namely, while *Ziv* discloses the use of biometric techniques to verify a user’s identity, *Gehlot* further discloses components and implementation examples for such biometric identification

devices. A POSITA would have been motivated to implement the biometric identification techniques of *Fish* and *Ziv* in accordance with *Gehlot*'s more specific components, techniques, and user prompts for biometric identification. This would provide additional security to the *Fish-Ziv* system and also provide a POSITA with more implementation guidance, predictability, and detail.

C. Claim 6

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

[268] *Fish* in view of *Ziv* and *Gehlot* discloses and renders obvious the device as in claim 5, wherein the identity capture device is a biometric device, as recited in claim 6. As discussed in relation to claim 5, a POSITA would have been motivated to implement *Gehlot*'s biometric authentication components and techniques in the system of *Fish* and *Ziv*. In such a system, as discussed above regarding claim 5, *Gehlot*'s more specific biometric components and techniques would accomplish the biometric-based security techniques of *Fish* and *Ziv*.

D. Claim 7

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

[269] *Fish* in view of *Ziv* and *Gehlot* discloses and renders obvious the device as in claim 5, wherein the identity capture device is a retinal scanning device, as recited in claim 7. As discussed in relation to claim 5, a POSITA would

have been motivated to implement *Gehl*'s biometric authentication, including retinal scanning methods. *See* Ex-1006, 2:16-20 ("In a preferred embodiment, 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." (emphasis added)), 3:6-12 ("With reference to FIGS. 1 to 4, the present invention, the vehicle data system ('VDS') 1, comprises 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**." (emphasis added)), 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**." (emphases added)), 6:28-33 ("Of course, the processing 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." (emphasis added)).

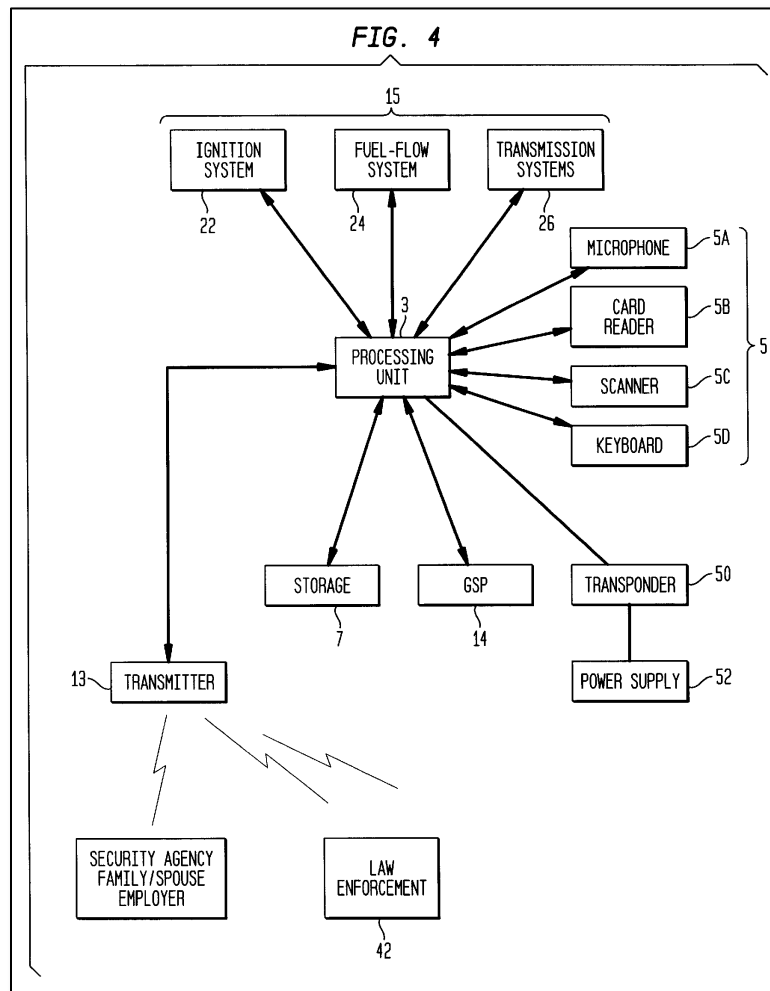
Indeed, a POSITA would have recognized it as obvious and advantageous that a retinal scan cannot easily be forged by a malicious actor, cannot easily be

recreated, cannot be written down, cannot be forgotten, is quick for a user to provide, and would be user-friendly to provide (i.e., without use of a full QWERTY keyboard in the confined space of an automobile).

E. Claim 8

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

[270] *Fish* in view of *Ziv* and *Gehlot* renders obvious the device as in claim 5, wherein the identity capture device is a fingerprint reader, as recited in claim 8. *Ziv* specifically teaches using “a **fingerprint reader**” for purposes of verifying a user’s identity. Ex-1005, ¶ 31. As discussed in relation to claim 5, a POSITA would have been motivated based on this teaching to implement *Gehlot*’s more specific and complete biometric authentication, including fingerprint and other verification methods together with user prompts. *See* Ex-1006, 2:16-20 (“In a preferred embodiment, 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.” (emphasis added)); claims 28-29. A POSITA would have been motivated to implement the “fingerprint reader” described by *Ziv* in the more specific structure of *Gehlot*, including *Gehlot*’s scanner 5C, shown below. Ex-1006, 3:10-12, 6:28-33.



Ex-1006, Fig. 4.

[271] Indeed, a POSITA would have recognized it as obvious and advantageous that a fingerprint scan cannot easily be forged by a malicious actor, cannot easily be recreated, cannot be written down, cannot be forgotten, is quick for a user to provide, and would be user-friendly to provide (i.e., without use of a full QWERTY keyboard in the limited spatial area of an automobile). Further, it would have been desirable to provide a user with more than one user verification

technique for purposes of flexibility, user-friendliness, and adaptability (e.g., in case one verification technique was not possible or convenient for a user).

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.**

[272] *Fish* in view of *Ziv* and *Gehlot*, alone or with the knowledge of a POSITA, discloses and renders obvious claim 18. *See* claim 5, above.

XV. GROUND 4: *FISH*, *ZIV*, *GEHLOT*, AND *STEVENSON* (CLAIMS 9-10)

[273] Claims 9-10 of the '192 patent are unpatentable as obvious in view of *Fish*, *Ziv*, *Gehlot*, and *Stevenson*, alone or in view of the knowledge of a POSITA.

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

[274] A POSITA in possession of *Fish*, *Ziv*, and *Gehlot* would have looked to *Stevenson* for its additional known techniques to enhance data security and user-access related to secure access to *Fish*'s data archive 10.

[275] 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]. A POSITA would have immediately and obviously recognized that *Stevenson* is in the same field of endeavor as *Fish*, as well as *Fish* as combined with *Ziv* and *Gehlot*. In particular,

like *Fish, Stevenson* relates to a vehicle-based control system 10. Ex-1007, Abstract, ¶¶ [0010], [0011], [0016], Fig. 1. Further, like *Fish, Stevenson* discloses techniques for user authentication or authorization. *Id.*, Abstract, ¶¶ [0005], [0006], [0008], [0010], [0012]-[0020], Fig. 1.

[276] A POSITA would have been motivated to combine *Fish-Ziv-Gehlot* with *Stevenson* because both *Gehlot* and *Stevenson* disclose the use of 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 **further** types of such user verification (e.g., **facial recognition** and **DNA recognition**), Ex-1007, Abstract, ¶¶ [0005], [0007], [0010], [0020].

[277] To further enhance security and provide greater user flexibility, a POSITA already implementing *Gehlot*'s biometric techniques in *Fish-Ziv*'s system (for the reasons described in § XIII.A above) would have found it further obvious and advantageous to utilize *Stevenson*'s biometric methods of **facial recognition** and **DNA detection**. In particular, *Stevenson*'s techniques would be used instead of, or in addition to, those of *Gehlot*. The combination would also enhance flexibility, simplify the user experience, and offer convenience by enabling different options for accessing encrypted data. For example, in some use cases, *Stevenson*'s facial recognition may be deemed easier to implement or more suitable

than *Gehlot*'s other biometric techniques. Similarly, *Stevenson*'s DNA-based techniques may also be deemed more convenient or secure than those in *Gehlot* (e.g., if the user was wearing sunglasses, had eye damage, had fingerprint damage, etc.). The combination would have been nothing more than the simple substitution of *Stevenson*'s known method (facial or DNA authentication) for predictable results (enhanced security and flexibility) in *Fish*'s system.

B. Claim 9

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

[278] *Fish-Ziv* in view of *Gehlot*, and further in view of *Stevenson*, renders obvious the device as in claim 5, wherein the identity capture device is a facial recognition reader, as recited in claim 9. As discussed in relation to claim 5, a POSITA would have been motivated to implement *Gehlot*'s biometric authentication techniques in combination with *Fish-Ziv-Gehlot*'s system.

[279] *Stevenson* further discloses facial recognition-based biometric authentication for vehicle entry and exit systems for restricted areas. Ex-1007, Abstract. *Stevenson* discloses its biometric based authentication methods could include **facial recognition**, iris recognition, palm prints, fingerprints, or "means for examining the DNA of a driver, such as from a sample of saliva." *Id.*, Abstract, ¶¶ [0007], [0018]-[0020]. For its facial recognition system, *Stevenson* describes

positioning a camera to recognize a user face and comparing camera images to stored images of a driver to authenticate the driver and allow the vehicle to enter a restricted area. *Id.*, Abstract, ¶ [0007].

[280] A POSITA would have been motivated to combine *Fish*, *Gehlot*, and *Stevenson* for the reasons described in § XV.A.

C. Claim 10

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

[281] *Fish* in view of *Ziv* and *Gehlot*, and further in view of *Stevenson*, discloses and renders obvious the device as in claim 5, wherein the identity capture device is a DNA detection device, as recited in claim 10.

[282] As discussed in relation to claim 9, a POSITA would have been motivated to implement *Stevenson*'s biometric authentication methods in *Fish-Ziv*'s system as modified by *Gehlot*. *Stevenson* discloses implementing **DNA**-based authentication methods for drivers as one approach to biometric authentication. Ex-1007, ¶¶ [0007], [0020]. 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. This disclosure of **DNA** verification in *Stevenson* is comparable, and indeed greater, than the '192 patent's own disclosure. *See*

Ex-1001, 5:64-66 (referencing “DNA detection” as an example of an identity verification device “not yet in use”).

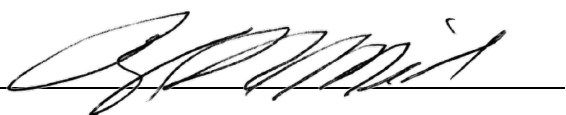
XVI. CONCLUSION

[283] For the reasons set forth above, in my opinion, a person of ordinary skill in the art would have found claims 1-22 of the '192 patent obvious.

[284] In signing this declaration, I understand that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

[285] I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: April 24, 2025

By: 
William R. Michalson, Ph.D.