

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD., and
SAMSUNG ELECTRONICS, AMERICA, INC.,

Petitioners

v.

FENDGO, LLC,

Patent Owner

Case IPR2024-00113

U.S. Patent No. 11,265,404

**DECLARATION OF WILLIAM R. MICHALSON, PH.D. IN SUPPORT
OF PETITION FOR INTER PARTES REVIEW
OF U.S. PATENT NO. 11,265,404**

TABLE OF CONTENTS

	<u>Page</u>
I. ASSIGNMENT	1
II. QUALIFICATIONS.....	1
III. SUMMARY OF CONCLUSIONS FORMED	6
IV. LEVEL OF ORDINARY SKILL IN THE ART.....	7
V. LEGAL PRINCIPLES.....	8
VI. MATERIALS CONSIDERED.....	11
VII. OVERVIEW OF THE '404 PATENT	13
A. THE SPECIFICATION	13
B. THE CLAIMS	16
C. THE PROSECUTION HISTORY	18
VIII. OVERVIEW OF THE PRIOR ART	19
A. <i>Walker</i>	19
B. <i>Zellner</i>	22
C. <i>Martin</i>	25
IX. INTERPRETATION OF THE '404 PATENT CLAIMS	29
X. SPECIFIC GROUNDS FOR CHALLENGE.....	29
A. GROUND 1A: <i>WALKER</i> IN COMBINATION WITH <i>KIM</i> RENDERS OBVIOUS CLAIMS 9, 10, 12-14	29
1. CLAIM 9	29
a. 9[pre] A mobile device, comprising.....	29
b. 9[a] a camera unit, adapted to obtain at least one of image data and audio data;	31
c. 9[b] a location unit, adapted to obtain location data	36
d. 9[c] a transmitting unit, adapted to transmit as emergency information the image data, the audio data, and the location data along with specific information including owner identification information; and.....	40

e.	9[d] & 9[e]	70
(i)	“a panic button ... wherein the panic button is activated by a series of depressings of the panic button”	70
(ii)	the panic button is “adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location when the panic button is activated”	91
2.	CLAIM 10: The mobile device as set forth in claim 9, wherein when the panic button is activated a public or private network for emergency purposes is dialed.	101
3.	CLAIM 12: The mobile device of claim 9, wherein a number of depressings of the panic button to activate the panic button is three.	110
4.	CLAIM 13	110
a.	13[pre], 13[a], 13[b], and 13[e]	110
b.	13[c]: a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location, along with specific information including owner identification information; and	110
c.	13[d]: “a panic button, which, when activated, performs the following panic button functions: (1) activating the camera unit, the location unit, and the transmitting unit to send the emergency information and the specific information to the specified location, and (2) dialing a public or private network for emergency purposes”	111
5.	CLAIM 14: “The mobile device of claim 13, wherein a number of depressings of the panic button to activate the panic button is five”	112
B.	GROUND 1B: WALKER IN VIEW OF KIM AND DIXIT RENDERS CLAIM 14 OBVIOUS	113
C.	GROUND 2: WALKER RENDERS OBVIOUS CLAIM 15	120
1.	CLAIM 15	120

a.	15[pre]: “An emergency safety device, comprising”	120
b.	15[a]: “a camera unit, adapted to obtain at least one of image data and audio data”; and 15[b]: “a location unit, adapted to obtain location data”	125
c.	15[c]: “a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location via text message, along with specific information including owner identification information; and”	125
d.	15[d] & 15[e]	133
(i)	“a panic button ... wherein the panic button is activated by a button sequence”	133
(ii)	A panic button “adapted to activate the transmitting unit when activated”	139
D.	GROUND 3A: ZELLNER IN COMBINATION WITH KIM RENDERS OBVIOUS CLAIMS 9-14	139
1.	CLAIM 9	140
a.	9[pre] A mobile device, comprising.....	140
b.	9[a] a camera unit, adapted to obtain at least one of image data and audio data;	142
c.	9[b] a location unit, adapted to obtain location data	146
d.	9[c] a transmitting unit, adapted to transmit as emergency information the image data, the audio data, and the location data along with the specific information including owner identification information; and.....	150
e.	9[d] & 9[e]	178
(i)	“a panic button...wherein the panic button is activated by a series of depressings of the panic button”	178
(ii)	the panic button is “adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location when the panic button is activated”	185

2.	CLAIM 10: The mobile device as set forth in claim 9, wherein when the panic button is activated a public or private network for emergency purposes is dialed.....	188
3.	CLAIM 11: “A mobile device as set forth in claim 9, wherein the specific information includes a pre-recorded emergency message.”	193
4.	CLAIM 12: “The mobile device of claim 9, wherein a number of depressings of the panic button to activate the panic button is three.”.....	196
5.	CLAIM 13	196
a.	13[c] a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location, along with specific information including owner identification information; and	196
b.	13[d] a panic button, which, when activated, performs the following panic button functions: (1) activating the camera unit, the location unit, and the transmitting unit to send the emergency information and the specific information to the specified location, and (2) dialing a public or private network for emergency purposes;.....	197
6.	CLAIM 14: “The mobile device of claim 13, wherein a number of depressings of the panic button to activate the panic button is five.”	199
E.	GROUND 3B: ZELLNER IN COMBINATION WITH KIM AND DIXIT RENDERS CLAIM 14 OBVIOUS.....	199
F.	GROUND 4A: <i>MARTIN</i> IN COMBINATION WITH KIM RENDERS OBVIOUS CLAIMS 9, 10, 12-14	200
1.	CLAIM 9	200
a.	9[pre] A mobile device, comprising.....	200
b.	9[a] a camera unit, adapted to obtain at least one of image data and audio data;	201
c.	9[b] a location unit, adapted to obtain location data	203
d.	9[c] a transmitting unit, adapted to transmit as emergency information the image data, the audio	

	data, and the location data along with specific information including owner identification information; and.....	205
e.	9[d] & 9[e]	210
	(i) “a panic button ... wherein the panic button is activated by a series of depressings of the panic button”	210
	(ii) the panic button is “adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location when the panic button is activated”	216
2.	CLAIM 10: The mobile device as set forth in claim 9, wherein when the panic button is activated a public or private network for emergency purposes is dialed.	224
3.	CLAIM 12: The mobile device of claim 9, wherein a number of depressings of the panic button to activate the panic button is three.	227
4.	CLAIM 13	227
	a. 13[pre], 13[a], 13[b], 13[e]	227
	b. 13[c]: a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location, along with specific information including owner identification information; and	227
	c. 13[d]: a panic button, which, when activated, performs the following panic button functions: (1) activating the camera unit, the location unit, and the transmitting unit to send the emergency information and the specific information to the specified location, and (2) dialing a public or private network for emergency purposes, ...	229
5.	CLAIM 14: The mobile device of claim 13, wherein a number of depressings of the panic button to activate the panic button is five.	230

G.	Grounds 4B: <i>Martin</i> in view of <i>Kim</i> and <i>Dixit</i> renders claim 14 obvious	231
XI.	CONCLUSION	231

I, William R. Michalson of Douglas, Massachusetts, declare that:

I. ASSIGNMENT

1. I have been retained on behalf of Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (together, “Samsung”), to offer technical opinions related to U.S. Patent No 11,265,404 (“the ’404 patent”) (Ex1001). I understand that Samsung is requesting that the Patent Trial and Appeal Board (“PTAB” or “Board”) institute an *inter partes* review (“IPR”) proceeding of the ’404 patent.

2. I have been asked to provide my independent analysis of the ’404 patent based on the prior art publications cited in this declaration.

3. I am not and never have been, an employee of Samsung. I received no compensation for this declaration beyond my normal hourly compensation based on my time actually spent analyzing the ’404 patent, the prior art publications cited below, and issues related thereto, and I will not receive any added compensation based on the outcome of any IPR or other proceeding involving the ’404 patent.

II. QUALIFICATIONS

4. I am over the age of 18 and am competent to write this declaration. I have personal knowledge, or have developed knowledge, of these technologies based upon education, training, or experience of the matters set forth herein.

5. I earned a B.S. in Electrical Engineering from Syracuse University in 1981, and an M.S. and a Ph.D. in Electrical Engineering from the Worcester Polytechnic Institute (WPI) in 1985 and 1989, respectively.

6. I am currently a tenured Professor in Robotics Engineering in the Robotics Engineering Department of WPI. I also hold appointments as a Professor of Computer Science, a Professor of Electrical and Computer Engineering, and as a Professor of Mechanical Engineering. At WPI, 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 systems for both civilian and military applications with a special emphasis on techniques focused on indoor, underground, or otherwise GPS-denied 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 level.

7. 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.

8. 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 to this

Declaration as Appendix A. 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.

9. I have been involved with numerous projects involving the tracking and control of remote objects, including objects traveling in the air, on the ground, and in the water. Starting with my work at 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, inertial guidance systems, including using augmentations to the GPS. As outlined in my CV, I have decades of experience using cellular and other radio technologies for passing telemetry (such as audio, video, location, and other information relevant to understanding the status of a system), performing remote control, and performing geolocation.

10. 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 computer systems, navigation, and communications for a large variety of applications in the air, on land, and on the sea.

11. I have received numerous awards and recognition for my work, including becoming a 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, the Academy of Model Aeronautics, and the National Academy of Inventors.

12. My curriculum vitae, attached as Exhibit A, includes a list of publications on which I am a named author. It contains further details regarding my experience, education, publications, and other qualifications provide to an expert opinion in connection with this proceeding.

III. SUMMARY OF CONCLUSIONS FORMED

13. This Declaration explains the conclusions that I have formed based on my analysis. To summarize those conclusions:

- Ground 1A: Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 9, 10, and 12-14 of the '404 patent are made obvious by *Walker* (EX1007) in view of *Kim* (EX1010).
- Ground 1B: Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claim 14 of the '404 patent is made obvious by *Walker* in view of *Kim* and *Dixit* (EX1011).
- Ground 2: Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claim 15 of the '404 patent is made obvious by *Walker*.

- Ground 3A: Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 9-14 of the '404 patent are made obvious by *Zellner* (1008) in view of *Kim*.
- Ground 3B: Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claim 14 of the '404 patent is made obvious by *Zellner* in view of *Kim* and *Dixit*.
- Ground 4A: Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 9, 10, and 12-14 of the '404 patent are made obvious by *Martin* (EX1009) in view of *Kim*.
- Ground 4B: Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claim 14 of the '404 patent is made obvious by *Martin* in view of *Kim* and *Dixit*.

IV. LEVEL OF ORDINARY SKILL IN THE ART

14. I have been informed by Petitioners' counsel that a person of ordinary skill in the art is a hypothetical person who is presumed to have the skill and experience of an ordinary worker in the field at the time of the priority date of the challenged patent. I have been asked to assume for the purposes of this Petition that the priority date is January 14, 2005.

15. Based on my knowledge and experience in the field and my review of the '404 patent and file history, I believe that a person of ordinary skill in the art in this matter would have had at least a Bachelor's of Science Degree (or equivalent) in an academic area emphasizing electrical engineering, computer engineering, computer science, or a related technical field, and about 1-2 years of experience working with telematics systems (e.g. familiarity with wireless

communications, geolocation systems, and human-computer interfaces). A greater amount of education in an academic area emphasizing electrical engineering, computer engineering, computer science, or a related technical field, would compensate for fewer years of work experience, and more years of work experience would compensate for less education. This is the appropriate level of skill, whether the claims are entitled to priority as of January 2005 or January 2019.

16. Based on my experiences, I have at least the skills of a person having ordinary skill in the art as well as a good understanding of the capabilities of a person having ordinary skill in the art. To be clear, all of my opinions in this declaration are from the perspective of one of ordinary skill in the art as I have defined it here during the relevant timeframe.

V. LEGAL PRINCIPLES

17. I am not an attorney and offer no legal opinions, but in the course of my work, I have had experience studying and analyzing patents and patent claims from the perspective of a person skilled in the art.

18. For the purposes of this declaration, I have been informed about certain aspects of the law that are relevant to forming my opinions. My understanding of the law is as follows.

19. Petitioner's counsel has informed me that for the prior art to inherently disclose a claimed limitation, the prior art need not expressly disclose the limitation, so long as the claimed limitation necessarily flows from a disclosure in the prior art. I also understand that it is acceptable to examine evidence outside the prior art reference (extrinsic evidence) in determining whether a feature, while not expressly discussed in the reference, is necessarily present in that reference.

20. Petitioner's counsel has informed me that a patent claim can be considered to have been obvious to a person of ordinary skill in the art at the time the application was filed. I am informed that this means that, even if all of the requirements of a claim are not found in a single prior art reference, the claim is not patentable if the differences between the subject matter in the prior art and the subject matter in the claim would have been obvious to a person of ordinary skill in the art at the time of the invention.

21. I have been informed by Petitioners' counsel that a determination of whether a claim would have been obvious should be based upon several factors, including, among others:

- the level of ordinary skill in the art at the time the application was filed;
- the scope and content of the prior art; and
- what differences, if any, existed between the claimed invention and the prior art.

22. I have been informed by Petitioners' counsel that a single reference can render a patent claim obvious if any differences between that reference and the claims would have been obvious to a person of ordinary skill in the art. Alternatively, I understand that the teachings of two or more references may be combined in the same way as disclosed in the claims, if such a combination would have been obvious to one having ordinary skill in the art. In determining whether a combination based on either a single reference or multiple references would have been obvious, it is appropriate to consider, among other factors:

- whether the teachings of the prior art references disclose known concepts combined in familiar ways, and when combined, would yield predictable results;
- whether a person of ordinary skill in the art could implement a predictable variation, and would see the benefit of doing so;
- whether the claimed elements represent one of a limited number of known design choices, and would have a reasonable expectation of success by those skilled in the art;
- whether a person of ordinary skill would have recognized a reason to combine known elements in the manner described in the claim;
- whether there is some teaching or suggestion in the prior art to make the modification or combination of elements claimed in the patent; and
- whether the innovation applies a known technique that had been used to improve a similar device or method in a similar way.

23. I have been informed by Petitioners' counsel that one of ordinary skill in the art has ordinary creativity and is not an automaton. Petitioner's counsel has also informed me that in considering obviousness, obviousness may

not be determined using the benefit of hindsight, including hindsight derived from the patent being considered.

VI. MATERIALS CONSIDERED

24. My analysis and conclusions set forth in this declaration are based on my educational background and experiences in the field (see Section II).

Based on my knowledge and experience, I believe that I am considered to be an expert in the field. Also, based on my knowledge and experience, I understand and know of the capabilities of persons of ordinary skill in the field since the early 2000s, and I taught, participated in organizations, and worked closely with many such persons in the field during that time frame.

25. As part of my independent analysis for this declaration, I have considered the following: the background knowledge/technologies that were commonly known to persons of ordinary skill in this art during the time before the earliest claimed priority date for the '404 patent; my own knowledge and experiences gained from my work experience in the field of the '404 patent and related disciplines; and my experience in working with others involved in this field and related disciplines.

26. In addition, I have analyzed the following publications and materials:

- U.S. Patent No. 11,265,404 to DiPerna (“the '404 Patent”) (EX1001);

- The Prosecution History of the '404 Patent (“the Prosecution History”) (EX1004);
- U.S. Provisional Application No. 60/643,865 (EX1005);
- U.S. Application No. 13/897,353 (EX1006);
- U.K. Publication No. GB 2 401 752A (“*Walker*”) (EX1007);
- U.S. Patent No. 6,807,564 (“*Zellner*”) (EX1008);
- U.S. Patent No. 6,839,552 (“*Martin*”) (EX1009);
- International Publication No. WO 2004/056000 A1 (“*Kim*”) (EX1010);
- U.S. Patent No. 6,449,472 (“*Dixit*”) (EX1011);
- International Publication No. WO 03/040995 (“*Chang*”) (EX1012);
- U.S. Publication No. 2006/0217105A1 (“*Kumar*”) (EX1013);
- U.S. Publication No. 2005/0287980 (“*Wood*”) (EX1014);
- U.S. Patent No. 5,712,679A (“*Coles*”) (EX1015);
- U.S. Publication No. 2003/0027547A1 (“*Wade*”) (EX1016);
- U.S. Patent No. 5,771,001 (“*Cobb*”) (EX1017);
- International Publication No. WO2004/042669 (“*Smith*”) (EX1018);
- U.S. Publication No. 2004/0203570 (“*Berger*”) (EX1019);
- International Publication No. WO1999026208A1 (“*Ahmad*”) (EX1020)
- U.S. Patent No. 6,963,283 (“*Gonzales*”) (EX1021);
- U.S. Patent No. 5,515,419 (“*Sheffer*”) (EX1022);

- Steven M. Kaplan, Wiley Electrical and Electronics Engineering Dictionary 697 (2004) (EX1023);
- WEBSTER’S NEW WORLD COLLEGE DICTIONARY 1109 (Michael Agnes et al. eds., 4th ed. 2004) (EX1024); and

and any other materials I refer to in this declaration in support of my opinions.

27. My analysis and conclusions set forth in this declaration are based on the perspective of a person having ordinary skill in the art.

VII. OVERVIEW OF THE ’404 PATENT

A. THE SPECIFICATION

28. The ’404 Patent is titled “Emergency personal protection system integrated with mobile devices.” It “relates generally to the field of personal safety devices.” EX1001, 1:21-22. The alleged invention “provides a self-defense device which is integrated with or used with a mobile phone/device” in which a “self-defense mechanism” is “attached to a mobile phone/device.” *Id.*, 4:52-56. “[T]he self-defense mechanism can be a separate panic button.” *Id.*, 5:40-42.

29. “[W]hen the self-defense mechanism is activated, a camera built into the mobile phone/device takes an image of the attacker, and the mobile phone/device sends image data and audio data to the authorities along with specific information such as, for example, the name and description of the owner

of the self-defense device, location information, a time and date stamp, etc.” *Id.*, 3:4-13. “In this way, the present invention utilizes a built-in camera to take still or moving images of the attacker and send the image and/or audio data to the authorities along with the specific information.” *Id.*, 3:13-16.

30. The ’404 patent discloses “a mobile device, comprising a camera unit, adapted to obtain at least one of image data and audio data; a location unit, adapted to obtain location data; a transmitting unit, adapted to transmit at least one of the image data, the audio data, and the location data; and a panic button, adapted to activate the camera, the location unit, and the transmitting unit.” *Id.*, 3:51-58.

31. The ’404 patent explains:

In one example, pushing a “panic button” on the mobile phone/device of the present invention can result in a still image or moving video being taken, as well as an audio recording being obtained. The present invention then wraps the data up and transmits it to an emergency service with the x-y coordinates. This enables the emergency service to have image and/or audio data as well as the relevant location information. ... For example, panic button can trigger the image/audio data and location information being obtained.

Id., 7:1-16.

32. The panic button may be activated in various ways:

The panic button may be activated by at least one of: (1) a depressing or series of depressions of the panic button, (2) a depressing of the panic button for a predetermined time period, (3) a depressing of the panic button together with another button, and (4) a codeword.

Id., 3:59-65.

33. The '404 patent discloses implementing a “safeguard against falsely triggering the device” such as “a button sequence, the number of times a button is depressed, etc.” *Id.*, 7:54-57.

34. The '404 patent discloses using “a number of ways to send image data and audio data.” *Id.*, 6:44-45. The '404 patent discloses using TCP/IP:

The present invention in one embodiment communicates the emergency information (image information, location information, owner information, etc.) through a TCP/IP (Transmission Control Protocol/internet Protocol) connection on the phone or mobile device, or through another such as WAP (Wireless Application Protocol). TCP/IP is a communications protocol that is used to connect hosts on the Internet, and TCP/IP is the de facto standard for transmitting data over networks.

Id., 6:20-28.

35. The '404 patent discloses using Multimedia Messaging Service (“MMS”):

The present invention may also use an MMS (Multimedia Message Service) system, which is a mix between internet

protocol and e-mail protocol. More specifically, MMS is a store-and-forward method of transmitting graphics, video clips, sound files, and short text messages over wireless networks using WAP. MMS implementations also support e-mail addressing, so that the device can send e-mails directly to an e-mail address. The presentation of the MMS message is coded into the presentation file so that images, sounds, and text are displayed in a predetermined order as one singular message. The most common use of MMS is for communication between mobile phones/devices. MMS is one method enabling the present invention to obtain video/audio information and send the data to a specified location. Of course, the present invention is not limited to using protocols such as TCP/IP and MMS.

Id., 6:28-43.

36. The '404 patent also discloses using “regular e-mail” or a “web service.” *Id.*, 6:47-51.

B. THE CLAIMS

37. The table below includes identifiers for the '404 patent claims and limitations, which are referenced throughout.

Claim 9	
9[pre]	A mobile device, comprising:
9[a]	a camera unit, adapted to obtain at least one of image data and audio data;
9[b]	a location unit, adapted to obtain location data;

9[c]	a transmitting unit, adapted to transmit as emergency information the image data, the audio data, and the location data along with specific information including owner identification information; and
9[d]	a panic button, adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location when the panic button is activated,
9[e]	wherein the panic button is activated by a series of depressings of the panic button.
Claim 10	
10	The mobile device as set forth in claim 9, wherein when the panic button is activated a public or private network for emergency purposes is dialed.
Claim 11	
11	A mobile device as set forth in claim 9, wherein the specific information includes a pre-recorded emergency message.
Claim 12	
12	The mobile device of claim 9, wherein a number of depressings of the panic button to activate the panic button is three.
Claim 13	
13[pre]	A mobile device, comprising:
13[a]	a camera unit, adapted to obtain at least one of image data and audio data;
13[b]	a location unit, adapted to obtain location data;
13[c]	a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location, along with specific information including owner identification information; and
13[d]	a panic button, which, when activated, performs the following panic button functions: (1) activating the camera unit, the location unit, and the transmitting unit to send the emergency information and the specific information to the specified location, and (2) dialing a public or private network for emergency purposes,

13[e]	wherein the panic button is activated by a series of depressings of the panic button.
Claim 14	
14	The mobile device of claim 13, wherein a number of depressings of the panic button to activate the panic button is five.
Claim 15	
15[pre]	15. An emergency safety device, comprising:
15[a]	a camera unit, adapted to obtain at least one of image data and audio data;
15[b]	a location unit, adapted to obtain location data;
15[c]	a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location via text message, along with specific information including owner identification information; and
15[d]	a panic button, adapted to activate the transmitting unit when activated,
15[e]	wherein the panic button is activated by a button sequence.

C. THE PROSECUTION HISTORY

38. The '404 patent issued from U.S. App. No. 16/262,835. During prosecution, the Patent Office rejected then-pending claims 16, 35, and 36 (issued claims 9, 13, and 15, respectively) in view of the prior art. *See* EX1004 at 43, 155, 162.

39. In response, the applicant made two amendments to claim 16. First, the applicant amended the claim 16 so that, instead of merely requiring that “at least one” of image, audio, location be transmitted, it requires that “**all four** pieces of information are transmitted by the transmitting unit when the panic

button is activated: the image data, the audio data, the location data (as ‘the emergency information’), along with the specific information including owner identification information.” *Id.*, 132-133 (emphasis in original).

40. Second, the applicant amended claim 16 to require “wherein the panic button is activated by a series of depressings of the panic button.” *Id.*, 133 (emphasis in original). The applicant also added new claims 38 and 39 (issued claims 12 and 14), which require that the number of depressings required to activate the panic button is three and five, respectively. *Id.*, 127.

41. After the other independent claims were similarly amended, the Patent Office allowed the application. *Id.*, 35-38.

VIII. OVERVIEW OF THE PRIOR ART

A. *Walker*

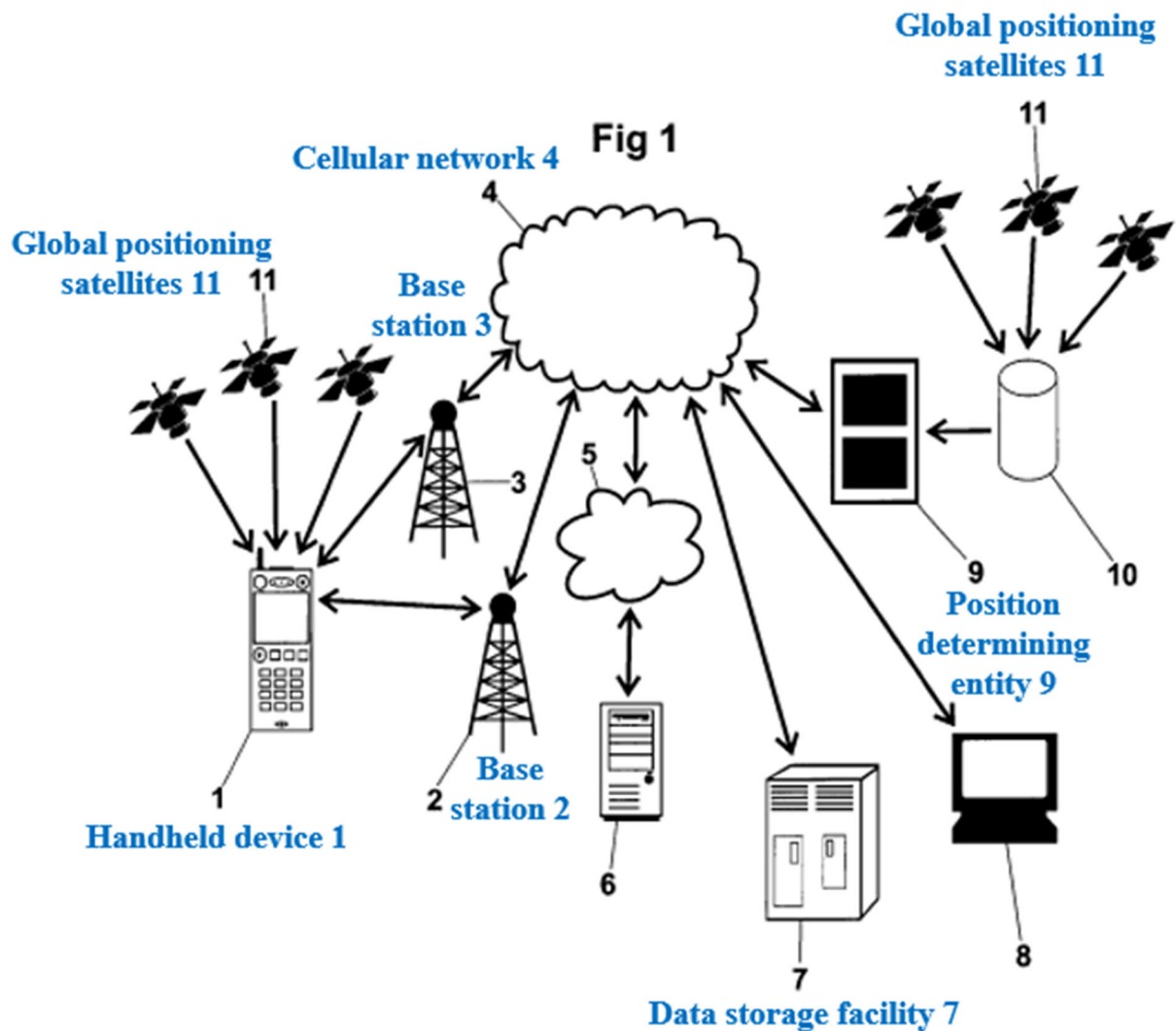
42. *Walker* relates to “a cellular handheld mobile communications device and external data storage system, and is intended to enhance personal safety and security, acting as an electronic eyewitness, helping to deter criminal activity and to reduce the incidence of crime.” EX1007 ¶[0001]. Walker explains that “Mobile communications handheld devices with digital camera and video recording functionality are available, enabling users to record photographic or digital images and sound, potentially capturing eyewitness

evidence relating to a crime or potential crime, but such devices do not currently serve as a deterrent against crime in their present form.” *Id.* ¶[0025].

43. *Walker*’s disclosure “provides a mobile communications handheld device and remote data recording and storage system which, in a single action, enables a user of the mobile communications handheld device to press a recessed eyewitness button or shout a voice command, which instantly initiates a series of actions, immediately capturing and transmitting streaming video and sound and environmental data detected by various sensors to a remote data storage facility, providing evidence of another individual's physical appearance, dress, behaviour, utterances and surroundings in real time and without any dial-up delay, together with precise geographical coordinates of the location and the precise time of the event, where the recorded data cannot be destroyed by an attacker even in the event that the handheld device is destroyed following such transmission.” *Id.* ¶[0038].

44. Figure 1, copied and annotated below, “shows the dataflow between the handheld mobile communications device 1, cellular network 4 and data storage facility 7, and between the handheld device 1 and positioning systems which include the cellular base stations 2 and 3, and position determining entity 9 and wide area reference network 10, and the constellation of global positioning satellites 11. Figure 1 additionally shows network services operators 8 and

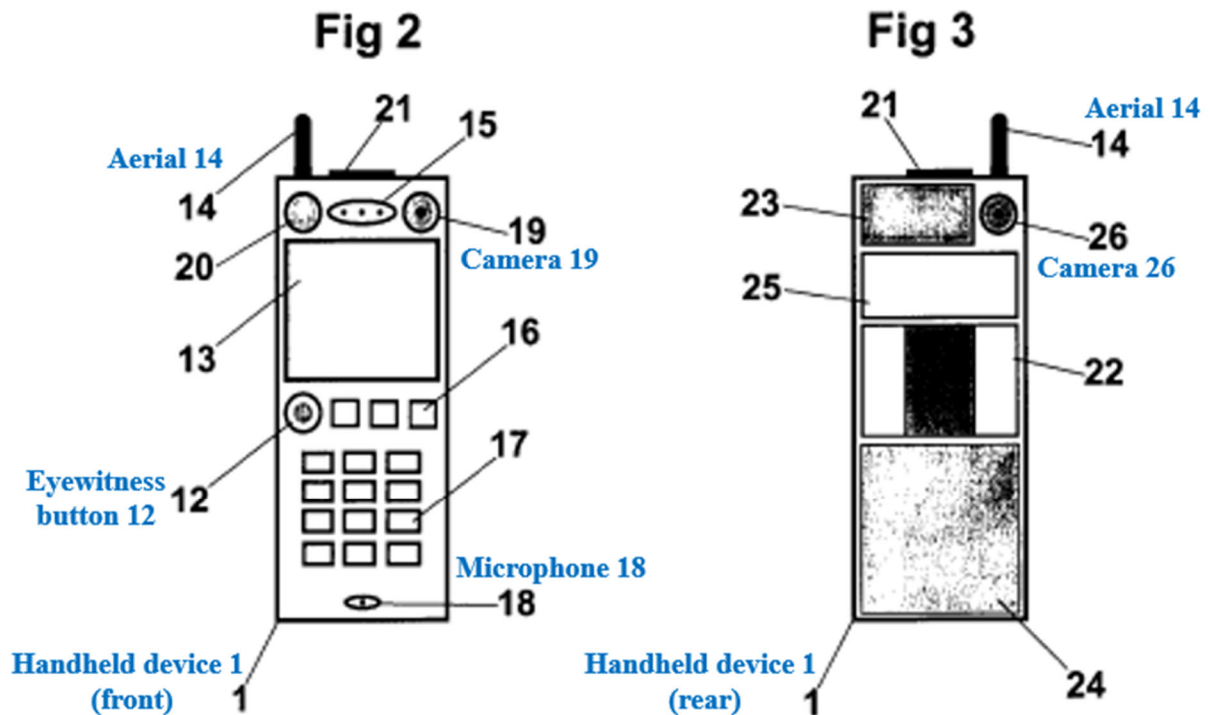
software applications based on a web based server 6 connected to the internet 5 and cellular network 4.” *Id.* ¶[0062].



EX1007, Fig. 1 (annotated).

45. Figures 2 and 3, copied and annotated below, show the handheld device. *Id.* ¶¶[0063], [0064]. Walker’s handheld device includes a recessed eyewitness button 12, aerial 14, high sensitivity microphone 18, location identification components and technology (e.g., a handset-based Global

Positioning System (GPS) receiver), two opposite-facing digital colour cameras with night vision sensitivity 19 and 26, and an array of other telecommunication, sensor, hardware, and software features. *Id.*



EX1007, FIGs. 2, 3 (annotated).

B. Zellner

46. *Zellner* relates to “emergency reporting devices, and more particularly, to a device that employs TCP/IP (Transmission Control Protocol/Internet Protocol) messaging to report a user's emergency condition to an emergency service center (e.g., the police).” EX1008, 1:14-19.

47. *Zellner* discloses a portable “IP device” with a built-in panic button. *Id.*, 6:55-58. *Zellner* explains that activating the panic button “by a user in need

of emergency help,” causes the device to automatically transmit “one or more TCP/IP messages over the Internet to an emergency service center requesting emergency help and identifying the user requesting such help.” *Id.*, 19:29-34.

48. Zellner discloses that the IP device includes “a built-in digital camera or other image capture device 36,” an “audio logic unit 40,” and “a user location identifier 59.” *Id.*, FIG. 6. The “camera 36 may be activated when the panic button 24 is pressed by the user” and can “take quick snapshots, or motion pictures, of the environment surrounding the user of the IP device 20.” *Id.*, 8:1-4. “The audio logic unit 40 may be connected to the microphone 34 and the speaker 32,” and “the user of the IP device 20 may speak into the microphone 34 to transmit the user’s voice over the internet 22.” *Id.*, 9:3-4; 9:22-23.

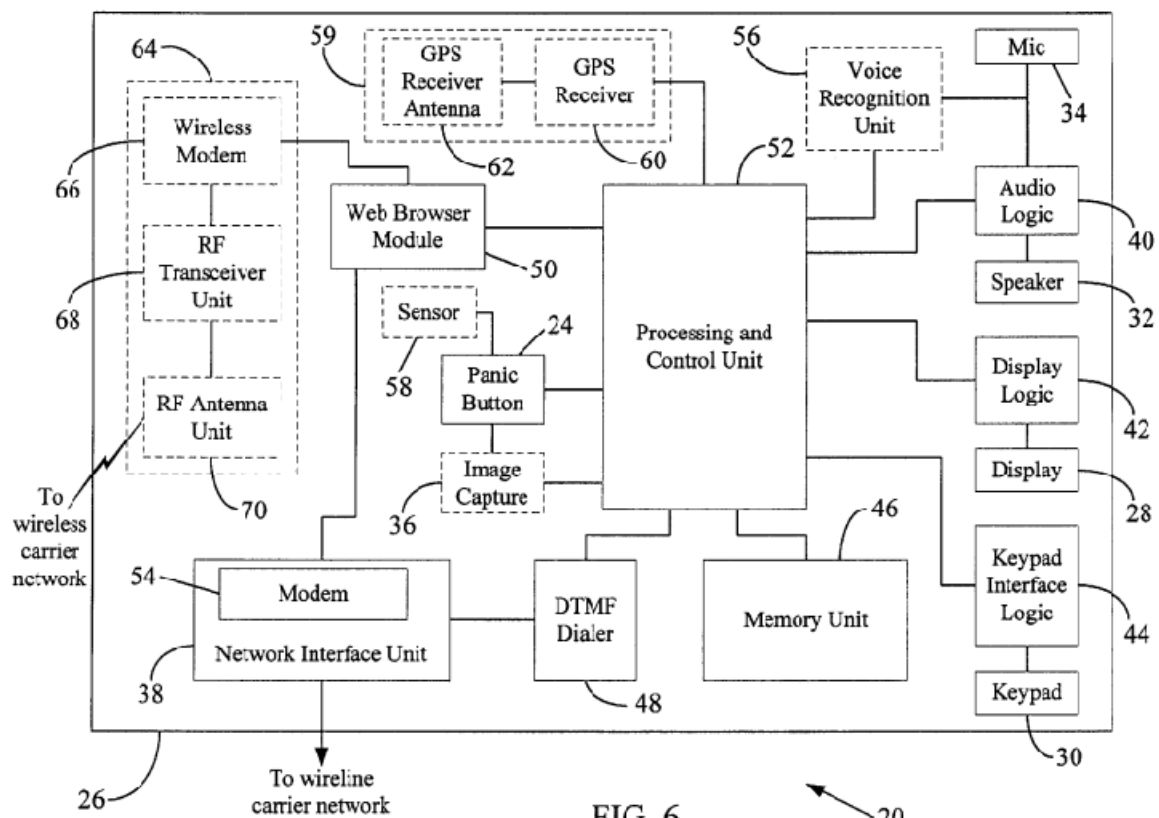


FIG. 6

EX1008, FIG. 6

49. The “location identifier unit 59,” supplies the current location of the device (and hence, of the user of the operating device) to the processing unit to be included as part of the help request message so that the ESC personnel may efficiently locate the user who requested the emergency help.” *Id.*, 3:34-38; FIG. 6. “The wireless data communication module 64 employs wireless devices to transfer data and information between the IP device 20 and the ESC over the Internet 22.” *Id.*, 14:39-41; FIG. 6.

C. *Martin*

50. *Martin* relates to “to a system and method for reporting an emergency situation using a wireless device.” EX1009, 1:8-10.

51. *Martin* describes how a crime victim’s situation worsens if that person is unable to “communicate with others to obtain help” and further jeopardizes his or her safety when attempting to use a wireless telephone ultimately intercepted by a kidnapper. *Id.*, 1:12–22.

52. *Martin* discloses a “wireless device to report an emergency situation to a called party” such as a Public Safety Answering Point (“PSAP”) using telecommunication capabilities. *Id.*, 1:29–33, 1:66–2:2.

53. *Martin*’s device 100 may be embodied as a wireless telephone including a microprocessor 110, keyboard 120, antenna 150, location system 180, and one or more sensing devices 160. Specifically, *Martin*’s location system 180 may be a Global Positioning System (GPS) receiver in communication with GPS satellites to provide wireless device position coordinates, and sensing device 160 may be a plurality of devices, including at least a camera and microphone. *Id.*, 3:36–37, 3:59–65. *Martin* also discloses keyboard 120 and “one special key” that can be pressed according to a “keystroke sequence” for placing a call to any of a PSAP, 911, an undercover

law enforcement operation center, and/or other parties. *Id.*, 6:29–34, 6:43–46, 7:18–25.

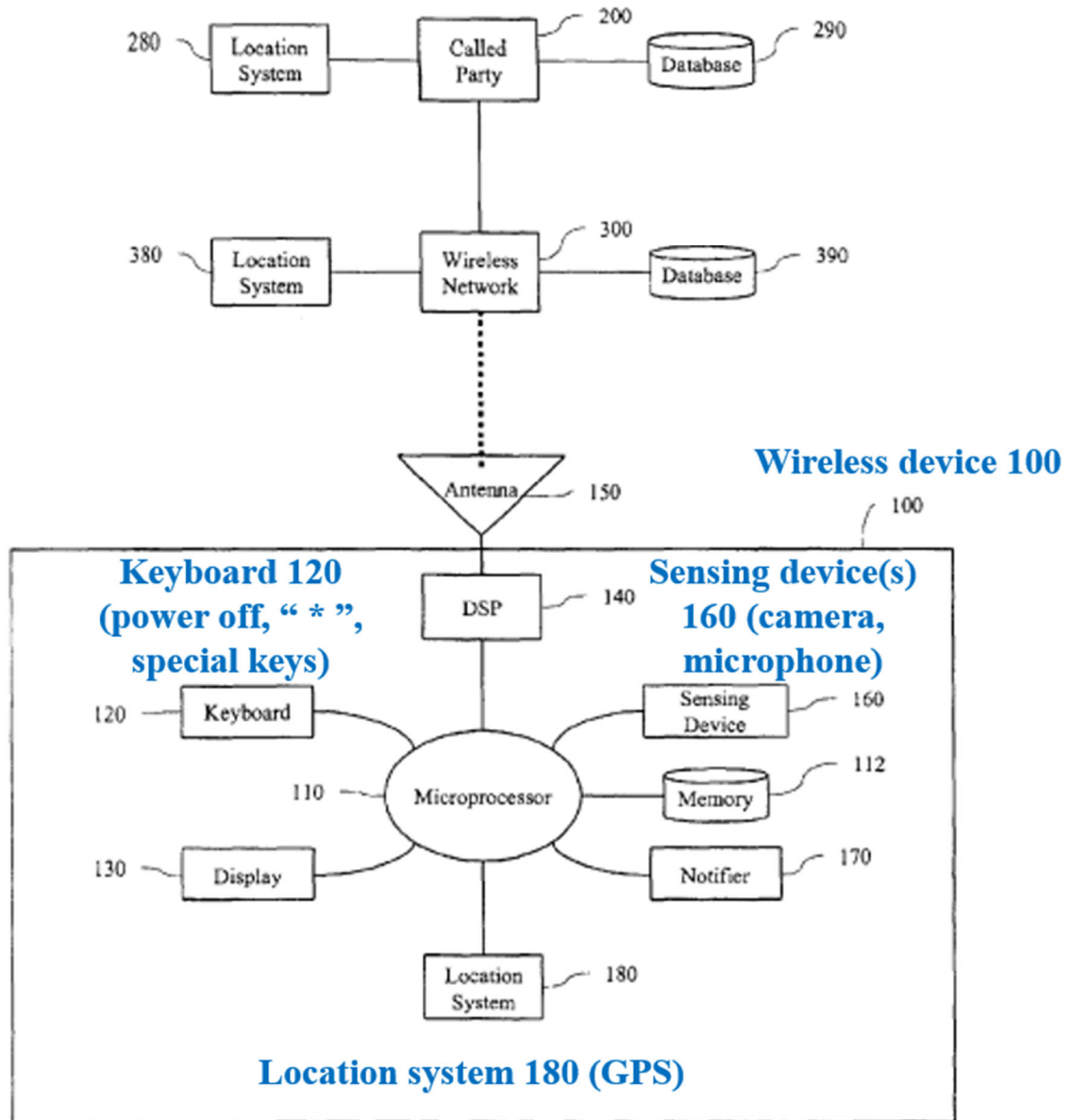


Figure 2

Martin, Fig. 2 (annotated).

54. Entering a keystroke sequence on *Martin's* wireless device initiates a wireless communication session with the called party and process to capture and provide circumstantial content in "steps and sub-steps ...implemented in any combination and in any logical order to accomplish a specific purpose." *Id.*, 4:9–20; *see also* Fig. 3, 4:40–42. *Martin* identifies digital signal processor ("DSP") 140 and antenna 150 as the components to establish the communication session. *Id.*, 5:1–3. User identification information associated with the wireless device in a user profile is provided to the called party. *Id.* 4:33–42. Location and content capture components are also initiated to capture sound, images, and GPS coordinate position information provided to the called party. *Id.*, Fig. 3 (steps 312, 314, 320, 322), 3:59–65, 5:4–14, 5:39–46.

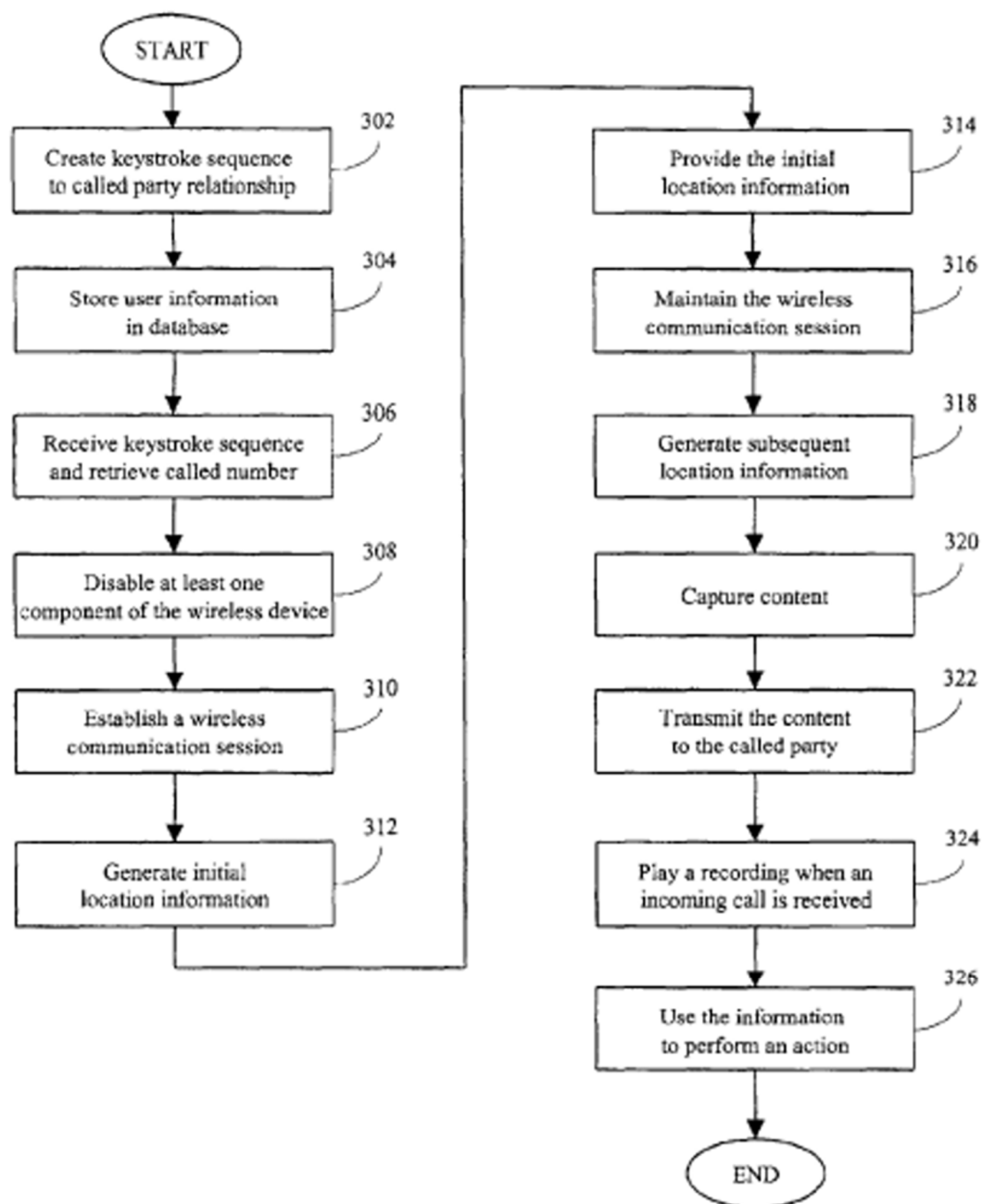


Figure 3

Martin, Fig. 3.

IX. INTERPRETATION OF THE '404 PATENT CLAIMS

55. I have given all the claim terms their plain and ordinary meaning, as would have been understood by a person having ordinary skill in the art, at the time of the alleged invention, having taken into consideration the language of the claims, the specification, and the prosecution history of record. My interpretation does not change regardless of whether the priority date is January 2005 or January 2019.

X. SPECIFIC GROUNDS FOR CHALLENGE

A. GROUND 1A: *WALKER* IN COMBINATION WITH *KIM* RENDERS OBVIOUS CLAIMS 9, 10, 12-14

1. CLAIM 9

a. 9[pre] A mobile device, comprising

56. In my opinion, to the extent the preamble is limiting, *Walker* discloses or suggests “a mobile device.”

57. *Walker* discloses a “mobile communications handheld device”:

The present invention provides a mobile communications handheld device and remote data recording and storage system which, in a single action, enables a user of the mobile communications handheld device to press a recessed eyewitness button or shout a voice command, which instantly initiates a series of actions, immediately capturing and transmitting streaming video and sound and environmental data detected by various sensors to a remote data storage facility, providing evidence of

another individual's physical appearance, dress, behaviour, utterances and surroundings in real time and without any dial-up delay, together with precise geographical coordinates of the location and the precise time of the event, where the recorded data cannot be destroyed by an attacker even in the event that the handheld device is destroyed following such transmission.

EX1007 ¶[0038]¹

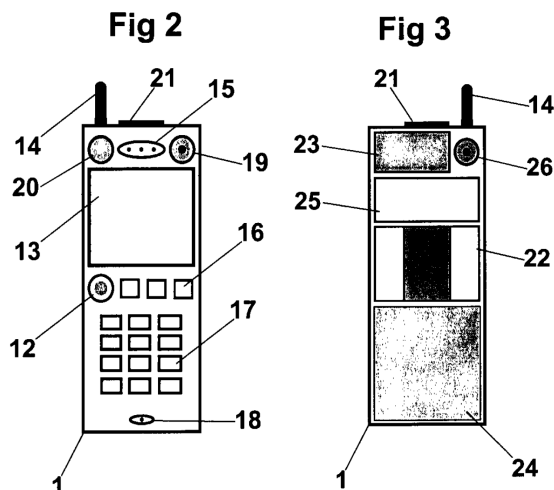
FIGURE 2 shows the front side of the *handheld device 1*, incorporating eyewitness button 12, LCD colour screen 13, aerial 14, loud speaker or earpiece 15, navigation buttons 16, keypad buttons 17, microphone 18, digital camera with night vision sensitivity 19, and infrared illumination 20.

Id. ¶[0063]

FIGURE 3 shows the reverse side of the *handheld device 1*, incorporating second digital camera with night vision sensitivity 26, aerial 14, rechargeable battery 24 held in place by the electronic locking mechanism (not shown), On/Off button 21, infrared movement sensor 22, infrared illumination 23, and combined torch & flashlight 25.

Id. ¶[0064]

¹ I understand that Petitioners have added paragraph numbers to the *Walker* reference. I am referring to the paragraph numbers shown in the version of *Walker* at Exhibit 1007.



Walker FIGs. 2, 3

58. In view of the above, a person having ordinary skill in the art would have understood *Walker* discloses or suggests a mobile device (“a mobile device”).

b. 9[a] a camera unit, adapted to obtain at least one of image data and audio data;

59. In my opinion, *Walker* discloses or suggests “a camera unit, adapted to obtain at least one of image data and audio data.”

60. *Walker* discloses that the mobile device includes a digital camera and captures video and sound:

The present invention provides a mobile communications handheld device and remote data recording and storage system which, in a single action, enables a user of the mobile communications handheld device to press a recessed eyewitness button or shout a voice command, which instantly initiates a series of actions, *immediately capturing and transmitting streaming*

video and sound and environmental data detected by various sensors to a remote data storage facility, providing evidence of another individual's physical appearance, dress, behaviour, utterances and surroundings in real time and without any dial-up delay, together with precise geographical coordinates of the location and the precise time of the event, where the recorded data cannot be destroyed by an attacker even in the event that the handheld device is destroyed following such transmission.

EX1007 ¶[0038]

FIGURE 2 shows the front side of the handheld device 1, incorporating eyewitness button 12, LCD colour screen 13, aerial 14, loud speaker or earpiece 15, navigation buttons 16, keypad buttons 17, microphone 18, *digital camera* with night vision sensitivity 19, and infrared illumination 20.

Id. ¶[0063]

FIGURE 3 shows the reverse side of the handheld device 1, incorporating second *digital camera* with night vision sensitivity 26, aerial 14, rechargeable battery 24 held in place by the electronic locking mechanism (not shown), On/Off button 21, infrared movement sensor 22, infrared illumination 23, and combined torch & flashlight 25.

Id. ¶[0064]

The preferred embodiment of the handheld mobile communications device 1 incorporates the following components and/or capabilities and/or features, some of which are not shown in the accompanying drawings:

... two colour digital cameras with night vision sensitivity positioned on opposing sides of the device 19 & 26, colour video recording and playback facility, still colour picture single frame recording, streaming video conferencing, video messaging, picture messaging...

Id. ¶¶[0081]-[0082]

61. *Walker* discloses an example use case that describes capturing video and sound:

The present invention may be used, for example, by a girl walking through a secluded park in the event that she is approached by a suspicious man. ***In such a circumstance, the girl simply presses the recessed eyewitness button on her mobile communications handheld device*** as soon as she begins to feel uncomfortable in the presence of the man. She holds the device as if to make a call or check some personal information stored in her phone, thereby not raising any suspicions, but ensuring that an integral camera is pointing in the direction of the suspicious man.

The girl immediately sees an image of the man appear on the screen of her device and knows that streaming video and sound and geographical and timeline data is immediately being transmitted to an external data storage facility, without any dialup delay, where it will be safely recorded and stored in real time. She also knows that even if the man subsequently destroys the device, his image and behaviour will remain stored at the data storage facility together with sound, geographic coordinates and the precise timeline of the encounter, linking him to her at that specific

location and at that specific time. The closer the man gets to the device, the higher the probability that his identity will be clearly captured by the camera and microphone and various other sensors (further embodiments of this invention include an odour sensor and fingerprint detector pad, and other such sensors, for capturing additional evidence in the event that the device is snatched from her hand).

Id. ¶¶[0043]-[0044]

62. *Walker* describes a method of using the mobile device that begins with pressing an “eyewitness button” and results in capturing video and sound with the integrated camera:

The entire process of capturing and transmitting data to the data storage facility is achieved with a single press of the eyewitness button 12 on the handheld device 1, followed by pointing ***the integral digital camera 26 on the reverse side of the device at the individual or individuals concerned. The integral digital camera on the front side of the device 19 simultaneously captures video data relating to the device user as the user holds the device in front of the user.***

Id. ¶[0091]

The preferred embodiment enables the device to be used in both daylight and dark conditions. For illustration purposes the following assumes that the invention is activated by the user in dark conditions. On pressing the eyewitness button 12 a series of automatic parallel or sequential actions are instantly initiated:

...

5) *The digital video camera circuitry and light sensor circuitry is powered up.* Light sensor data configures the device 1 and video cameras 19 & 26 to operate in night vision mode, and automatically powers up the two infrared illumination sources 20 & 23 to *enable images to be captured* in darkness. The infrared illumination source 20 is a low powered wide beam for illuminating the user, and the infrared illumination source 23 is a higher powered wide beam, for illuminating other individuals and the surrounding environment.

6) *The device begins transmitting ongoing streaming video and sound data* and other data to the data storage facility 7 where compatible recording equipment is permanently on standby to receive, record and log the automatic transmission of mission critical data from the handheld device 1 in real time. The video data transmitted are simultaneously displayed on the device screen 13, enabling the user to monitor what video data are being transmitted.

Id. ¶¶[0092], [0098], [0099].

63. *Walker's* description is consistent with how the '404 patent describes this feature:

In another embodiment, the present invention provides a self-defense device including a self-defense mechanism which is integrated with a mobile phone/device such that *when the self-defense mechanism is activated, a camera built into the mobile phone/device takes an image of the attacker, and the mobile*

phone/device sends image data and audio data to the authorities along with specific information such as, for example, the name and description of the owner of the self-defense device, location information, a time and date stamp, etc. In this way, the present invention utilizes a built-in camera to take still or moving images of the attacker and send the image and/or audio data to the authorities along with the specific information. The self-defense mechanism can be a vial containing pepper spray or mace, for example, or simply a separate panic button located on the device which activates the above-mentioned processes. Of course, the present invention is not limited to the examples discussed herein.

EX1001, 3:4-21

64. In my opinion, and based on my background and experience, a person having ordinary skill in the art would have understood video to comprise “image data,” and “sound” to comprise “audio data.”

65. Therefore, a person having ordinary skill in the art would have understood that *Walker* discloses or suggests a handheld mobile communications device with a camera (“camera unit”) that captures pictures, videos, and/or sound (“adapted to obtain at least one of image data and audio data”).

c. 9[b] a location unit, adapted to obtain location data

66. In my opinion, *Walker* discloses or suggests “a location unit, adapted to obtain location data.”

67. *Walker* discloses that the mobile device includes “A-GPS circuitry”:

The preferred embodiment enables the device to be used in both daylight and dark conditions. For illustration purposes the following assumes that the invention is activated by the user in dark conditions. On pressing the eyewitness button 12 a series of automatic parallel or sequential actions are instantly initiated:

...

3) *The hybrid A-GPS circuitry built into the handheld device 1* is powered up.

...

8) Within 6 seconds of pressing the eyewitness button 12 *the hybrid A-GPS circuitry* obtains sufficient data from the satellite constellation 11 and cellular network 4. *From such data the location coordinates are calculated.* The calculation is performed by the handheld device 1 or network 4 and the coordinates are immediately transmitted to the data storage facility 7, integrated with the continuing video stream, sound data and other data. As the transmission of video and sound and other data continues, hybrid A-GPS data are regularly updated and transmitted to the data storage facility 7.

Id. ¶¶[0092], [0096], [0101]

The preferred embodiment of the handheld mobile communications device 1 incorporates the following components and/or capabilities and/or features, some of which are not shown in the accompanying drawings:

Quad-mode, quad-band CDMA2000 1xEV-DV Cell/PCS+ GSM/GPRS + **A-GPS** + AMPS cellular communications and technology

EX1007 ¶[0081]-[0082]

68. *Walker* explains that A-GPS circuitry enabled handsets can determine their location:

Assisted GPS (A-GPS) enabled handsets provide increased location determination accuracy over pure network based positioning solutions or pure GPS, and support roaming among different countries onto different carrier networks, and into different wireless infrastructures. A single location server on the destination network supports this functionality without the need of any additional infrastructure equipment.

Hybrid (AFLT and A-GPS) technologies improve the speed and accuracy of A-GPS location determination, utilizing signals from both the GPS satellite constellation 11 and from CDMA cell sites 2 and 3, enhancing services availability in addition to shortening the time period involved in location determination, making rapid accurate position location information available in all environments, including large buildings, to an accuracy of 5-50 meters in most environments, enabling position determination in under 6 seconds.

Hybrid positioning technology involves end-to-end, system level position location solutions, providing location server functionality 9 at the infrastructure end of the system and a chipset solution at the mobile station 1. Wide Area Reference Network 10 solutions

consist of an interconnected network of GPS reference receivers and fully redundant communications links connected to data gateways, which then connect to location servers 9 operating positioning software.

Id. ¶[0077]-[0079]

69. And, as noted above, the mobile device calculates “location coordinates” from data obtained by the A-GPS circuitry. *Id.* ¶[0101].

70. Based on my background and experience, a person having ordinary skill in the art would have understood that “location coordinates” are expressed in a latitude and longitude pair, such as in x-y format.

71. *Walker*’s disclosure is consistent with the ’404 patent’s description. The ’404 patent states:

The present invention can obtain location information in a number of different ways, for example through a tower-based location system. As is well known in the art, cell towers triangulate to figure out where a person is. As another example, the present invention can also obtain location information through a form of GPS (Global Positioning System) on the device (GPS or AGPS, which is assisted GPS). Location information for the present invention can be an x-y coordinate or close to it that the phone obtains and transmits to 911.

EX1001, 6:64-7:6

72. Thus, in my opinion, a person having ordinary skill in the art would have understood that data obtained by *Walker*'s A-GPS circuitry and the calculated coordinates are "location data."

73. Accordingly, in my opinion, *Walker* discloses or suggests that the mobile device includes A-GPS circuitry ("a location unit") to obtain data used by the device to calculate location coordinates ("adapted to obtain location data.").

d. 9[c] a transmitting unit, adapted to transmit as emergency information the image data, the audio data, and the location data along with specific information including owner identification information; and

74. In my opinion, *Walker* discloses or suggests "a transmitting unit, adapted to transmit as emergency information the image data, the audio data, and the location data along with specific information including owner identification information."

75. *Walker* discloses that the mobile device includes "cellular communications equipment" for transmitting data via cellular communications protocols and the Internet:

The handheld device includes cellular communications equipment enabling all relevant data to be transmitted in real time, and one or more of each of the following components or

technologies: microprocessor, colour screen, data storage components and device controls.

EX1007 ¶[0054]

The preferred embodiment of the handheld mobile communications device 1 and cellular network 4 includes chipset/s and technology based on the 3G or third generation cellular mobile communications technology CDMA2000 1xEV-DV standard, (1G was analogue cellular, 2G was digital PCS). CDMA stands for Code Division Multiple Access, and 1xEV-DV refers to 1x Evolution-Data & Voice. CDMA2000 1xEV-DV provides near-broadband packet data speeds for wireless access to the Internet, and is an alternative to Wideband CDMA (WCDMA). Both are considered 3G technologies, and this invention can operate with both technologies.

Id. ¶[0065]

76. *Walker* provides a summary of CDMA2000 1xEV-DV and how it is advantageous for *Walker's* system, including because it is optimized for the Internet and incorporates a flexible architecture based on standard Internet Protocols:

CDMA2000 1xEV-DV enables users to always remain on-line and connected to mobile services, meaning that information can be sent or received as needed, without the delay of establishing a dial-up modem connection. ***CDMA2000 1xEV-DV is optimised for the Internet and incorporates a flexible architecture based on standard Internet Protocols (IP).***

The CDMA2000 1xEV-DV standard has been endorsed by both the Third Generation Partnership Project 2 (3GPP2), and by the Telecommunications Industry Association (TIA), and approved by the International Telecommunication Union (ITU) as an IMT-2000 3G global standard.

CDMA2000 1xEV-DV belongs to the CDMA2000 family of standards including CDMA2000 1X and CDMA2000 1xEV-DO, which have previously been recognized by the ITU as 3G technologies.

The CDMA2000 1xEV-DO standard was originally proposed by Nokia, Motorola, Sprint and Texas Instruments as a digital wireless standard enabling dynamic multimedia for mobile communications. The CDMA2000 1xEV-DO standard also provides effective enabling technology for this invention, but provides a less attractive technical solution.

The CDMA2000 1xEV-DV standard offers the flexibility to dynamically balance voice and data traffic by allocating bandwidth on demand, and allows two high-value tasks to be performed simultaneously on a single RF section device. Unlike other CDMA standards such as 1xEV-DO, 1xEV-DV provides integrated voice with simultaneous high-speed packet data services and packet data connection. 1xEV-DV enables real-time streaming video communications, video-conferencing and other multimedia services. CDMA2000 1xEV-DV is backwards compatible with IS-95 and CDMA2000 1X.

Privacy is designed into CDMA. The data bits used to convey real information are mixed with digital coding which is recognised

only by the base station and the mobile terminal. The data appears as unintelligible noise to an eavesdropper.

In an IP-based 1xEV-DV network, radio nodes perform radio frequency processing, baseband modulation/demodulation and packet scheduling. A 1xEV-DV network delivers instantaneous data rates up to 4.8M bit/sec, and takes advantage of off-the-shelf IP equipment such as routers and servers, and uses open standards for network management. Radio nodes installed at a cell site can support hundreds of subscribers. 1xEV-DV networks have the flexibility to support both user and application-level quality of service (QoS). Flexible 1xEV-DV packet schedulers combined with differentiated services-based QoS mechanisms can enable QoS within an entire wireless network.

CDMA2000 1xEV-DV thus provides effective enabling technology for this present invention. Quad-mode, quad-band CDMA2000 1X Cell/PCS + GSM/GPRS + GPS + AMPS technology is presently available, providing a complete solution for full coverage global roaming. A mobile device incorporating such technology may be set to automatically adjust mode of operation to suit the particular network it is operating within.

Id. ¶¶[0066]-[0074]

77. *Walker* also discloses implementing the mobile device with related or alternative technologies for transmitting data. For example, *Walker* discloses that the mobile device includes an aerial, which a person of ordinary skill in the art would have understood to be an antenna:

FIGURE 2 shows the front side of the handheld device 1, incorporating eyewitness button 12, LCD colour screen 13, *aerial 14*, loud speaker or earpiece 15, navigation buttons 16, keypad buttons 17, microphone 18, digital camera with night vision sensitivity 19, and infrared illumination 20.

Walker ¶[0063]

78. *Walker* discloses implementing the mobile device with Bluetooth and/or similar technologies to connect the storage facility:

In another embodiment of the invention the handheld device 1 connects to the data storage facility 7 *through technology known as “Bluetooth” and/or other similar technologies.*

Walker ¶[0140]

The preferred embodiment of the handheld mobile communications device 1 incorporates the following components and/or capabilities and/or features, some of which are not shown in the accompanying drawings:

Quad-mode, quad-band CDMA2000 1xEV-DV Cell/PCS+ GSM/GPRS + A-GPS + AMPS cellular communications and technology enabling the device to receive precise time signals and to transmit and receive packet data and information to and from one or more cellular telecommunications networks 4 and wireless LAN (WLAN) networks including 802.11 WLAN (enabling seamless roaming between private, public, and personal networks), wireless personal area networks (WPANs) connectivity, ... “always connected” network interface, ...

streaming video conferencing, video messaging, picture messaging, text messaging capability, ... voice dialling/calling, ... microprocessor/s, memory chip/s and/or memory card/s and/or memory disc/s and/or hard drive/s and/or magnetic tape/s and/or other digital data storage devices, ... speed dialling, ... three way calling, WAP microbrowser, XHTML browser, Audio/Video/Image coders and decoders, graphics accelerator, hardware accelerator, streaming video ... **USB, Bluetooth, PAN (IPv6), ESDP (Universal Plug and Play over PAN)**, fax/modem, dial-up networking.

Id. ¶¶[0081]-[0082]

79. *Walker* discloses using dial-up networking to connect and transmit the recorded data to the storage facility:

In the event that the handheld device 1 is operating in a network 4 where a dial-up model is involved and/or a successful connection is not achieved between the handheld device 1 and data storage facility 7 at the first dialling attempt, or in the event that a successful transmission from the handheld device 1 to the data storage facility 7 is not achieved, video, sound, positioning and other data are recorded inside ***the handheld device 1 whilst the device automatically and constantly attempts to resend the data or redials a preset number until a connection is made and the data are transmitted***, or until the deactivating code known only to the user is entered or until the device is destroyed, providing that such destruction occurs before a successful connection and transmission is achieved and providing that such destruction

destroys the recorded data stored inside the memory components of the device and not just the communications and recording capabilities of the device 1.

Id. ¶[0103]

In the event that a connection between the handheld device 1 and the data storage facility 7 is lost, ***the handheld device 1 immediately and automatically redials until a new connection is made*** or until the correct deactivation code known only to the user is entered through the keypad 17 by the user. During such interrupted transmissions, images and data are recorded inside the memory components or facilities of the device 1 until a new connection is made between the device 1 and the data storage facility 7 when such data are automatically transmitted to the data storage facility 7. The data recording facility 7 organises all received data according to timeline data so as to provide a continuous and unbroken record of events consistent with a continuous timeline from pressing the eyewitness button.

Id. ¶[0107]

The time involved between pressing the eyewitness button 12 and safely storing images and data at the data storage facility 7 linking an individual to a specific place at a specific time takes no more than a few seconds, providing that a clear connection exists between the device 1 and the cellular network 4 at the time, ***or that a dial-up telephone connection is obtained at the first automatic dialling attempt.***

Id. ¶[0109]

In another embodiment of the invention the handheld device includes technology enabling the device to connect to multiple protocol cellular networks, and includes technology capable of automatically formatting and transmitting data according to each protocol, including CDMA and WCDMA and UTMS and GSM and GPRS and AMPS protocols, *some of which may involve initiating a dial up connection.*

Id. ¶[0159]

80. *Walker* also discloses using email or other electronic messaging services to transmit the recorded data:

In another embodiment of the invention the handheld device 1 transmits recorded data to the data storage facility 7 through a dialup connection or by email or by email attachment or by an electronic messaging service.

Id. ¶[0134]. A person having ordinary skill in the art would have understood the “recorded data” refers to the video, sound, location, and other data recorded by the mobile device, as explained by *Walker* in, for example, paragraphs 103 and 105.

81. This is consistent with how the ’404 patent describes the “transmitting unit.” The ’404 patent describes that the alleged invention may be used with cellular telephones:

The present invention is for use with all mobile devices including, but not limited to, cellular telephones, beepers, pagers, ipods, and Blackberry-type devices.

EX1001, 8:29-31

82. The '404 patent also describes using various communication protocols to transmit the data such as TCP/IP, MMS, and e-mail:

The present invention in one embodiment communicates the emergency information (image information, location information, owner information, etc.) ***through a TCP/IP (Transmission Control Protocol/internet Protocol) connection*** on the phone or mobile device, or through another such as WAP (Wireless Application Protocol). TCP/IP is a communications protocol that is used to connect hosts on the Internet, and TCP/IP is the de facto standard for transmitting data over networks. ***The present invention may also use an MMS (Multimedia Message Service) system***, which is a mix between internet protocol and e-mail protocol. More specifically, MMS is a store-and-forward method of transmitting graphics, video clips, sound files, and short text messages over wireless networks using WAP. MMS implementations also support e-mail addressing, so that the device can send e-mails directly to an e-mail address. The presentation of the MMS message is coded into the presentation file so that images, sounds, and text are displayed in a predetermined order as one singular message. The most common use of MMS is for communication between mobile phones/devices. MMS is one method enabling the present invention to obtain video/audio

information and send the data to a specified location. *Of course, the present invention is not limited to using protocols such as TCP/IP and MMS.*

To expand upon this further, there are a number of ways to send image data and audio data using the present invention. *As one example, image data can be sent through regular e-mail to a dispatching center and then to a police station.* As another example, image data can be sent through a *picture-based e-mail type system* (such as MMS). *As another example, image data can be sent through a regular TCP/IP to a web service, which enables internet access on a cell phone.* Of course, the present invention is not limited to these examples, and various modifications are envisioned.

Id., 6:20-53.

83. A person having ordinary skill in the art would have understood that cellular telephones have cellular communications equipment, and that TCP/IP is a standard Internet protocol.

84. In view of the above, in my opinion, a person having ordinary skill in the art would have understood *Walker* to disclose or suggest a “transmitting unit.”

85. *Walker* also discloses that the mobile device transmits video, sound, and location coordinates:

The preferred embodiment enables the device to be used in both daylight and dark conditions. For illustration purposes the

following assumes that the invention is activated by the user in dark conditions. On pressing the eyewitness button 12 a series of automatic parallel or sequential actions are instantly initiated:

...

6) *The device begins transmitting ongoing streaming video and sound data and other data to the data storage facility 7* where compatible recording equipment is permanently on standby to receive, record and log the automatic transmission of mission critical data from the handheld device 1 in real time. The video data transmitted are simultaneously displayed on the device screen 13, enabling the user to monitor what video data are being transmitted.

...

8) Within 6 seconds of pressing the eyewitness button 12 the hybrid A-GPS circuitry obtains sufficient data from the satellite constellation 11 and cellular network 4. From such data the location coordinates are calculated. *The calculation is performed by the handheld device 1 or network 4 and the coordinates are immediately transmitted to the data storage facility 7, integrated with the continuing video stream, sound data and other data.* As the transmission of video and sound and other data continues, hybrid AGPS data are regularly updated and transmitted to the data storage facility 7.

EX1007 ¶¶[0092], [0099], [0101]

In the event that the handheld device 1 is operating in a network 4 where a dial-up model is involved and/or a successful connection

is not achieved between the handheld device 1 and data storage facility 7 at the first dialling attempt, or in the event that a successful transmission from the handheld device 1 to the data storage facility 7 is not achieved, ***video, sound, positioning and other data are recorded inside the handheld device 1 whilst the device automatically and constantly attempts to resend the data or redials a preset number until a connection is made and the data are transmitted***, or until the deactivating code known only to the user is entered or until the device is destroyed, providing that such destruction occurs before a successful connection and transmission is achieved and providing that such destruction destroys the recorded data stored inside the memory components of the device and not just the communications and recording capabilities of the device 1.

Id. ¶[0103]

86. *Walker* discloses that the audio, video, and location data are used to inform others of a crime or when the user is being attacked:

Personal safety and security is a key issue for all people and particularly for women, children, the elderly and disabled persons. ***Individuals are particularly vulnerable to attack when they become isolated by location or circumstance from other people. In such situations criminals often feel confident that their identity will not be discovered in committing a crime against a person, with no eyewitnesses at the scene other than the victim.*** In such circumstances assault, intimidation, harassment, rape,

murder, robbery, blackmail and other such serious crimes against the individual frequently occur.

EX1007 ¶[0021]

A cellular hand held mobile communications device and external data storage system, intended to enhance personal safety and security, acting as an electronic eyewitness, helping to deter criminal activity and to reduce the incidence of crime. ***Where crime is committed, the invention assists authorities and security services in obtaining evidence linking the identities of criminals to their crimes.*** The areas involved include 3G wireless electronic mobile communications, cellular telecommunication networks and infrastructure, data networks and data storage, electronic and wireless protocols, digital camera devices, storage of digital data, hybrid positioning (AFLT and Wireless A-GPS) technologies, odour and chemical profiling, electronic sensors, burglar alarms, personal and public safety, crime prevention and detection. ***The invention is a collaborative approach to these areas, providing a means of reducing the incidence of intimidation, bullying and victimisation, and particularly crimes of violence against individuals or crimes which can lead to violence.*** The invention additionally provides a means of reducing property theft and mobile phone theft.

Id. at Abstract

The present invention may be used, for example, by a girl walking through a secluded park in the event that she is approached by a suspicious man. ***In such a circumstance, the girl simply presses***

the recessed eyewitness button on her mobile communications handheld device as soon as she begins to feel uncomfortable in the presence of the man. She holds the device as if to make a call or check some personal information stored in her phone, thereby not raising any suspicions, but ensuring that an integral camera is pointing in the direction of the suspicious man.

The girl immediately sees an image of the man appear on the screen of her device and knows that streaming video and sound and geographical and timeline data is immediately being transmitted to an external data storage facility, without any dialup delay, where it will be safely recorded and stored in real time. She also knows that even if the man subsequently destroys the device, his image and behaviour will remain stored at the data storage facility together with sound, geographic coordinates and the precise timeline of the encounter, linking him to her at that specific location and at that specific time. ...

Any member of the public having this invention in their possession and witnessing a crime may discretely transmit sound and images and environmental data relating to the incident at the press of the eyewitness button, for later analysis by police.

Should a mugger snatch a woman's handbag in a crowded street and run, any member of the public in possession of this invention seeing the mugger escaping may simply press the eyewitness button and transmit the incident as it happens, in real time. Should the criminal snatch the device and destroy it, the information will remain, recorded and logged at the data storage facility, and depending on which version of this invention the user is in

possession of, the criminal's odour and fingerprints may additionally be captured and transmitted on snatching the device, before the criminal has a chance to destroy the device.

Police and security services may potentially access databases held by data storage facilities when seeking evidence in connection with crimes, by entering a time and location of a crime into the database application holding or accessing all data recorded by the appropriate data storage facility. Central databases and/or applications may be created, linking and combining the data of all data storage facilities within a certain region or jurisdiction. Authorities may potentially access any recordings made within a selected range of distances of a particular location and within a selected range of times. Through such access, authorities will be able to increase the probabilities of linking guilty criminals to their crimes and of identifying witnesses to crimes.

Id. ¶¶[0043]-[0049]

87. A person having ordinary skill in the art would have therefore understood that the transmitted image, audio, and location data therefore related to an ongoing emergency, and that this is consistent with how the '404 patent describes “emergency information”:

The present invention in one embodiment communicates the emergency information (image information, location information, owner information, etc.

EX1001, 6:20-23

In this way, the present invention utilizes a built-in camera to take image(s) of the attacker and send the specific information to the authorities along with the image information and audio information. ...

The present invention integrates with mobile phones/devices to send image data of the attack, which could be either still image data or moving video, along with location information, and/or audio information, so that help can be dispatched right away. The system can be linked in with an emergency assistance number such as 911 or to a private emergency network specifically set up for these purposes to work with the public authorities in assisting victims. By virtue of the features of the present invention, authorities will be able to proceed directly to the location of the incident, equipped with specific information such as location information, image and/or audio data of the attack (which can of course aid in identifying the perpetrator), and information as to who owns the mobile phone/device including a description of that person. Audio data (either a pre-recorded help message or audio of the attack itself) can also be sent to the authorities.

Id. 5:34-59

88. Thus, a person having ordinary skill in the art would have understood *Walker* to disclose or suggest that the mobile device transmitting unit is “adapted to transmit as emergency information the image data, the audio data, and the location data.”

89. *Walker* also discloses that when the emergency button is pressed, the remote data storage facility creates a file that is linked with the “device owner’s identity”:

On pressing the eyewitness button 12 a series of automatic parallel or sequential actions are instantly initiated:

...

4)The handheld device 1 communicates with the data storage facility 7 through the "always connected" wireless connection to the cellular network 4, which enables the device 1 to push data without requiring the user to establish a dial-up session, and transmits the time as displayed by the handheld device 1 to the data storage facility 7. ***The data storage facility 7 creates a unique electronic file to hold all data recorded during the call into this unique file. A new file is created for each new call received by the data storage facility 7. A database link between each file and the device owner's identity or account is made, enabling the device owner and the data storage facility 7 to lookup and access files in the future which have previously been recorded by the device owner.***

EX1007 ¶¶[0092], [0097]

Once the data storage facility 7 has received and recorded the data stored in the memory components of the handheld device 1, ***the data storage facility 7 continues to record all images, sounds and other live signals detected and transmitted by the handheld***

device 1 in real time, for as long as the connection between the handheld device 1 and the data storage facility 7 is maintained.

Id. ¶[0106]

90. Based on that, a person having ordinary skill in the art would have understood *Walker* to disclose the mobile device transmitting information to identify the device owner (“owner identification information”).

91. If Patent Owner argues or the Board finds that *Walker* does not disclose transmitting owner identification information, then, at a minimum, a person having ordinary skill in the art would have found it obvious to modify *Walker* to transmit information to identify the device owner.

92. As I described above, *Walker* discloses that the remote data storage facility creates a file linked with the “device owner’s identity” to record the data transmitted from the mobile device.

93. *Walker* is also concerned with the device owner’s identity because *Walker* discloses that the invention is meant to help identify the individuals at the scene of a crime or other event by, for example, enabling the police to “locate all individuals who activate this function”:

The present invention relates to a cellular handheld mobile communications device and external data storage system, and is intended to enhance personal safety and security, *acting as an electronic eyewitness, helping to deter criminal activity and to reduce the incidence of crime. Where crime is committed, the*

invention assists authorities and security services in obtaining evidence linking the identities of criminals to their crimes.

EX1007 ¶[0001]

The invention thus provides a strong deterrent to criminal activity, increasing both personal and public safety through acting as a digital mobile eyewitness and crime prevention tool, *linking the identity and behaviour of a recorded individual or individuals to a specific place at a specific time and to the physical presence of the user at the location at that time*, within moments of pressing the eyewitness button.

The present invention additionally enables police to access all such recordings made by any individuals in possession of this mobile communications handheld device at or near the scene of a crime, thereby aiding the collection of evidence in connection with crimes. *The invention additionally enables police to locate all individuals who activate this function of the device, within a selected range of times and distances of any crime scene, thereby aiding police in locating and interviewing potential witnesses to a crime. The location of users is only recorded and made accessible to police on pressing the eyewitness button of the device.* When the device is used in it's [sic] normal capacity as a handheld mobile communications device the whereabouts of the user is not tracked, unless the user opts in to additional services and activates an automatic tracking function.

Id. ¶¶[0040]-[0041]

The present invention may be used, for example, by a girl walking through a secluded park in the event that she is approached by a suspicious man. In such a circumstance, the girl simply presses the recessed eyewitness button on her mobile communications handheld device as soon as she begins to feel uncomfortable in the presence of the man. She holds the device as if to make a call or check some personal information stored in her phone, thereby not raising any suspicions, but ensuring that an integral camera is pointing in the direction of the suspicious man.

Id. ¶[0043]

Any member of the public having this invention in their possession and witnessing a crime may discretely transmit sound and images and environmental data relating to the incident at the press of the eyewitness button, for later analysis by police. Should a mugger snatch a woman's handbag in a crowded street and run, any member of the public in possession of this invention seeing the mugger escaping may simply press the eyewitness button and transmit the incident as it happens, in real time.

Should the criminal snatch the device and destroy it, the information will remain, recorded and logged at the data storage facility, and depending on which version of this invention the user is in possession of, the criminal's odour and fingerprints may additionally be captured and transmitted on snatching the device, before the criminal has a chance to destroy the device.

Police and security services may potentially access databases held by data storage facilities when seeking evidence in connection

with crimes, by entering a time and location of a crime into the database application holding or accessing all data recorded by the appropriate data storage facility. Central databases and/or applications may be created, linking and combining the data of all data storage facilities within a certain region or jurisdiction. Authorities may potentially access any recordings made within a selected range of distances of a particular location and within a selected range of times. ***Through such access, authorities will be able to increase the probabilities of linking guilty criminals to their crimes and of identifying witnesses to crimes.***

Id. ¶¶ [0048]-[0049].

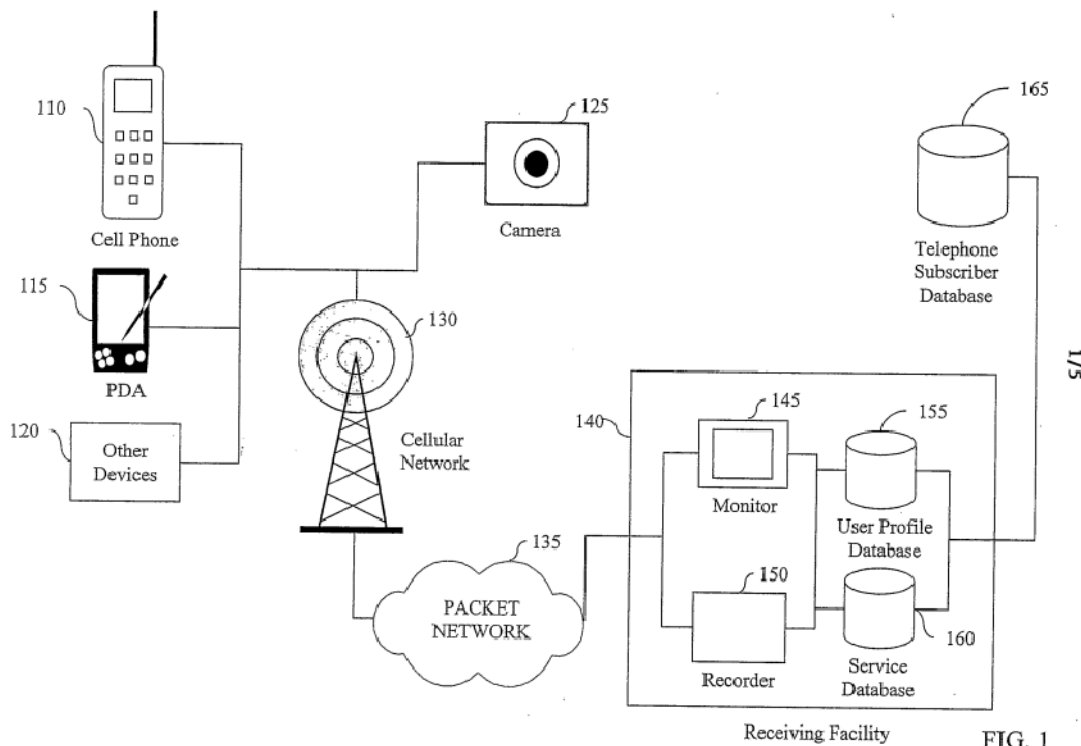
94. These disclosures are at least an express suggestion to transmit information to identify the owner of the device. A person having ordinary skill in the art would have understood that transmitting the owner identification information would have allowed the remote storage facility to link the recorded information with the device owner's identity and would have advanced *Walker's* objective to identify individuals present at the scene of the emergency described by the image, audio, and location data.

95. A person having ordinary skill in the art would have had a reasonable expectation of success in modifying *Walker* to transmit information to identify the owner to accomplish *Walker's* objectives because techniques for doing so were well-known.

96. For example, *Chang*, which is listed on the last page of *Walker*, describes a system similar to the '404 patent and *Walker*. *Chang* discloses a “video-capture device (125), connected to a wireless communication device (130)” and transmitting captured audio and images to a “receiving facility,” such as a “security office.”

A method and system for recording a digital video image is described. An embodiment of the present invention includes a video-capture device (125), connected to a wireless-communication device (130). ***The wireless-communication device transmits images captured by the real-time video-capture device to a receiving facility (140) via a communications network. The receiving facility may compromise, for example, a security office.*** The receiving facility processes the images, monitoring, storing, forwarding and deleting the images as necessary.

EX1012, Abstract.



Chang, FIG. 1

97. *Chang* discloses that it is advantageous to identify the user transmitting the video image. For that purpose, *Chang*'s system includes a "user-identification device," which may comprise the "wireless-communication device" or a "smart card." *Id.*, 3:6-14. *Chang* discloses including "user-identification information with the transmitted video signal" and that a "subscriber identity module" in the device may be used to store user-specific information. *Id.*, 11:1-7. When the "receiving facility receives the images, the receiving facility processes the images. As part of the processing, the receiving facility links the images to the user identified in the transmission. To accomplish

linking, the receiving facility may use a user-profile database.” *Id.*, 3:15-22. The user-identification information, such as the user’s wireless-handset number, “is used to retrieve user-profile information from the user-profile database” such as the user’s home address. *Id.*, 12:13-18. Figure 3A, shown below, illustrates how user-identification information is added to the transmission of audio/video data. To note, while *Chang*’s description focuses on “user” identification data, a person having ordinary skill in the art would have understood that the same techniques would be applicable to “owner” identification information, particularly as the “user” would, in practice, often be the device owner.

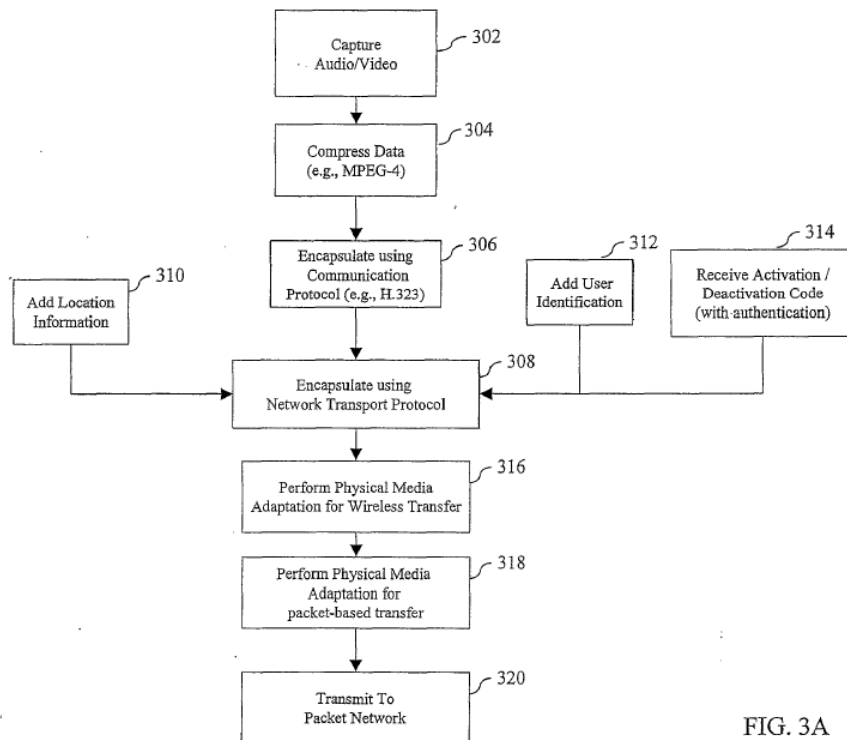


FIG. 3A

Chang, Fig. 3A

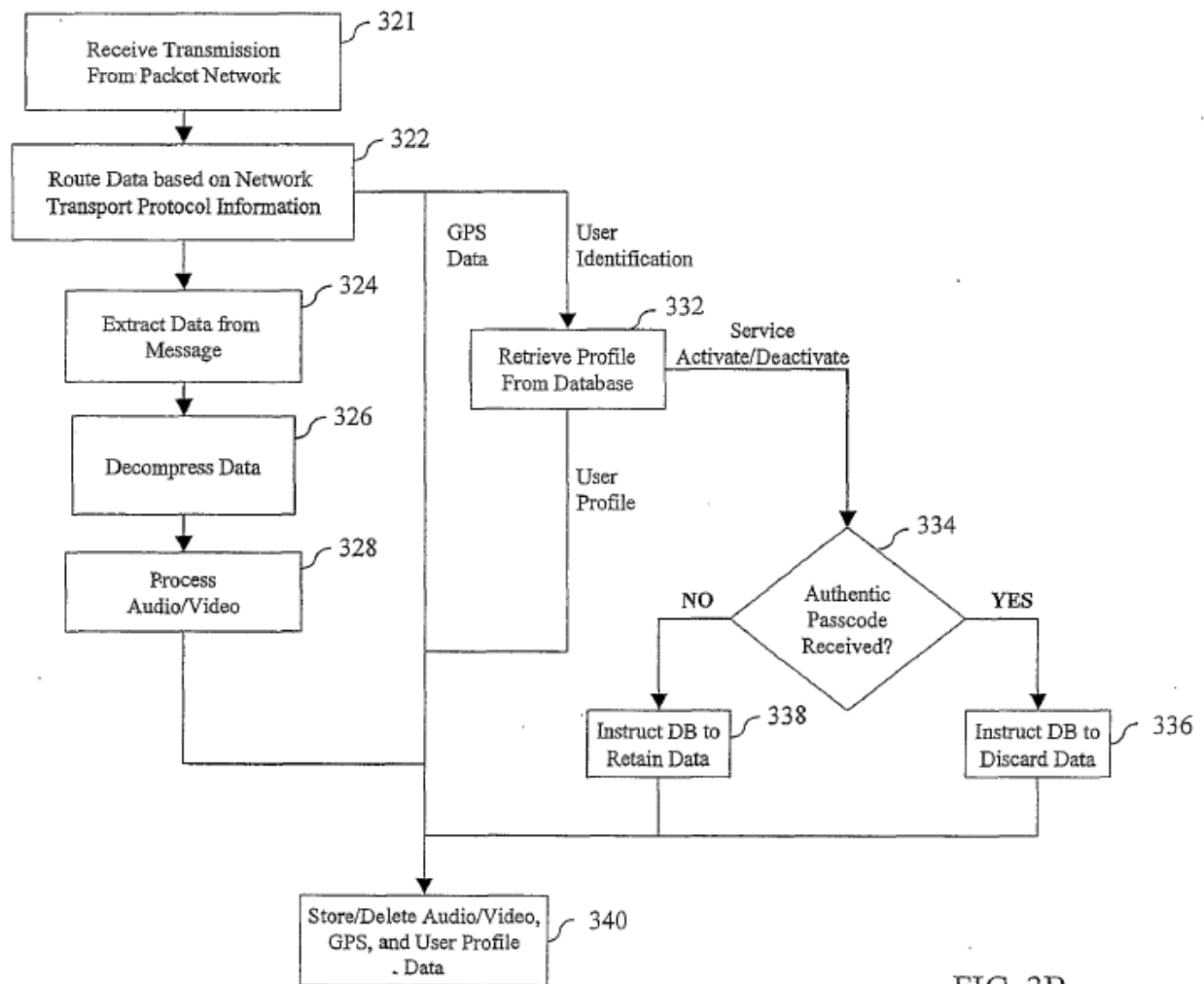


FIG. 3B

Chang, FIG. 3B

98. A person having ordinary skill in the art would have further understood *Walker* to disclose or suggest that the owner identification information is transmitted in a manner that associates it with the transmitted image, audio, and location data because that is how a person of ordinary skill in the art would have understood the storage facility could link the transmitted data to the owner's identity and appropriately notify emergency services.

99. For example, as I've described above, *Walker* discloses that the steps of creating the owner-identity linked file and transmitting the video, sound, and location data are initiated automatically and in parallel in response to the press of the eyewitness button:

On pressing the eyewitness button 12 a series of automatic parallel or sequential actions are instantly initiated:

...

4)The handheld device 1 communicates with the data storage facility 7 through the "always connected" wireless connection to the cellular network 4, which enables the device 1 to push data without requiring the user to establish a dial-up session, and transmits the time as displayed by the handheld device 1 to the data storage facility 7. ***The data storage facility 7 creates a unique electronic file to hold all data recorded during the call into this unique file. A new file is created for each new call received by the data storage facility 7. A database link between each file and the device owner's identity or account is made, enabling the device owner and the data storage facility 7 to lookup and access files in the future which have previously been recorded by the device owner.***

...

6) ***The device begins transmitting ongoing streaming video and sound data and other data to the data storage facility 7*** where compatible recording equipment is permanently on standby to receive, record and log the automatic transmission of mission

critical data from the handheld device 1 in real time. The video data transmitted are simultaneously displayed on the device screen 13, enabling the user to monitor what video data are being transmitted.

...

8) Within 6 seconds of pressing the eyewitness button 12 the hybrid A-GPS circuitry obtains sufficient data from the satellite constellation 11 and cellular network 4. From such data the location coordinates are calculated. The calculation is performed by the handheld device 1 or network 4 ***and the coordinates are immediately transmitted to the data storage facility 7, integrated with the continuing video stream, sound data and other data. As the transmission of video and sound and other data continues, hybrid A-GPS data are regularly updated and transmitted to the data storage facility 7.***

...

In the event that the handheld device 1 is operating in a network 4 where a dial-up model is involved and/or a successful connection is not achieved between the handheld device 1 and data storage facility 7 at the first dialling attempt, or in the event that a successful transmission from the handheld device 1 to the data storage facility 7 is not achieved, ***video, sound, positioning and other data are recorded inside the handheld device 1 whilst the device automatically and constantly attempts to resend the data or redials a preset number until a connection is made and the data are transmitted,*** or until the deactivating code known only to the user is entered or until the device is destroyed, providing that

such destruction occurs before a successful connection and transmission is achieved and providing that such destruction destroys the recorded data stored inside the memory components of the device and not just the communications and recording capabilities of the device 1.

...

Once a successful connection is made between the handheld device 1 and the data storage facility 7, the recorded images, sound, geographical coordinates detailing the location of the device 1, and timestamp generated by the handheld device 1 against the recordings, and other data stored in the memory chips and/or memory cards and/or memory discs and/or hard drives, and/or tapes and/or other data storage facilities of the handheld device 1 are immediately and automatically transmitted by the handheld device 1 to the data storage facility 7 for safe storage.

EX1007 ¶¶[0092]-[0105].

The time involved between pressing the eyewitness button 12 and safely storing images and data at the data storage facility 7 linking an individual to a specific place at a specific time takes no more than a few seconds, providing that a clear connection exists between the device 1 and the cellular network 4 at the time, or that a dial-up telephone connection is obtained at the first automatic dialling attempt.

Id. ¶[0109].

100. Thus, a person having ordinary skill in the art would have understood that, at a minimum, the device owner identity information was transmitted in parallel or close in time to the video, sound, and location data.

101. This is consistent with how the '404 patent describes transmitting emergency information "along with" specific information so that help can be dispatched right away and the authorities will be "equipped with specific information such as location information, image and/or audio data of the attack (which can of course aid in identifying the perpetrator), and information as to who owns the mobile phone/device including a description of that person":

In another embodiment, the present invention provides a self-defense device including a self-defense mechanism which is integrated with a mobile phone/device such that when the self-defense mechanism is activated, a camera built into the mobile phone/device takes an image of the attacker, and *the mobile phone/device sends image data and audio data to the authorities along with specific information such as, for example, the name and description of the owner of the self-defense device, location information, a time and date stamp, etc.* In this way, the present invention utilizes a built-in camera to take still or moving images of the attacker and send the image and/or audio data to the authorities along with the specific information. The self-defense mechanism can be a vial containing pepper spray or mace, for example, or simply a separate panic button located on the device

which activates the above-mentioned processes. Of course, the present invention is not limited to the examples discussed herein. The present invention integrates with mobile phones/devices to send image data of the attack, which could be either still image data or moving video, along with location information, and/or audio information, *so that help can be dispatched right away*. The system can be linked in with an emergency assistance number such as 911 or to a private emergency network specifically set up for these purposes to work with the public authorities in assisting victims. *By virtue of the features of the present invention, authorities will be able to proceed directly to the location of the incident, equipped with specific information such as location information, image and/or audio data of the attack (which can of course aid in identifying the perpetrator), and information as to who owns the mobile phone/device including a description of that person*. Audio data (either a pre-recorded help message or audio of the attack itself) can also be sent to the authorities.

EX1001, 5:24-57

102. Thus, in my opinion, a person having ordinary skill in the art would have understood *Walker* to disclose or suggest transmitting image, audio, and location data “along with” owner identification information.

103. Accordingly, *Walker* discloses or suggests a mobile device with cellular communications equipment and various additional or alternative transmission technologies (a “transmitting unit”) to transmit image, audio, and

location data in emergencies (“adapted to transmit as emergency information the image data, the audio data, and the location data”) in addition to information to identify the owner of the device so that it could be linked at the storage facility and provided to emergency services (“along with specific information including owner identification information”).

e. **9[d] & 9[e]**

(i) “a panic button ... wherein the panic button is activated by a series of depressings of the panic button”

104. In my opinion, *Walker* in combination with *Kim* discloses or suggests “a panic button ... wherein the panic button is activated by a series of depressings of the panic button.”

105. *Walker* discloses that the handheld mobile device includes an “eyewitness button 12” and that when it is pressed once (which could be during an attack), initiates various operations including collecting and transmitting information about the attack:

On pressing the eyewitness button 12 a series of automatic parallel or sequential actions are instantly initiated:

...

4)The handheld device 1 communicates with the data storage facility 7 through the "always connected" wireless connection to the cellular network 4, which enables the device 1 to push data without requiring the user to establish a dial-up session, and

transmits the time as displayed by the handheld device 1 to the data storage facility 7. The data storage facility 7 creates a unique electronic file to hold all data recorded during the call into this unique file. A new file is created for each new call received by the data storage facility 7. A database link between each file and the device owner's identity or account is made, enabling the device owner and the data storage facility 7 to lookup and access files in the future which have previously been recorded by the device owner.

...

6) *The device begins transmitting ongoing streaming video and sound data and other data to the data storage facility 7* where compatible recording equipment is permanently on standby to receive, record and log the automatic transmission of mission critical data from the handheld device 1 in real time. The video data transmitted are simultaneously displayed on the device screen 13, enabling the user to monitor what video data are being transmitted.

...

8) Within 6 seconds of pressing the eyewitness button 12 the hybrid A-GPS circuitry obtains sufficient data from the satellite constellation 11 and cellular network 4. From such data the location coordinates are calculated. The calculation is performed by the handheld device 1 or network 4 *and the coordinates are immediately transmitted to the data storage facility 7, integrated with the continuing video stream, sound data and other data. As the transmission of video and sound and other data continues,*

hybrid A-GPS data are regularly updated and transmitted to the data storage facility 7.

...

In the event that the handheld device 1 is operating in a network 4 where a dial-up model is involved and/or a successful connection is not achieved between the handheld device 1 and data storage facility 7 at the first dialling attempt, or in the event that a successful transmission from the handheld device 1 to the data storage facility 7 is not achieved, video, sound, positioning and other data are recorded inside the handheld device 1 whilst the device automatically and constantly attempts to resend the data or redials a preset number until a connection is made and the data are transmitted, or until the deactivating code known only to the user is entered or until the device is destroyed, providing that such destruction occurs before a successful connection and transmission is achieved and providing that such destruction destroys the recorded data stored inside the memory components of the device and not just the communications and recording capabilities of the device 1.

...

Once a successful connection is made between the handheld device 1 and the data storage facility 7, the recorded images, sound, geographical coordinates detailing the location of the device 1, and timestamp generated by the handheld device 1 against the recordings, and other data stored in the memory chips and/or memory cards and/or memory discs and/or hard drives, and/or tapes and/or other data storage facilities of the handheld

device 1 are immediately and automatically transmitted by the handheld device 1 to the data storage facility 7 for safe storage.

EX1007 ¶¶[0092]-[0105].

106. A person having ordinary skill in the art would have understood that Walker's eyewitness button 12 is consistent with how the '404 patent describes the claimed "panic button." The '404 patent describes a "separate panic button located on the device" such as "panic button 20":

The self-defense mechanism can be a vial containing pepper spray or mace, for example, or simply a separate panic button located on the device which activates the above-mentioned processes. Of course, the present invention is not limited to the examples discussed herein.

EX1001, 3:16-21

The self-defense mechanism can be, for example, a vial containing pepper spray or mace, a personal alarm, a stun gun, a stench ointment, or the like. Further, the self-defense mechanism can be a separate panic button located on the device which activates the above-mentioned processes.

Id., 5:37-42.

Panic button 20 is included in this embodiment.

Id., 8:2-3

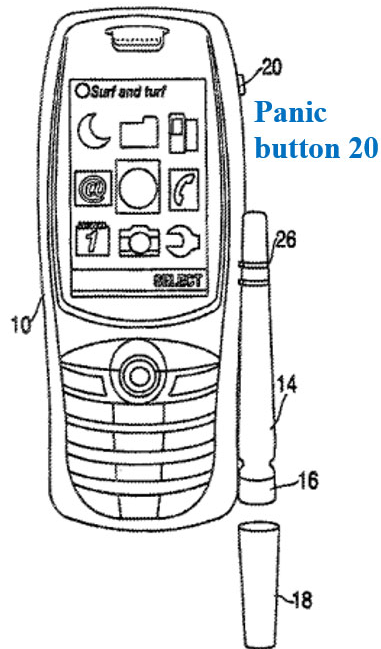


FIG. 2A

EX1001, FIG. 2A (annotated)

107. A person having ordinary skill in the art would have understood the “panic button” was a dedicated button with a panic function (as opposed to a button with multiple functions), for example, because the ’404 patent describes that it may be activated with a single press. A person having ordinary skill in the art would have understood that the single press indicates a dedicated button because it assumes that there is no other function that the button performs if it is only pressed once. In addition, the ’404 patent does not attribute any non-panic related functions to it (for example, that it also functions as a digit key for dialing phone number). Similarly, *Walker* does not ascribe any non-panic-related

functions to the eyewitness button 12 and, accordingly, a person having ordinary skill in the art would therefore have understood it to be a dedicated button.

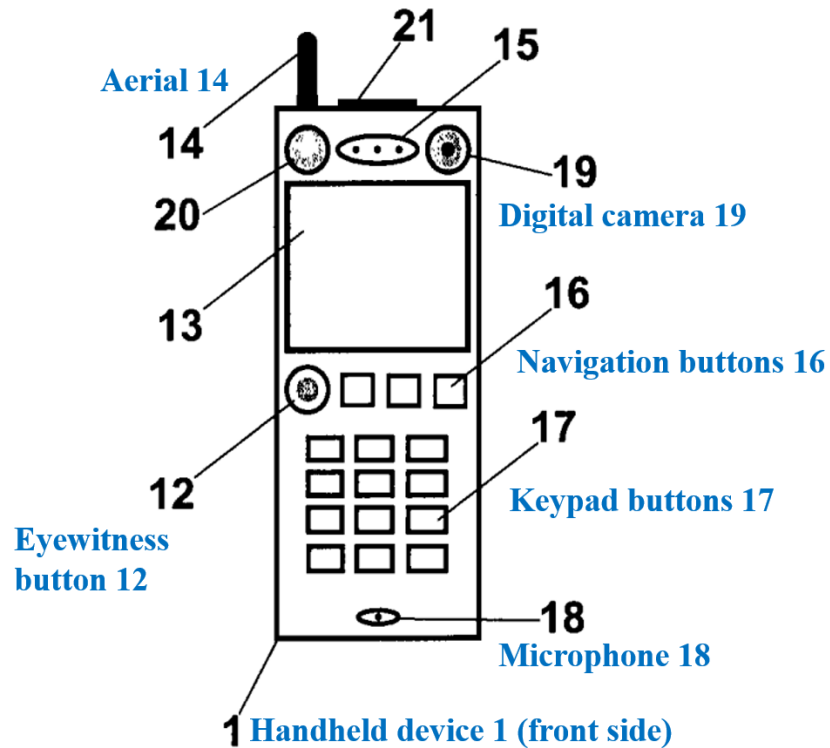
108. *Walker* describes the “eyewitness button 12” as “recessed and set to operate at a higher finger pressure than other buttons on the device so as to minimise [*sic*] the occurrence of accidental activation:”

The preferred embodiment of the handheld mobile communications device 1 incorporates the following components and/or capabilities and/or features, some of which are not shown in the accompanying drawings:

...

The eyewitness button 12 is recessed and set to operate at a higher finger pressure than other buttons on the device so as to minimise the occurrence of accidental activation.

Id. ¶¶[0081], [0083]



Walker, FIG. 2 (annotated)

109. A person having ordinary skill in the art would have understood that there were other known ways to design a panic button to minimize the occurrence of accidental activation.

110. For example, *Kim* is similar to the '404 patent and *Walker*. *Kim* generally discloses “[a]n apparatus for processing an emergency call using a mobile communication network” with a method “to transmit emergency information to an emergency contact with a simple manipulation of a button on a mobile phone handset”:

An apparatus for processing an emergency call using a mobile communication network and a method thereof configured to

transmit emergency information to an emergency contact with a simple manipulation of a button on a mobile phone handset to thereby enable to advise an emergency situation and to maintain security by way of switch to mute/no-light modes, the apparatus comprising: an emergency function input unit for performing an input function for notifying an emergency situation that occurs to a subscriber of a relevant mobile phone handset; a memory unit stored with telephone number information of an emergency contact to be notified of the emergency situation according to the input function of the emergency function input unit, and emergency information equipped with notification contents of the emergency situation; and a controller for executing an emergency mode according to the input function of the emergency function input unit to make a call connection with the emergency contact, and transmitting the emergency information contained in the memory unit to the emergency contact, and executing a wire-tapping mode according to the emergency transmission from the emergency contact to prohibit reception of voice signals from the receiving unit and to allow only the voice to be transmitted via the transmitting unit.

EX1010 at Abstract.

111. *Kim* discloses a mobile phone with an emergency key button 32 mounted on an external lateral surface of the phone:

In other words, as illustrated in Figure 3a, the key pad 30 includes a communication key button 30a for forming a communication route in order to make it possible to communicate via voice with a

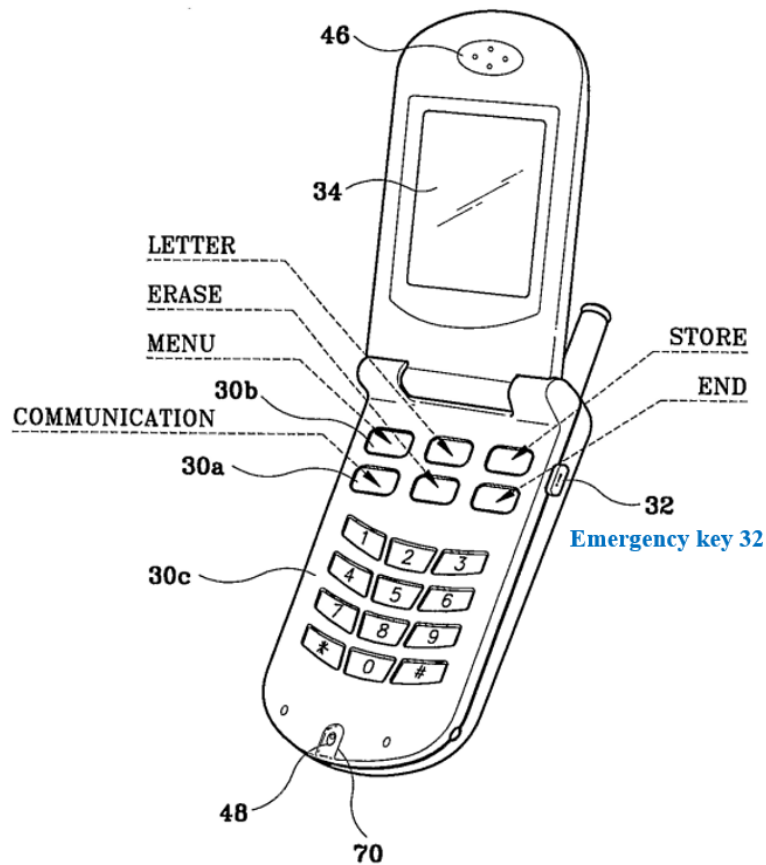
controller at an emergency contact office by releasing a wire-tapping mode under an emergency mode, a menu key button 30b for performing a set-up manipulation for releasing an emergency mode, and a number key button 30c for inputting a predetermined secret number in order to release an emergency mode, *where the emergency key button 32 is mounted at an external lateral surface of a related mobile phone handset 2 for a mobile phone subscriber to easily manipulate same under emergency situations.*

Id., 9:2-11.

FIGs. 3a and 3b are schematic drawings of the exterior of a mobile phone handset where an emergency call processing apparatus is applied according to an embodiment of the present invention;

Id., 4:24-26

FIG.3a



Kim FIG. 3a (annotated)

112. The emergency key button 32 “executes an emergency mode for notifying an emergency state by way of button manipulation”:

Furthermore, the emergency key button 32 executes an emergency mode for notifying an emergency state by way of button manipulation by a mobile phone subscriber while a stand-by power is received regardless of the power on/off state of a related mobile phone 2 handset. It is preferable to execute the emergency mode by continuous manipulation of the related

emergency key button 32 for over a few seconds, e.g., over 3 seconds.

Id., 8:22-9:1

When a call connection with the emergency information control server 12 of an emergency contact is implemented according to the execution of the emergency mode, the controller 60 processes the emergency information stored at the memory 58 by way of ***short messages to send same to the emergency information control server 12 via the transmitter 42*** and the duplexer 38.

At this time, although the controller 60 is allowed to execute the emergency mode according to the manipulation of the emergency key button 32 for a few seconds continuously, e.g., three seconds, it should be apparent that the emergency mode may be allowed to be executed if the related emergency key button 32 is manipulated a plurality of times, e.g., three times, within a set period of time.

Id., 12:22-13:6

When a user of a mobile phone handset 2 is being assailed by a robber, is confined in a bounded area against his or her will, is being chased, is being attacked in a house by a burglar, or is distressed in a mountainous area, the user may ***simply manipulate an emergency key button disposed on the handset which transmits emergency information*** intrinsically stored therein to an emergency contact such as a police station, fire station or dispatcher via a mobile communication network.

Id., 5:16-22.

113. A person having ordinary skill in the art would have understood that *Kim*'s emergency key button is similar to *Walker*'s eyewitness button 12 insofar as it is a dedicated button, but unlike *Walker*'s eyewitness button 12, *Kim* does not describe the emergency key button 32 as recessed, or that it is set to operate at a higher finger pressure than other buttons. It is also different from the eyewitness button 12 because of instead of requiring a single press, the user executes *Kim*'s emergency mode when the "emergency key button 32 is manipulated a plurality of times, e.g., three times, within a set period of time":

At this time, although the controller 60 is allowed to execute the emergency mode according to the manipulation of the emergency key button 32 for a few seconds continuously, e.g., three seconds, ***it should be apparent that the emergency mode may be allowed to be executed if the related emergency key button 32 is manipulated a plurality of times, e.g., three times, within a set period of time.***

Id., 13:1-6.

114. *Kim*'s disclosure related to emergency key button 32 is consistent with how the '404 patent describes a panic button that is activated by a series of presses.

115. The '404 patent also describes that "the panic button may be activated by ... a depressing or series of depressions of the panic button." *Id.*, 3:60-62. A person having ordinary skill in the art would have understood that in

the '404 patent, a “series of depressions” means more than one depression because the '404 patent describes activating the panic button by a “depressing or series of depressions.” *Id.* Because the '404 patent describes using a single “depressing” or alternatively a “series of depressions,” a person having ordinary skill in the art would have understood the '404 patent to distinguish between a single “depressing” and a “series of depressions.” That meaning is also consistent with how a person of ordinary skill in the art would have understood the term “series.” The Wiley 2004 dictionary, for example, defines “series” as “an arrangement of two or more related things, entities, or events, in a given order” or “in a successive order.” EX1023. This is consistent with how *Kim* describes that the emergency key button 32 is manipulated a plurality of times, e.g., three times, to execute the emergency mode.

116. Therefore, in my opinion, a person having ordinary skill in the art would have understood *Kim* to disclose or suggest that the emergency key button 32 is activated to trigger the emergency mode by being manipulated, i.e., pressed, a plurality (e.g., three) times.

117. In my opinion, a person having ordinary skill in the art would have been motivated to combine *Walker* and *Kim* and would have considered it obvious to substitute *Kim*'s dedicated emergency key button that requires being manipulated a plurality of times (e.g., three times) for *Walker*'s recessed

eyewitness button requiring a higher finger pressure to initiate *Walker's* collection and transmission of data. The combination discloses or suggests a mobile device with a dedicated emergency key button that, when pressed a plurality of times (e.g., three times), triggers a series of operations, including *Walker's* collection and transmission of data.

118. A person having ordinary skill in the art would have appreciated that *Kim's* emergency key button serves the same purpose as *Walker's* eyewitness button. They are both used to trigger transmission of information from a mobile device related to an emergency, and a person having ordinary skill in the art would have understood that *Kim's* technique of requiring the emergency key button to be pressed a plurality of times (e.g., three times) serves the same purpose to minimize accidental activation as implementing *Walker's* eyewitness button in a recessed fashion and setting it to operate at a higher finger pressure.

119. *Kim* does not expressly describe that the purpose of requiring the user to manipulate or press the emergency key button a plurality of times (e.g., three times) within a time period was for the purpose of reducing accidental or false activations, but a person having ordinary skill in the art would have understood that to be the reason for *Kim's* design in this regard. It was well-known in the art that reducing the incidence of false or accidental activations

was important, and that one way of doing so was to design the system to require the panic button to be pressed more than once.

120. For example, the *Wade* reference, published in 2003, discloses “[a]n improved emergency communications system which provides voice communication between an emergency caller 27 and the 911 emergency response operator 28 through either a base station unit 38 or a wireless remote personal pendant 40.” EX1016 at Abstract. The “wireless pendent 40” has “automatic dialing call and voice capability that is in radio frequency communication with a base unit 38, wherein the base unit 38 can have automatic dialing call and voice capability to communicate over existing phone lines 29 to the 911 emergency response operator 28.” *Id.* The pendant 40 has a “momentary push button 50” that causes the base unit “to make the emergency call.” *Id.*

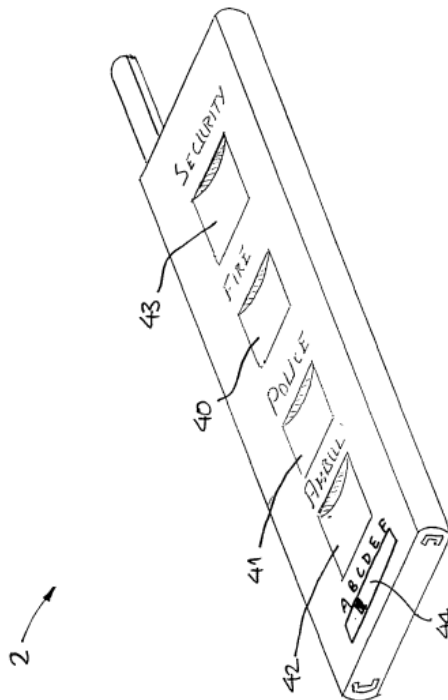
¶[0279]. *Wade* explains that “[i]n the case of an emergency situation the emergency caller should depress the pendent button 50, 3 times, step 226, ***the 3 button depressions minimize the occurrence of a false alarm or accidental emergency call being made.***” *Id.* ¶[0317]. Thus, *Wade* expressly discloses that using three button presses, as disclosed by *Kim*, will “minimize the occurrence of a false alarm or accidental emergency call being made.”

121. There are other examples of prior art references that show that requiring that a panic button be pressed a plurality of times was a known technique to reduce the risk of accidental or false activation.

122. The *Ahmad* reference, published in May 1999 discloses a portable transmitter unit for use in a security system and describes a “double strike” technique to avoid accidental operation:

The transmitter unit 2 may incorporate means to avoid accidental activation of an alarm by inadvertent operation of the switches. Such means may comprise a circuit design such that a double strike of a button, or an extended press of a button, is required to trigger a transmission of an alarm signal. Alternatively, a hinged cover or covers might be provided to switches.

EX1020 at 8:6-11.



EX1020 at FIG. 4

123. The *Sheffer* reference, published in May 1996 discloses a portable or mobile phone that “includes a processor for generating an emergency signal on detection of an emergency condition and transmitting the emergency signal to a remote monitoring station via the wireless telephone network.” EX1022 at Abstract. The portable phone “has a conventional keypad 114 for dialing selected telephone numbers and additionally has a panic button 116 for pressing by the person carrying the unit in the event of an emergency.” *Id.*, 11:30-39. “An alarm is initiated by the user hitting the designated alarm or panic button on the keypad ***rapidly and more than twice in a row, to eliminate or reduce the risk of accidental alarm initiation.***” *Id.*, 12:53-56.

124. The *Gonzales* reference, filed in 2001 and issued in November 2008 discloses a “child alert system that uses radio transmitters and receivers to provide the location of a child,” and “[t]he transmitter unit includes a panic button for allowing the wearer of the transmitter unit to send a panic signal when they feel endangered.” EX1021 at Abstract. *Gonzales* explains that “***[t]he panic button would have to be pushed twice, which would prevent accidental activation,*** in order to send out a signal that would be picked up by the receiver unit of the present invention to alert the receiver unit that the wearer of the transmitter unit requires aid or assistance.” *Id.*, 1:32-40.

125. In view of the foregoing, in my opinion, a person having ordinary skill in the art would have understood that implementing *Kim*'s emergency key button into *Walker* would have been consistent with and retained *Walker*'s goal to minimize the risk of accidental activation.

126. Accordingly, in my opinion, a person having ordinary skill in the art would have understood that modifying *Walker* to use *Kim*'s emergency key button that is pressed a plurality of times would have amounted to the simple substitution of one known element (*Kim*'s emergency key button 32 that must be pressed a plurality of times (e.g., three times)) for another (eyewitness button 12 that is recessed and set to operate at a higher finger pressure) to obtain predictable results (*Walker*'s mobile device with an emergency key button that, when pressed a plurality of times (e.g., three times), triggers collection and transmission of data).

127. A person having ordinary skill in the art would have had a reasonable expectation of success in making the substitution at least because *Walker* itself states that any "input feature" "may be set to act as the eyewitness button" and that any "series" of inputs can initiate the collecting and transmitting of data:

In another embodiment of the invention, the handheld device 1 ***does not have a eyewitness button 12***, but any button or navigation

control or *input feature* or combination of such inputs of the device *may be set to act as the eyewitness button*.

Id. ¶[0151]

In another embodiment of the invention the series of automatic actions initiated by pressing the eyewitness button 12 may instead or additionally be set to initiate by inputting a code into the keypad 17, or by nominating another button or navigation control 16 through the device controls to act as the eyewitness button 12, or by pressing a nominated button on the device and holding down this button beyond a certain time period, or *by pressing a nominated button a predetermined number of times*, or by sliding a cover to expose a button and then depressing that button, or by pressing two or more buttons simultaneously, which may be located on different sides of the device and which may be recessed, *or by any other sequence or series of actions and/or inputs into the device*.

Id. ¶[0132].

128. In addition, the prior art has several examples of buttons that were similarly configured to be activated by a plurality of presses, which further demonstrates that configuring *Walker* to have a dedicated emergency key button activated in that manner would have been within the skill of a person having ordinary skill in the art. In addition to the *Wade*, *Ahmad*, *Sheffer*, and *Gonzales* references above, *Berger* discloses, holding or pressing an emergency button “repeatedly”:

In an emergency situation, a user would either hold the emergency button 214 or press the button repeatedly. If the person that the user is communicating with does not appear to be able to assist the user, *then the user may continue to activate the emergency button 214 in attempt to contact the emergency response center.* Thus, if the emergency button 214 is still activated at step 414, then the processor 302 terminates the existing call at step 418 and dials an emergency number associated with the emergency response center or otherwise contacts the center via the transceiver 323 at step 410. Thereafter, after the call is terminated by the mobile communication device 300 or the emergency response center at step 412, the processor returns to monitoring the emergency button or buttons 214 of the accessory 200 at step 404.

EX1019 ¶[0026].

129. As another example, the *Cobb* reference, which discloses a watch with an emergency button and that the “emergency button 64 is pressed twice”:

When the emergency button 64 is pressed twice the electronic transmitter 41 sends the signal to the cellular relay station 12.

EX1017, 4:12-14.

130. The *Smith* reference discloses pressing the “panic button 36 three times in quick succession”:

When armed by using the first button 24 as described above in relation to the first embodiment, *a user can press the panic button 36 three times in quick succession.* This will cause the device to

automatically send a text message to a set cellphone. The device may be used by a child, for example, to send a text message to a parent's cellphone.

EX1019, 9:1-8.

131. To note, a person having ordinary skill in the art would have understood that the substitution would have involved a tradeoff, as a recessed button set to operate at higher finger pressure has different advantages than a non-recessed button that must be pressed a plurality of times. For example, the former may be more difficult for some people (such as the elderly) to locate and press than the latter, while the latter may be more susceptible to being falsely activated by, for example, other items (e.g., by a book or other clutter if stored in a bag) than the former. A person having ordinary skill in the art would have appreciated such tradeoffs and would have nevertheless considered the substitution obvious.

132. I also note that while *Walker* discloses that a “nominated button” may be pressed a series of times to initiate *Walker*’s collection and transmission of data, a person having ordinary skill in the art would have understood that using a dedicated button that required pressing a plurality of times was advantageous. For example, a dedicated button provides a simpler design and a lower risk of user-confusion in emergency situations. With a dedicated button, the user would not need to remember which multi-function button was set to act

as the panic button, and there would be lower risk of confusion related to knowing whether the user had activated the panic function, or a different function associated with the button.

133. Accordingly, in my opinion, the *Walker-Kim* combination discloses or suggests a mobile device with a dedicated emergency key button (“panic button”) that, when pressed a plurality of times (e.g., three times) activates the emergency key to trigger the collection and transmission of emergency information (“wherein the panic button is activated by a series of depressings of the panic button”).

- (ii) **the panic button is “adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location when the panic button is activated”**

134. In my opinion, *Walker* in combination with *Kim* discloses or suggests the panic button is “adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location when the panic button is activated.”

135. *Walker* discloses that when the eyewitness button is pressed, it initiates various operations including obtaining and transmitting the data (i.e., video, sound, location, and owner identification information) to the remote data storage facility:

On pressing the eyewitness button 12 a series of automatic parallel or sequential actions are instantly initiated:

...

4) The handheld device 1 communicates with the data storage facility 7 through the "always connected" wireless connection to the cellular network 4, which enables the device 1 to push data without requiring the user to establish a dial-up session, and transmits the time as displayed by the handheld device 1 to the data storage facility 7. ***The data storage facility 7 creates a unique electronic file to hold all data recorded during the call into this unique file. A new file is created for each new call received by the data storage facility 7. A database link between each file and the device owner's identity*** or account is made, enabling the device owner and the data storage facility 7 to lookup and access files in the future which have previously been recorded by the device owner.

...

6) ***The device begins transmitting ongoing streaming video and sound data and other data to the data storage facility 7*** where compatible recording equipment is permanently on standby to receive, record and log the automatic transmission of mission critical data from the handheld device 1 in real time. The video data transmitted are simultaneously displayed on the device screen 13, enabling the user to monitor what video data are being transmitted.

...

8) Within 6 seconds of pressing the eyewitness button 12 the hybrid A-GPS circuitry obtains sufficient data from the satellite constellation 11 and cellular network 4. From such data the location coordinates are calculated. The calculation is performed by the handheld device 1 or network 4 ***and the coordinates are immediately transmitted to the data storage facility 7, integrated with the continuing video stream, sound data and other data. As the transmission of video and sound and other data continues, hybrid A-GPS data are regularly updated and transmitted to the data storage facility 7.***

...

In the event that the handheld device 1 is operating in a network 4 where a dial-up model is involved and/or a successful connection is not achieved between the handheld device 1 and data storage facility 7 at the first dialling attempt, or in the event that a successful transmission from the handheld device 1 to the data storage facility 7 is not achieved, video, sound, positioning and other data are recorded inside the handheld device 1 whilst the device automatically and constantly attempts to resend the data or redials a preset number until a connection is made and the data are transmitted, or until the deactivating code known only to the user is entered or until the device is destroyed, providing that such destruction occurs before a successful connection and transmission is achieved and providing that such destruction destroys the recorded data stored inside the memory components of the device and not just the communications and recording capabilities of the device 1.

...

Once a successful connection is made between the handheld device 1 and the data storage facility 7, the recorded images, sound, geographical coordinates detailing the location of the device 1, and timestamp generated by the handheld device 1 against the recordings, and other data stored in the memory chips and/or memory cards and/or memory discs and/or hard drives, and/or tapes and/or other data storage facilities of the handheld device 1 are immediately and automatically transmitted by the handheld device 1 to the data storage facility 7 for safe storage.

...

The time involved between pressing the eyewitness button 12 and safely storing images and data at the data storage facility 7 linking an individual to a specific place at a specific time takes no more than a few seconds, providing that a clear connection exists between the device 1 and the cellular network 4 at the time, or that a dial-up telephone connection is obtained at the first automatic dialling attempt.

EX1007 ¶¶[0092]-[0109].

136. This is consistent with how the '404 patent describes “activating” the camera unit, the location unit, and the transmitting unit to perform a function:

In another embodiment, the present invention provides a self-defense device including a self-defense mechanism which is integrated with a mobile phone/device such that *when the self-*

defense mechanism is activated, a camera built into the mobile phone/device takes still or moving images of the attacker, and the mobile phone/device sends the image data to the authorities along with specific information such as, for example, the name and description of the owner of the self-defense device, the location information, etc. audio information can be obtained by the camera and sent as well. In this way, the present invention utilizes a built-in camera to take image(s) of the attacker and send the specific information to the authorities along with the image information and audio information. The self-defense mechanism can be, for example, a vial containing pepper spray or mace, a personal alarm, a stun gun, a stench ointment, or the like. Further, the self-defense mechanism can be a separate panic button located on the device *which activates the above-mentioned processes.*

EX1001, 5:24-42.

In one example, pushing a “panic button” on the mobile phone/device of the present invention can result in a still image or moving video being taken, as well as an audio recording being obtained. The present invention then wraps the data up and transmits it to an emergency service with the x-y coordinates. This enables the emergency service to have image and/or audio data as well as the relevant location information. Other features are included as well. *For example, a panic button can trigger the image/audio data and location information being obtained.* Further, the panic button can also trigger a separate self-defense

mechanism such as pepper spray, mace, or a personal alarm. These can be triggered, by a panic button or buttons or button sequence.

Id., 7:8-21.

According to another embodiment, the panic button can be a big (e.g. red) button in the center of the phone (or elsewhere on the phone) that the user holds down for a predetermined time period. This can safeguard against falsely triggering the device. Other safeguards can include a button sequence, the number of times a button is depressed, etc. The user can choose to dial or say 911 and thereby activate the device that way. Or the user can have their own special code word for activation. The button can send a signal to a controller inside the device *to activate this process*. The button can start the speech recognition process in one embodiment, to trigger the device.

Id., 7:51-62.

137. And as I discussed above in §X.A.1.e(i), in the *Walker-Kim* combination, *Kim*'s emergency key button is substituted for *Walker*'s eyewitness button to initiate the same operations when the emergency key button is pressed a plurality of times (e.g., three times).

138. A person having ordinary skill in the art would have understood *Walker* to disclose that data from the handheld communications device is transmitted to a specified location (for example, a data storage facility) as opposed to merely broadcast.

139. For example, *Walker* explains that the device transmits data through a “dialup connection” or by email, or by an electronic messaging service:

In another embodiment of the invention the handheld device 1 transmits recorded data to the data storage facility 7 ***through a dialup connection or by email or by email attachment or by an electronic messaging service.***

EX1007 ¶[0134]

The following details ***the preferred embodiment of the data recording and storage facility 7:***

Computerised automatic digital data recording equipment fully compatible with the 3G handheld mobile communications device transmissions, embedded within a cellular network architecture and ***accessible through one or more IP addresses or email addresses or other such electronic domains, and/or through one or more dialup telephone numbers*** and/or through one or more internet or intranet websites, such equipment capable of receiving and organising mission critical packet data transmissions and communications according to timeline data, from a plurality of handheld devices 1, and configured within the architecture to communicate with such handheld devices and to receive, organise according to timeline data, record, store and log all mission critical data and communications transmissions in real time from such handheld devices into a database or databases against device ID's or user accounts

Id. ¶[0084]-[0085]

1. A personal safety and crime prevention system combining existing technologies, characterised by a handheld mobile communications device incorporating precision timekeeping technologies, and incorporating an electronic locking mechanism for securing removable components in place, and incorporating geographical positioning technologies, and incorporating a number of sensors sensitive to a range of stimuli, and incorporating a simple trigger, wherein the triggering of said simple trigger initiates a series of automatic parallel or sequential actions causing said handheld device to instantly power up said sensors, and to instantly activate said electronic locking mechanism, and to instantly generate and integrate accurate timeline data with data generated by said sensors as said sensors react to both the environmental conditions at the geographical location of said handheld device and to the behaviour and activities of any individuals present at said location within range of said sensors, wherein said integrated data are further integrated with regularly updating geographical positioning data, and wherein said handheld device instantly transmits all said data as one or more streams of data through one or more wireless connections to one or more telecommunications networks, wherein said data are routed to a data storage facility, wherein said data are automatically organised and stored as evidence linking said individuals to said location according to said timeline, and to the physical presence of the user of said handheld device.

86. A handheld device as claimed in Claim 1 wherein *said handheld device transmits said data to said data storage facility*

through a dialup connection or by email or by email attachment or by an electronic messaging service.

Id. at claim 86.

140. A person having ordinary skill in the art would have understood that a dial-up connection, email, or electronic messaging service would have required a recipient location to be selected or specified, for example, by the system designer or the user (for example, by inputting a phone number or an email address). And a person having ordinary skill in the art would have understood that “electronic messaging service” refers to, for example, MMS. The Wiley dictionary from 2004 defines “electronic messaging” as “[a]ny form of sending, receiving, and exchanging messages, such as emails, instant messages, MMSs, or SMSs, utilizing a communications network.” EX1023.

141. This is consistent with how the ’404 patent describes transmitting to a “specified location.” The ’404 patent uses MMS as an example protocol that allows the user to transmit data to a “specified location”:

The most common use of MMS is for communication between mobile phones/devices. MMS is one method enabling the present invention to obtain video/audio information and send the data *to a specified location.*

EX1001, 6:38-42.

142. The ’404 patent also describes sending data to specific places or individuals and using “regular e-mail”:

In another embodiment the present invention allows the user to pre-record a personal warning message which is transmitted to the emergency personnel in the event of an attack during a specific time period.

Id., 7:41-44.

In another embodiment, the present invention provides a self-defense device including a self-defense mechanism which is integrated with a mobile phone/device such that when the self-defense mechanism is activated, a camera built into the mobile phone/device takes an image of the attacker, and the mobile phone/device sends image data and audio data ***to the authorities*** along with specific information such as, for example, the name and description of the owner of the self-defense device, location information, a time and date stamp, etc. In this way, the present invention utilizes a built-in camera to take still or moving images of the attacker and send the image and/or audio data ***to the authorities*** along with the specific information. The self-defense mechanism can be a vial containing pepper spray or mace, for example, or simply a separate panic button located on the device which activates the above-mentioned processes. Of course, the present invention is not limited to the examples discussed herein.

Id., 3:4-21.

To expand upon this further, there are a number of ways to send image data and audio data using the present invention. As one example, image data can be sent ***through regular e-mail*** to a dispatching center and then to a police station. As another

example, image data can be sent through a picture-based e-mail type system (such as MMS). As another example, image data can be sent through a regular TCP/IP to a web service, which enables internet access on a cell phone. Of course, the present invention is not limited to these examples, and various modifications are envisioned.

Id., 6:44-53.

143. Accordingly, in my opinion, the *Walker-Kim* combination discloses or suggests a mobile device with a dedicated emergency key button (“a panic button”) that initiates various operations, including capturing and transmitting video, sound, and coordinates, along with information to identify the owner of the device to the data storage facility (“adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location”) when the emergency key button is pressed a plurality of times (e.g., three times) (“when the panic button is activated, wherein the panic button is activated by a series of depressings of the panic button.”).

2. CLAIM 10: The mobile device as set forth in claim 9, wherein when the panic button is activated a public or private network for emergency purposes is dialed.

144. *Walker* in combination with *Kim* discloses or suggests “[t]he mobile device as set forth in claim 9, wherein when the panic button is activated a public or private network for emergency purposes is dialed.”

145. As detailed in §X.A.1.e, a person having ordinary skill in the art would have understood the *Walker-Kim* combination to disclose or suggest that when the emergency key button is pressed a plurality of times (e.g., three times), it initiates a number of actions, including communication between the mobile device and the data storage facility.

146. *Walker* discloses that the communication between the handheld device and the storage facility can use various communication networks. For example, *Walker* discloses using the Public Switched Telephone Network (PSTN):

The data recording facility may be embedded within or connected to the communications infrastructure or network architecture of one or more cellular telephone networks, or be embedded within or connected to one or more telecommunications network architectures, or be embedded within or connected to the internet, or be embedded within or connected to one or more local or wide area data network architectures, ***or be embedded within or connected to the Public Switched Telephony Network (PSTN), or be embedded within or connected to any combination of any such structures***, and may involve Storage Area Network (SAN) configurations or Network Attached Storage (NAS) configurations or Direct Attached Storage (DAS) configurations or distributed data storage configurations, and may include InfiniBand technologies, or iSCSI, or Internet Fibre Channel Protocol (iFCP), or Fibre Channel over IP (FCIP), or Network File

System (NFS), or Direct Access File System (DAFS) and other similar and emerging technologies.

EX1007 ¶[0060]

51. A data storage facility as claimed in Claim 1 *wherein said data storage facility is accessible through one or more IP addresses or email addresses or other such electronic domains, or through one or more dialup telephone numbers or through one or more internet or intranet websites.*

Id., claim 51

147. *Walker* also discloses that the storage facility is accessible through a dialup telephone number:

The following details the preferred embodiment of the data recording and storage facility 7:

Computerised automatic digital data recording equipment fully compatible with the 3G handheld mobile communications device transmissions, embedded within a cellular network architecture and accessible through one or more IP addresses or email addresses or other such electronic domains, *and/or through one or more dialup telephone numbers* and/or through one or more internet or intranet websites, such equipment capable of receiving and organising mission critical packet data transmissions and communications according to timeline data, from a plurality of handheld devices 1, and configured within the architecture to communicate with such handheld devices and to receive, organise according to timeline data, record, store and log all mission critical

data and communications transmissions in real time from such handheld devices into a database or databases against device ID's or user accounts.

Id. ¶¶[0084]-[0085]

148. *Walker* also discloses that the recorded video, sound, and location data can be transmitted to the storage facility via the dialup connection:

In another embodiment of the invention the handheld device 1 transmits recorded data to the data storage facility 7 through a dialup connection or by email or by email attachment or by an electronic messaging service.

Id. ¶[0134]

149. *Walker* also explains that if the handheld device is using a dial-up connection, the device dials and redials the preset number until the connection is made and the data is transmitted:

In the event that the handheld device 1 is operating in a network 4 where a dial-up model is involved and/or a successful connection is not achieved between the handheld device 1 and data storage facility 7 ***at the first dialling attempt***, or in the event that a successful transmission from the handheld device 1 to the data storage facility 7 is not achieved, video, sound, positioning and other data are recorded inside the handheld device 1 whilst ***the device automatically and constantly attempts to resend the data or redials a preset number until a connection is made*** and the data are transmitted, or until the deactivating code known only to

the user is entered or until the device is destroyed, providing that such destruction occurs before a successful connection and transmission is achieved and providing that such destruction destroys the recorded data stored inside the memory components of the device and not just the communications and recording capabilities of the device 1.

Id. ¶[0103]

The time involved between pressing the eyewitness button 12 and safely storing images and data at the data storage facility 7 linking an individual to a specific place at a specific time takes no more than a few seconds, providing that a clear connection exists between the device 1 and the cellular network 4 at the time, or that a dial-up telephone connection is obtained at the first automatic dialling attempt.

Id. ¶[0109]

150. In view of the above, in my opinion, a person having ordinary skill in the art would have understood *Walker* in combination with *Kim* to disclose or suggest that when the emergency key button is pressed a plurality of times (e.g., three times), the handheld mobile device dials a number to form a dial-up connection to the remote data storage facility on the PSTN to transmit recorded data.

151. In addition, *Walker* discloses that the transmitted and recorded data is used to assist security and police in responding to crimes:

The present invention relates to a cellular handheld mobile communications device and external data storage system, and is *intended to enhance personal safety and security, acting as an electronic eyewitness, helping to deter criminal activity and to reduce the incidence of crime. Where crime is committed, the invention assists authorities and security services in obtaining evidence linking the identities of criminals to their crimes.*

Id. ¶[0001]

The invention thus provides a strong deterrent to criminal activity, increasing both personal and public safety through acting as a digital mobile eyewitness and crime prevention tool, *linking the identity and behaviour of a recorded individual or individuals to a specific place at a specific time and to the physical presence of the user at the location at that time*, within moments of pressing the eyewitness button.

The present invention additionally enables police to access all such recordings made by any individuals in possession of this mobile communications handheld device at or near the scene of a crime, thereby aiding the collection of evidence in connection with crimes. *The invention additionally enables police to locate all individuals who activate this function of the device, within a selected range of times and distances of any crime scene, thereby aiding police in locating and interviewing potential witnesses to a crime. The location of users is only recorded and made accessible to police on pressing the eyewitness button of the device.* When the device is used in it's [sic] normal capacity as a

handheld mobile communications device the whereabouts of the user is not tracked, unless the user opts in to additional services and activates an automatic tracking function.

Id. ¶¶[0040]-[0041]

The present invention may be used, for example, by a girl walking through a secluded park in the event that she is approached by a suspicious man. In such a circumstance, the girl simply presses the recessed eyewitness button on her mobile communications handheld device as soon as she begins to feel uncomfortable in the presence of the man. She holds the device as if to make a call or check some personal information stored in her phone, thereby not raising any suspicions, but ensuring that an integral camera is pointing in the direction of the suspicious man.

Id. ¶[0043]

Any member of the public having this invention in their possession and witnessing a crime may discretely transmit sound and images and environmental data relating to the incident at the press of the eyewitness button, for later analysis by police. Should a mugger snatch a woman's handbag in a crowded street and run, any member of the public in possession of this invention seeing the mugger escaping may simply press the eyewitness button and transmit the incident as it happens, in real time.

Should the criminal snatch the device and destroy it, the information will remain, recorded and logged at the data storage facility, and depending on which version of this invention the user is in possession of, the criminal's odour and fingerprints may

additionally be captured and transmitted on snatching the device, before the criminal has a chance to destroy the device.

Police and security services may potentially access databases held by data storage facilities when seeking evidence in connection with crimes, by entering a time and location of a crime into the database application holding or accessing all data recorded by the appropriate data storage facility. Central databases and/or applications may be created, linking and combining the data of all data storage facilities within a certain region or jurisdiction. Authorities may potentially access any recordings made within a selected range of distances of a particular location and within a selected range of times. Through such access, authorities will be able to increase the probabilities of linking guilty criminals to their crimes and of identifying witnesses to crimes.

Id. ¶¶ [0048]-[0049]

In another embodiment of the invention the handheld device 1 incorporates video conferencing technology, enabling the user to simultaneously take part in a video conference with emergency services and/or other individuals whilst the series of actions initiated by pressing the eyewitness button 12 continues, and to automatically ***transmit data to emergency services enabling emergency services to immediately locate and access data files relating to the pressing of the eyewitness button.***

Id. ¶[0141]

152. This is consistent with how the '404 patent describes this feature as linking the device to an “emergency assistance number such as 911” or to a “private emergency network”:

The present invention integrates with mobile phones/devices to send image data of the attack, which could be either still image data or moving video, along with location information, and/or audio information, so that help can be dispatched right away. ***The system can be linked in with an emergency assistance number such as 911 or to a private emergency network specifically set up for these purposes to work with the public authorities in assisting victims.*** By virtue of the features of the present invention, authorities will be able to proceed directly to the location of the incident, equipped with specific information such as location information, image and/or audio data of the attack (which can of course aid in identifying the perpetrator), and information as to who owns the mobile phone/device including a description of that person. Audio data (either a pre-recorded help message or audio of the attack itself) can also be sent to the authorities.

EX1001, 5:43-59

153. Accordingly, in my opinion, the *Walker-Kim* combination discloses or suggests a device with a dedicated emergency key button that, when pressed a plurality of times (e.g., three times) (“wherein when the panic button is activated”), the handheld wireless device automatically establishes a dial-up connection to the storage facility embedded within a PSTN to transmit

information to be used in assisting emergency response personnel in responding to emergencies (“a public or private network for emergency purposes is dialed”).

3. CLAIM 12: The mobile device of claim 9, wherein a number of depressings of the panic button to activate the panic button is three.

154. *Walker* in combination with *Kim* discloses or suggests this feature for the reasons discussed in §X.A.1.e(i)

4. CLAIM 13

a. 13[pre], 13[a], 13[b], and 13[e]

155. *Walker* in combination with *Kim* discloses or suggests claim 13.

With respect to 13[pre], 13[a], 13[b], and 13[e], see sections X.A.1.a, X.A.1.b, X.A.1.c, and X.A.1.e(i), respectively.

b. 13[c]: a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location, along with specific information including owner identification information; and

156. Limitation 13[c] requires “a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location, along with specific information including owner identification information.” This is the same as 9[c] except that it further requires that the transmitting unit is adapted to transmit data and information to a “specified location.” The *Walker-Kim* combination discloses or suggests 9[c] as explained in §X.A.1.d. As explained in §X.A.1.e(ii), a person having ordinary

skill in the art would have understood *Walker* to disclose or suggest transmitting the data and information to a specified location.

157. Accordingly, in my opinion, the *Walker-Kim* combination discloses or suggests cellular communications equipment and various additional or alternative transmission technologies (a “transmitting unit”) to transmit image, audio, and location data in emergencies to remote storage facility (“adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location”) along with information to identify the owner of the device (“along with specific information including owner identification information”).

- c. **13[d]: “a panic button, which, when activated, performs the following panic button functions: (1) activating the camera unit, the location unit, and the transmitting unit to send the emergency information and the specific information to the specified location, and (2) dialing a public or private network for emergency purposes”**

158. Limitation 13[d] is the same as limitation 9[d] except that it also requires the dialing function described in claim 10. The *Walker-Kim* combination discloses or suggests 9[d] as explained in §X.A.1.e. And the *Walker-Kim* combination discloses or suggests claim 10 as explained in §X.A.2.

159. Accordingly, in my opinion, the *Walker-Kim* combination discloses or suggests that when the emergency key button is pressed a plurality of times

(e.g., three times) (“when the panic button is activated”) it causes the device to initiate various operations, including capturing and transmitting video, sound, and coordinates, along with information to identify the owner of the device (“performs the following panic button functions: (1) activating the camera unit, the location unit, and the transmitting unit to send the emergency information and the specific information to the specified location”); and to automatically establish a dial-up connection to the storage facility embedded within a PSTN to transmit information to be used in assisting emergency response personnel in responding to emergencies (“and (2) dialing a public or private network for emergency purposes”).

5. CLAIM 14: “The mobile device of claim 13, wherein a number of depressings of the panic button to activate the panic button is five”

160. *Walker* in combination with *Kim* discloses or suggests “[t]he mobile device of claim 13, wherein a number of depressings of the panic button to activate the panic button is five.”

161. As explained in §X.A.1.e(i), the combination of *Walker* and *Kim* discloses or suggests a mobile device with a dedicated emergency key button (“panic button”) that, when pressed a plurality of times (e.g., three times), triggers the collection and transmission of emergency information (“wherein the panic button is activated by a series of depressings of the panic button”).

162. Based on my background and experience, a person having ordinary skill in the art would have understood that pressing a key a “plurality of times” discloses pressing the key two or more times. The 2004 Webster dictionary also defines “plurality” as “the condition of being plural or numerous.” EX1024. A range of two or more presses does not have an upper bound, so it overlaps and encompasses the five presses required by claim 14. The ’404 patent does not disclose that there is something special or critical about five button presses, as the ’404 patent does not specifically describe using five presses at all.

163. Accordingly, in my opinion, the *Walker-Kim* combination discloses or suggests that the emergency key button is pressed a plurality of times to activate the emergency key button (“wherein a number of depressings of the panic button to activate the panic button is five.”).

**B. GROUND 1B: WALKER IN VIEW OF KIM AND DIXIT
RENDERS CLAIM 14 OBVIOUS**

164. As explained in §X.A.5, *Walker* in combination with *Kim* renders claim 14 obvious. To the extent the Board disagrees, then it is my opinion that claim 14 would have been obvious in view of *Walker*, *Kim*, and *Dixit*.

165. *Dixit* is similar to the ’404 patent, *Walker*, and *Kim*. *Dixit* is titled “System and method for remote convenience function control with at-vehicle and remote assistance-summoning functions.” *Dixit* discloses a “remote convenience system 10” with a “portable hand-held transmitter unit 12”:

A remote convenience system (10) and an associated function remotely control convenience functions at a vehicle (16). A receiver/controller (14), located at the vehicle (16), receives vehicle remote convenience function request signals (30) that convey remote function request messages and controls vehicle systems (e.g., 48, 50, 52, and 68) to perform the remotely requested vehicle functions. The receiver/controller (14) includes a messaging processing portion (110) for providing a signal (e.g., 128/130) to activate an at-vehicle alarm component (e.g., 50/52) and for providing a signal (132) to activate a remote assistance-summoning component (68). *A portable transmitter outputs the remote convenience function request signals (30) to cause remote control performance. The transmitter (12) includes a manually actuatable emergency pushbutton switch (94). The switch (94) is actuatable in a first operation mode (e.g., a single actuation) to cause activation of the at-vehicle alarm component (50/52), and is actuatable in a second, different operation mode (e.g., a plurality of actuations) to cause activation of the remote assistance-summoning component (68).*

Dixit, Abstract.

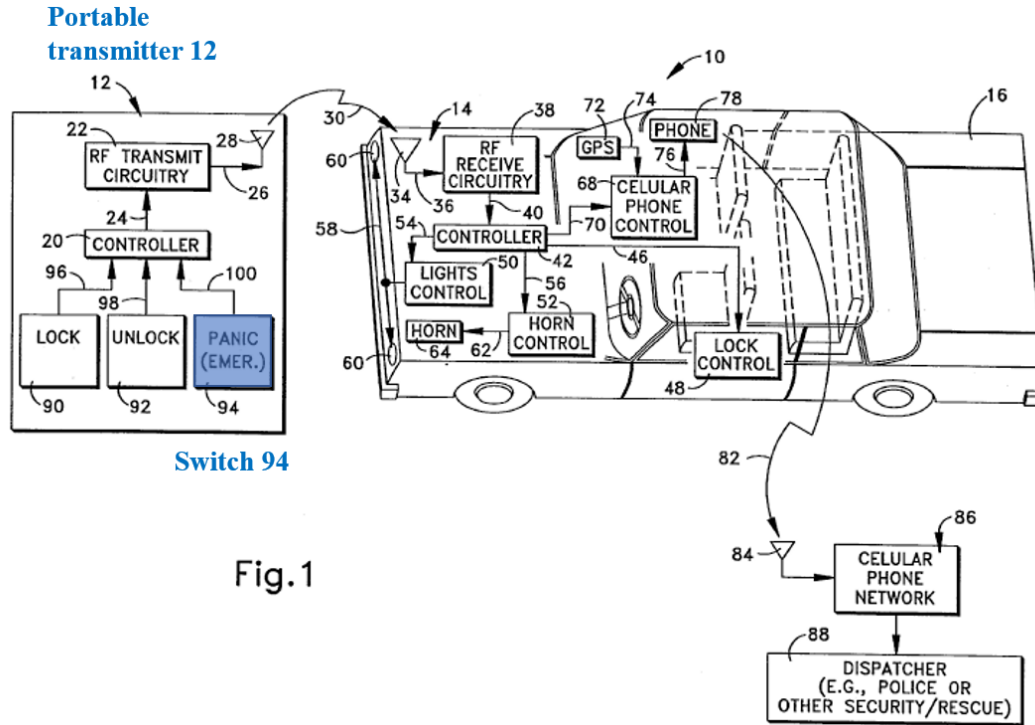


Fig. 1

Dixit, FIG. 1 (annotated)

166. The portable transmitter 12 has a panic “switch 94” that, when “actuated five times” causes the vehicle to transmit a remote assistance-summoning request to, for example, the police:

In the preferred embodiment, the first operation mode of the third pushbutton switch 94 is a single actuation of the third pushbutton switch. The second, different operation mode of the third pushbutton switch is *a plurality of actuations of the third pushbutton switch 94 within a predetermined time period. In one example, for the second operation mode the third pushbutton switch 94 is actuated five times, with each actuation coming not more that one second after the previous actuation (i.e., a total*

five actuations within five seconds). For each actuation of the third pushbutton switch 94, the transmitter 12 outputs the broadcast signal 30 that conveys the PANIC message.

At the vehicle 16, the controller 42 determines the remote control function that is being requested. Specifically, within the controller 42, a message processing portion 110 (FIG. 2) receives its input 112 from the RF receive circuitry 38. The message processing portion 110 may be comprised of discrete hardwire circuitry or a processor performing a program. The message processing portion 110 accesses 114 a memory 116 to make a determination regarding whether the received message is intended for the vehicle 16 (i.e., comparison of security code, etc.).

The message processing portion 110 also makes an initial determination as to whether the received signal conveys a lock control request or PANIC function request. If the message is directed to door locking/unlocking, the message processing portion 110 immediately outputs an appropriate signal 118 to the lock control 48. *If the message is a PANIC message, the message processing function performs a routine to determine whether the remote function requested is the at-vehicle alarm function or the remote assistance summoning function.*

It is to be recalled that each actuation of the third pushbutton switch 94 at the transmitter 12 causes transmission of the broadcast signal 30 that conveys the PANIC message. Also, it is to be recalled that remote assistance summoning is accomplished by timely transmission of a plurality of PANIC messages, which when taken individually would be requests for an at vehicle alarm

function. Thus, in order to determine which of the two functions (i.e., either at-vehicle alarm or remote assistance-summoning) is currently being requested, the message processing portion 110 performs a routine.

When a PANIC message is received via broadcast signal 30, the message processing portion 110 communicates 120 with a timer 122 to activate the timer. The message processing portion 110 also communicates 124 with a PANIC request counter 126. The message processing portion 110 utilizes the timer 122 and the PANIC request counter 126 to determine if the predetermined plurality of PANIC messages are received within the predetermined specified time to indicate a remote assistance-summoning request. *Depending on whether an at-vehicle alarm function is requested or a remote assistance-summoning function is requested (i.e., single PANIC message or plurality of PANIC messages within specified time parameter), the message processing portion 110 outputs appropriate signals 128, 130 to the light and horn controls 50 and 52, or outputs a signal 132 to the cellular phone control 68.*

A flowchart for a process 200 performed within the receiver/controller 14 at the vehicle 16 is shown in FIG. 3. The process 200 begins at step 202 and proceeds to step 204. At step 204, the receiver/controller 14 awaits reception of a message via the broadcast signal 30. At step 206, it is determined whether the received message is the PANIC message.

Dixit, 4:47-5:40.

If the determination at step 220 is affirmative (i.e., five PANIC messages have been timely received), the process 200 goes from step 220 to step 222. At step 222, the remote assistance-summoning function is performed. Specifically, the message processing portion 110 provides a signal to activate the cellular phone control 68. The cellular phone control 68 receives location information from the GPS 72 and provides a message to the cellular phone 78 for conveyance to the dispatcher 88 via the cellular phone network 86. Upon completion of step 222, the process 200 loops back to step 204.

Dixit, 5:41-49

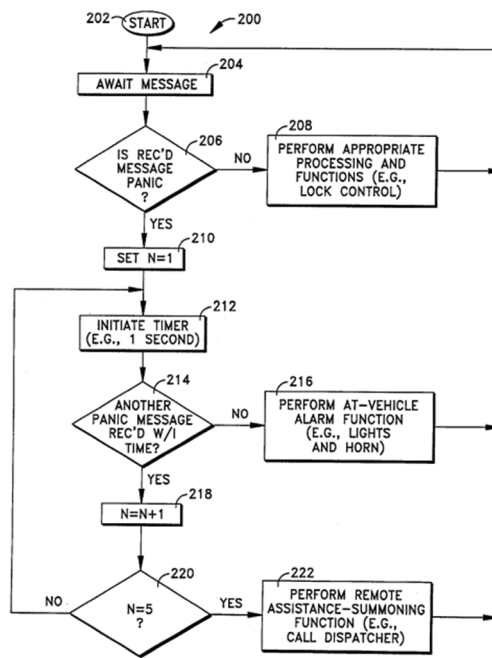


Fig.3

Dixit, FIG. 3

167. As detailed in §X.A.1.e(i), person having ordinary skill in the art would have understood that using a plurality of button presses was a well-known technique for minimizing the risk of accidental activation.

168. The '404 patent does not disclose any special or critical results in terms of risk reduction from using five button presses compared to any other number of button presses more than one. To be sure, a person having ordinary skill in the art would have understood that requiring five button presses would predictably lead to fewer accidental activations compared to four, three, or two button presses with a corresponding tradeoff in terms of how easy it is to activate the panic button when needed. But considering the pros and cons, a person having ordinary skill in the art would not have been dissuaded from requiring five button presses, as demonstrated by *Dixit*.

169. Thus, in my opinion, a person having ordinary skill in the art would have been motivated to use five button presses instead of three to, for example, further reduce the risk of accidental activation of the panic button.

170. In my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood the proposed combination to amount to the simple substitution of one known element (a panic button that must be pressed five times) for another (a panic button that must be

pressed three times) to obtain predictable results (a panic button that is activated after five presses).

171. Accordingly, in my opinion, a person having ordinary skill in the art would have understood that the *Walker-Kim-Dixit* combination discloses or suggests a mobile device with a dedicated emergency key button that must be pressed five times (“wherein a number of depressings of the panic button to activate the panic button is five.”).

C. GROUND 2: WALKER RENDERS OBVIOUS CLAIM 15

1. CLAIM 15

a. 15[pre]: “An emergency safety device, comprising”

172. In my opinion, to the extent the preamble is limiting, *Walker* discloses or suggests “[a]n emergency safety device.”

173. For example, *Walker* discloses that its mobile device may be used to increase personal safety, for example, when someone being threatened by an attacker, by transmitting information for use by the police:

The present invention provides a mobile communications handheld device and remote data recording and storage system which, in a single action, enables a user of the mobile communications handheld device to press a recessed eyewitness button or shout a voice command, which instantly initiates a series of actions, immediately capturing and transmitting streaming video and sound and environmental data detected by various

sensors to a remote data storage facility, providing evidence of another individual's physical appearance, dress, behaviour, utterances and surroundings in real time and without any dial-up delay, together with precise geographical coordinates of the location and the precise time of the event, where the recorded data ***cannot be destroyed by an attacker even in the event that the handheld device is destroyed following such transmission.***

...

The invention thus provides a strong deterrent to criminal activity, increasing both personal and public safety through acting as a digital mobile eyewitness and crime prevention tool, linking the identity and behaviour of a recorded individual or individuals to a specific place at a specific time and to the physical presence of the user at the location at that time, within moments of pressing the eyewitness button.

...

HOW THE INVENTION MAY BE USED

The present invention may be used, for example, by a girl walking through a secluded park in the event that she is approached by a suspicious man. In such a circumstance, the girl simply presses the recessed eyewitness button on her mobile communications handheld device as soon as she begins to feel uncomfortable in the presence of the man. She holds the device as if to make a call or check some personal information stored in her phone, thereby not

raising any suspicions, but ensuring that an integral camera is pointing in the direction of the suspicious man.

The girl immediately sees an image of the man appear on the screen of her device and knows that streaming video and sound and geographical and timeline data is immediately being transmitted to an external data storage facility, without any dialup delay, where it will be safely recorded and stored in real time. She also knows that even if the man subsequently destroys the device, his image and behaviour will remain stored at the data storage facility together with sound, geographic coordinates and the precise timeline of the encounter, linking him to her at that specific location and at that specific time. The closer the man gets to the device, the higher the probability that his identity will be clearly captured by the camera and microphone and various other sensors (further embodiments of this invention include an odour sensor and fingerprint detector pad, and other such sensors, for capturing additional evidence in the event that the device is snatched from her hand).

Once the girl is satisfied that the man's image and/or behaviour has been clearly captured, she may decide to briefly point the digital camera at herself, to record her own presence at the scene (her handheld device may alternatively incorporate two video cameras set on opposing sides of the device, simultaneously capturing and transmitting her image and that of a potential attacker). She may then put her phone in her pocket or bag, or hold it in her hand, yet

still have the device recording and transmitting any sounds within reach of the microphone, together with any images captured by the digital camera, until she decides to enter the appropriate deactivation code into the keypad to cease the recording. She also knows that if the man tries to force her to enter the code, she can enter a dummy deactivation code instead, which will make the device appear the same as if she had entered the correct code, yet the device will continue recording. An attacker has no way of knowing if his intended victim enters the correct deactivation code, and cannot remove the battery or batteries without entering a code to unlock an electronic locking device securing them in place, which has a time-delay feature, thereby preventing the batteries from being removed immediately regardless of which code is entered.

Should the man become aggressive towards the girl at this point, the girl may simply inform the man that his image and/or voice have already been captured and stored externally, linking him to that specific location and with her at that specific time. On hearing this, the man will know that in all probability he will be brought to justice for any assault against the girl.

In the event that the device is snatched from the girl by the man before she has had a chance to press the eyewitness button, she may shout a voice command to trigger the eyewitness commands.

...

Police and security services may potentially access databases held by data storage facilities when seeking evidence in connection with crimes, by entering a time and location of a crime into the database application holding or accessing all data recorded by the appropriate data storage facility. Central databases and/or applications may be created, linking and combining the data of all data storage facilities within a certain region or jurisdiction. Authorities may potentially access any recordings made within a selected range of distances of a particular location and within a selected range of times. Through such access, authorities will be able to increase the probabilities of linking guilty criminals to their crimes and of identifying witnesses to crimes.

EX1007 ¶¶[0038]-[0049]

174. This is consistent with how the '404 patent describes this feature:

Accordingly, it is an object of this invention to provide a self-defense device that a person may be less likely to forget to carry while traveling. ***It is also an object of this invention to provide a self defense device which is capable of quickly notifying the authorities that an attack is under way***, and of providing the authorities with specific information in order to be able to come to the aid of the person being attacked.

EX1001, 2:36-42.

175. Accordingly, in my opinion, a person having ordinary skill in the art would have understood that *Walker* discloses or suggests a mobile device that may be used by someone under attack (“[a]n emergency safety device.”).

- b. 15[a]: “a camera unit, adapted to obtain at least one of image data and audio data”; and 15[b]: “a location unit, adapted to obtain location data”**

176. Limitations 15[a] and 15[b] are the same as limitations 9[a] and 9[b]. Therefore, in my opinion, *Walker* discloses or suggests 15[a] and 15[b] for the same reasons discussed above in sections X.A.1.b and X.A.1.c, respectively.

- c. 15[c]: “a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location via text message, along with specific information including owner identification information; and”**

177. In my opinion, *Walker* discloses or suggests “a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location via text message, along with specific information including owner identification information.”

178. Limitation 15[c] is the same as limitation 9[c] except that 15[c] further requires that the transmitting unit is adapted to transmit data and information to a “specified location via text message.”

179. In my opinion, *Walker* discloses or suggests limitation 9[c] for the same reasons discussed above in §X.A.1.d.

180. As explained in §X.A.1.e(ii), in my opinion, and based on my experience and background, a person having ordinary skill in the art would have

understood *Walker* discloses or suggests transmitting the data and information to a specified location.

181. With respect to transmission “via text message,” *Walker* discloses that the handheld mobile communications device is capable of “text messaging,” “picture messaging,” “video messaging,” and “email”:

The preferred embodiment of the handheld mobile communications device 1 incorporates the following components and/or capabilities and/or features, some of which are not shown in the accompanying drawings:

Quad-mode, quad-band CDMA2000 1xEV-DV Cell/PCS+ GSM/GPRS + A-GPS + AMPS cellular communications and technology enabling the device to receive precise time signals and to transmit and receive packet data and information to and from one or more cellular telecommunications networks 4 and wireless LAN (WLAN) networks including 802.11 WLAN (enabling seamless roaming between private, public, and personal networks), wireless personal area networks (WPANs) connectivity, circuitry enabling the device to determine and transmit the location coordinates of the device through hybrid satellite/cellular network positioning, "always connected" network interface, telephone keypad 17, navigation keys 16, recessed eyewitness button 12, on off switch 21, colour LCD screen/interface 13, high sensitivity microphone 18, speaker and/or earpiece 15, automatic location identification (ALI) and/or

geographic information system (GIS) and/or other geographical mapping components and/or technology, two colour digital cameras with night vision sensitivity positioned on opposing sides of the device 19 & 26, colour video recording and playback facility, still colour picture single frame recording, streaming video conferencing, ***video messaging, picture messaging, text messaging capability***, infrared movement sensor 22, infrared illumination 20 & 23, visible light frequency combined torch & flashlight 25, internet access and email, MP3, speakerphone, voice memos, voice dialling/calling, speech recognition, speech understanding and synthesis, machine learning and distributed artificial intelligence capability, large phone book & contact list, organizer & PDA functions, SIM card and/or UIM card and/or other identification device, microprocessor/s, memory chip/s and/or memory card/s and/or memory disc/s and/or hard drive/s and/or magnetic tape/s and/or other digital data storage devices, power input socket and circuitry, rechargeable battery 24, electronic locking mechanism, secure encryption, speed dialling, variable user profiles, caller ID, three way calling, WAP microbrowser, XHTML browser, Audio/Video/Image coders and decoders, graphics accelerator, hardware accelerator, streaming video player, sound synthesizer, games, USB, Bluetooth, PAN (IPv6), ESDP (Universal Plug and Play over PAN), fax/modem, dial-up networking.

EX1007 ¶¶[0081]-[0082]

182. *Walker* also discloses transmitting the recorded data (e.g., the video, sound, and location data) to the data storage facility “by email or by email attachment or by an electronic messaging service”:

In another embodiment of the invention the handheld device 1 transmits recorded data to the data storage facility 7 through a dialup connection or *by email or by email attachment or by an electronic messaging service.*

Id. ¶[00134]

In the event that the handheld device 1 is operating in a network 4 where a dial-up model is involved and/or a successful connection is not achieved between the handheld device 1 and data storage facility 7 at the first dialling attempt, or in the event that a successful transmission from the handheld device 1 to the data storage facility 7 is not achieved, video, sound, positioning and other data are recorded inside the handheld device 1 whilst the device automatically and constantly attempts to resend the data or redials a preset number until a connection is made and the data are transmitted, or until the deactivating code known only to the user is entered or until the device is destroyed, providing that such destruction occurs before a successful connection and transmission is achieved and providing that such destruction destroys the recorded data stored inside the memory components of the device and not just the communications and recording capabilities of the device 1.

From a criminal's perspective, destroying the handheld device 1 is pointless, as the data are transmitted within moments in most cases and will therefore continue to exist externally. Any activity in attempting to destroy the device 1 may also be transmitted before the device ceases to function, and may continue to exist within surviving memory components or facilities of the device even in the event that the device ceases to function before a successful transmission is made, in the same way that an aircraft black box recorder retains recorded information even after it becomes unable to function as a recording device.

Once a successful connection is made between the handheld device 1 and the data storage facility 7, the *recorded images, sound, geographical coordinates detailing the location of the device 1, and timestamp generated by the handheld device 1 against the recordings, and other data stored in the memory chips and/or memory cards and/or memory discs and/or hard drives, and/or tapes and/or other data storage facilities of the handheld device 1* are immediately and automatically transmitted by the handheld device 1 to the data storage facility 7 for safe storage.

Id. ¶¶[0103]-[0105]

183. The Wiley dictionary from 2004 defines “electronic messaging” as “[a]ny form of sending, receiving, and exchanging messages, such as emails, instant messages, MMSs, or SMSs, utilizing a communications network.”

EX1023.

184. Therefore, in my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood *Walker*'s disclosure of using an "electronic messaging service" to be an express suggestion to use, for example, a Multimedia Messaging Service ("MMS"), to transmit the recorded video, sound, and location data.

185. In my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood would have understood that in the context of the '404 patent, MMS is a form of text messaging that includes multimedia files such as pictures and audio:

The present invention may also use an MMS (Multimedia Message Service) system, which is a mix between internet protocol and e-mail protocol. More specifically, MMS is a store-and-forward method of transmitting graphics, video clips, sound files, and short text messages over wireless networks using WAP.

MMS implementations also support e-mail addressing, so that the device can send e-mails directly to an e-mail address. The presentation of the MMS message is coded into the presentation file so that images, sounds, and text are displayed in a predetermined order as one singular message. The most common use of MMS is for communication between mobile phones/devices. MMS is one method enabling the present invention to obtain video/audio information and send the data to a specified location. Of course, the present invention is not limited to using protocols such as TCP/IP and MMS.

EX1001, 6:28-43

186. In my opinion, a person having ordinary skill in the art would have had a reasonable expectation of success in implementing *Walker*'s mobile device to transmit the recorded video, sound, and location data using MMS because prior art describing very similar devices discloses using MMS for that same purpose. For example, the *Wood* reference describes "a mobile terminal that may transmit an emergency message and information indicative of the emergency to a service center." EX1014 ¶[0008]. *Wood* describes sending image, audio, and location information in the emergency message via MMS:

The emergency message typically includes the time of activation of the mobile terminal 20, as well as recorded information, such as the location of the phone (if the mobile terminal supports this feature), and imagery information (if the mobile terminal supports this feature). Therefore, immediately following user input to activate the mobile terminal 20, the recording device 34 begins to record audio information, which could include the user's voice, as well as any other audible sounds that are capable of being received by the audio device 36. Further, if the mobile terminal includes an imagery device 38, such as a digital camera, a photograph or video will be taken without auditory feedback. Similarly, if the mobile terminal 20 has a location device 40, such as a GPS receiver, that may provide a location of the mobile terminal, this may also be included with the emergency message. ***As such, if the emergency message only includes audio information, the emergency***

message could be a SMS message, or if imagery or location information in addition to, or in place of, the audio information is included, the message could be a MMS message. Therefore, it is understood that the emergency message could be any message capable of being transmitted to the service center 10 and containing sufficient information to notify the service center that a potential emergency is at hand. As such, the emergency message could include any number and combination of textual, audio, imagery, or location information that may be transmitted to the service center 10.

EX1014 ¶[0036]. The *Kumar* reference similarly describes a “wireless device” and “for providing pertinent information including location, multimedia data, and other information regarding an emergency situation using the wireless device.” EX1013 ¶[0001]. *Kumar* also describes sending an emergency message via MMS:

According to some embodiments, a wireless device provides an apparatus and methods for automatically transmitting a MMS (Multimedia Message Service) message including location data indicative of a location of the wireless device and multimedia data captured by the wireless device from a local vicinity of the location of the wireless device to an emergency contact entity. The MMS message may be transmitted in response to a single user input or action to the wireless device. *For example, the wireless device may be activated by actuation of a softkey to enter into a mode of operation wherein a MMS message is automatically sent to an*

emergency contact entity to notify the emergency entity of a location of the wireless device and a number of parameters in the vicinity of the wireless device. The parameters in the vicinity of the wireless device may relate to an emergency situation and may include, for example, a sound, a motion, an image, video data, and/or a combination thereof in the local vicinity of the wireless device. The particular parameter transmitted may be selectively monitored for detection, capture, and/or transmission by the wireless device.

EX1013 ¶[0012].

187. Accordingly, in my opinion, a person having ordinary skill in the art would have understood that *Walker* discloses or suggests a mobile device with a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location via MMS (“via text message”), along with specific information including owner identification information.

d. 15[d] & 15[e]

(i) “a panic button ... wherein the panic button is activated by a button sequence”

188. *Walker* discloses an “eyewitness button 12” that, when pressed once (e.g., during an attack), initiates various operations related to collecting and transmitting information about the attack:

The preferred embodiment enables the device to be used in both daylight and dark conditions. For illustration purposes the following assumes that the invention is activated by the user in dark conditions. ***On pressing the eyewitness button 12 a series of automatic parallel or sequential actions are instantly initiated:***

...

3) The hybrid A-GPS circuitry built into the handheld device 1 is powered up.

4) The handheld device 1 communicates with the data storage facility 7 through the “always connected” wireless connection to the cellular network 4, which enables the device 1 to push data without requiring the user to establish a dial-up session, and transmits the time as displayed by the handheld device I to the data storage facility 7. The data storage facility 7 creates a unique electronic file to hold all data recorded during the call into this unique file. A new file is created for each new call received by the data storage facility 7. A database link between each file and the device owner's identity or account is made, enabling the device owner and the data storage facility 7 to lookup and access files in the future which have previously been recorded by the device owner.

5) The digital video camera circuitry and light sensor circuitry is powered up. Light sensor data configures the device 1 and video cameras 19 & 26 to operate in night vision mode, and

automatically powers up the two infrared illumination sources 20 & 23 to enable images to be captured in darkness. The infrared illumination source 20 is a low powered wide beam for illuminating the user, and the infrared illumination source 23 is a higher powered wide beam, for illuminating other individuals and the surrounding environment.

6) The device begins transmitting ongoing streaming video and sound data and other data to the data storage facility 7 where compatible recording equipment is permanently on standby to receive, record and log the automatic transmission of mission critical data from the handheld device I in real time. The video data transmitted are simultaneously displayed on the device screen 13, enabling the user to monitor what video data are being transmitted.

...

8) Within 6 seconds of pressing the eyewitness button 12 the hybrid A-GPS circuitry obtains sufficient data from the satellite constellation 11 and cellular network 4. From such data the location coordinates are calculated. The calculation is performed by the handheld device 1 or network 4 and the coordinates are immediately transmitted to the data storage facility 7, integrated with the continuing video stream, sound data and other data. As the transmission of video and sound and other data continues, hybrid A-GPS data are regularly updated and transmitted to the data storage facility 7.

...

Once a successful connection is made between the handheld device 1 and the data storage facility 7, the recorded images, sound, geographical coordinates detailing the location of the device 1, and timestamp generated by the handheld device 1 against the recordings, and other data stored in the memory chips and/or memory cards and/or memory discs and/or hard drives, and/or tapes and/or other data storage facilities of the handheld device 1 are immediately and automatically transmitted by the handheld device 1 to the data storage facility 7 for safe storage.

Once the data storage facility 7 has received and recorded the data stored in the memory components of the handheld device 1, the data storage facility 7 continues to record all images, sounds and other live signals detected and transmitted by the handheld device 1 in real time, for as long as the connection between the handheld device 1 and the data storage facility 7 is maintained.

...

The time involved between pressing the eyewitness button 12 and safely storing images and data at the data storage facility 7 linking an individual to a specific place at a specific time takes no more than a few seconds, providing that a clear connection exists between the device 1 and the cellular network 4 at the time, or that a dial-up telephone connection is obtained at the first automatic dialling attempt.

189. *Walker*'s disclosure related to eyewitness button 12 is consistent with how the '404 patent describes a panic button, as described above in §X.A.1.e(i).

190. For context, I note that unlike limitations 9[e] and 13[e], limitation 15[e] does not require that the panic button itself be pressed. Claim 15 requires that the panic button is activated by “a button sequence,” but it does not require that the button sequence is input on the mobile device itself. Nor does the claim limitation exclude activating the panic button by a “button sequence” that is input on a remote device. A person having ordinary skill in the art would not have understood the specification or prosecution history of the '404 patent to require a narrower interpretation of the claimed “button sequence.”

191. *Walker* also discloses that “the user of the handheld device may activate or deactivate the eyewitness button 12 of the device and other device functionality remotely by dialling [*sic*] a telephone number related to the handheld device from another handheld device ... and entering a code known only to the user”:

In another embodiment of the invention the user of the handheld device may activate or deactivate the eyewitness button 12 of the device and other device functionality remotely by dialling a telephone number related to the handheld device from another

handheld device or from any telephone device connected to the international telephone network, or through connecting to the handheld device through email or through an electronic messaging service or through a website or other internet based or electronic or wireless connection, or through the data storage facility 7, or data storage facility network, or through a cellular network, and entering a code known only to the user, and wherein the user may activate the eyewitness button or other device functionality silently and without causing the device to sound a ringing tone or light up any illumination components of the device on making a connection to the device. Such embodiment enables the user and/or authorities to determine the location of the device, and to capture data relating to it's [sic] whereabouts. Such data may lead to identifying an individual or individuals currently in possession of the device, and such access may prevent any such individuals from making any calls or communications from the device.

EX1007 ¶[0130]

192. In my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood that inputting a telephone number and/or a code comprises inputting a button sequence because they both encompass inputting a sequence of buttons on a device.

193. This is consistent with how the '404 patent describes this feature:

For example, a panic button can trigger the image/audio data and location information being obtained. Further, the panic but

ton can also trigger a separate self-defense mechanism such as pepper spray, mace, or a personal alarm. *These can be triggered, by a panic button or buttons or button sequence.*

EX1001, 7:16-21

194. Accordingly, in my opinion, a person having ordinary skill in the art would have understood that *Walker* discloses or suggests a mobile device with an eyewitness button 12 (“a panic button”) that the user may activate by entering a telephone number and/or a code (“wherein the panic button is activated by a button sequence”).

(ii) A panic button “adapted to activate the transmitting unit when activated”

195. As explained in §X.A.1.e(ii), *Walker*’s disclosure is also consistent with how the ’404 patent describes “activating” the transmitting unit to perform a function. Accordingly, in my opinion, a person having ordinary skill in the art would have understood that *Walker* discloses or suggests that the eyewitness button 12 (“panic button”) triggers the device to obtain and transmit the data (“adapted to activate the transmitting unit when activated”).

D. GROUND 3A: ZELLNER IN COMBINATION WITH KIM RENDERS OBVIOUS CLAIMS 9-14

196. For purposes of my analysis below, I discuss certain aspects of the “IP device 20” as described and illustrated with reference to *Zellner*’s Figures 3-6. Figure 3 is described schematically illustrating “IP device 20” sending

emergency help request messages. *Zellner*, 5:16-19. Figures 4 and 5 further detail the IP device 20 (i.e., the IP device 20 illustrated in Figure 3). *Id.*, 6:55-57, 7:65-67. *Zellner* explains that Figure 5 is identical to Figure 4 except for the addition of a digital camera. *Id.*, 8:28-29. And *Zellner* describes Figure 6 as showing the “circuit blocks within the housing 26” of Figure 4 (*id.*, 7:10-12) and that it also includes the digital camera of the embodiment of Figure 5 (*id.*, 13:9-13). A person having ordinary skill in the art would have understood *Zellner* to expressly disclose combining its description of IP device 20 of Figures 3-6 together.

1. CLAIM 9

a. 9[pre] A mobile device, comprising

197. In my opinion, to the extent the preamble is limiting, *Zellner* discloses or suggests “[a] mobile device.”

198. *Zellner* discloses an “IP device 20” implemented as a “portable or wearable unit”:

The term “IP device” may be construed to include a number of devices equipped with panic button and capable of TCP/IP-based data communication when the panic button is activated. The panic button functionality may be accomplished with a hardware panic button (for example, the panic button 24 in FIG. 4) or a software panic button (described hereinbelow with reference to FIG. 7).

The IP devices may include commercially available gadgets such

as a wireless pager, a cellular telephone, a hand-held computing device (similar, e.g., to a PalmPilot), etc., modified to include the panic button functionality as described hereinbelow.

Alternatively, a number of household devices, e.g., an alarm clock or a refrigerator, may be equipped with Internet access capability and a panic button to be covered by the term “IP device.”

EX1008 5:65-6:12.

FIG. 4 is an illustration of an embodiment of the IP device 20 of the present invention wherein the IP device 20 has a physically built-in panic button 24. *The IP device 20 may be a portable or wearable unit.*

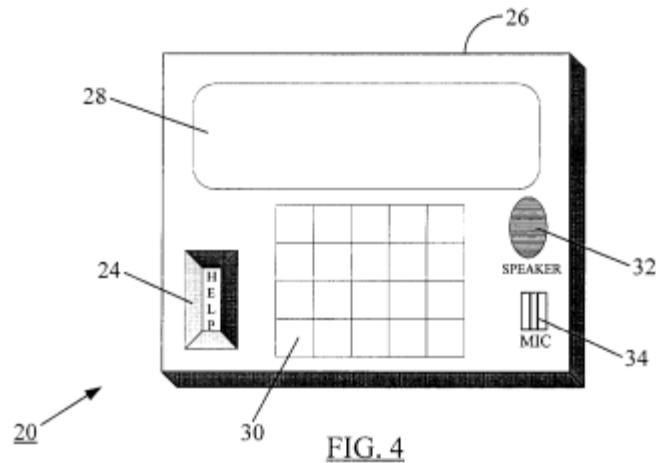
Id. 6:55-58.

In the case of a *hand-held, portable IP device 20*, the housing 26 may be built of relatively hard and unbreakable plastic or a shock-resistant material ABS (Acrylonitrile Butadiene Styrene) so that to allow a user, for example, to carry around the IP device 20 on his/her person.

Id. 7:6-9.

The web browser software may include, for example, an HTML browser or a WAP (Wireless Application Protocol) browser because of the small size and *portable nature of the IP device 20* and because of the smaller display 28 and limited memory space (in the memory unit 46) available for the IP device 20.

Id. 11:38-44.



Zellner FIG. 4

199. Accordingly, in my opinion, a person having ordinary skill in the art would have understood that *Zellner* discloses or suggests a portable or wearable unit (“a mobile device”).

b. 9[a] a camera unit, adapted to obtain at least one of image data and audio data;

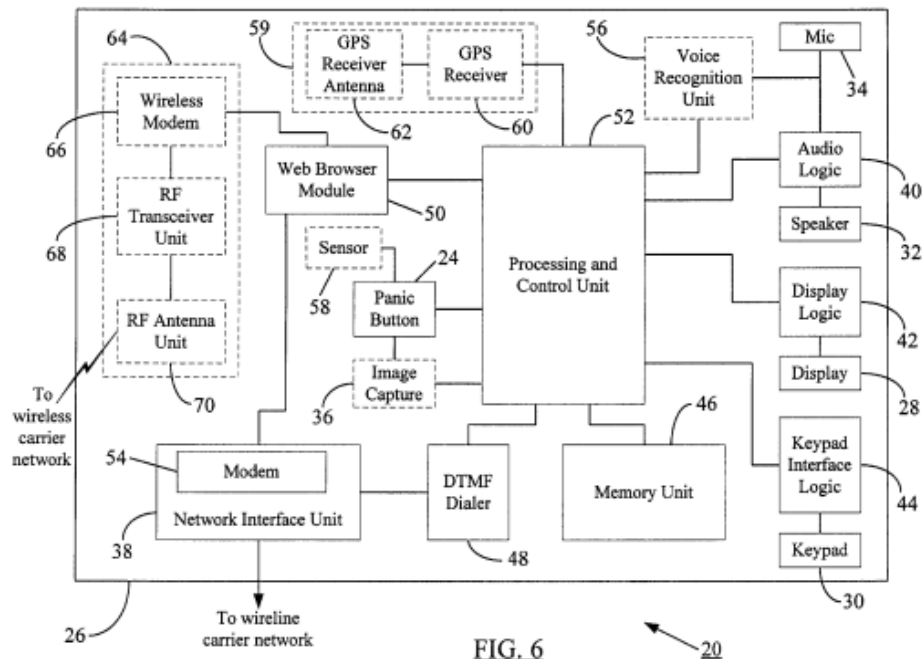
200. In my opinion, *Zellner* discloses or suggests “a camera unit, adapted to obtain at least one of image data and audio data.”

201. *Zellner* discloses that the portable device includes a “built-in digital camera” or “image capture device” to take “snapshots” or “motion pictures”:

FIG. 5 illustrates another embodiment of the IP device 20 having a built-in digital camera or other image capture device 36. A miniature digital camera 36 may be built into the housing 26 to take quick snapshots, or motion pictures, of the environment surrounding the user of the IP device 20. The camera 36 may be activated when the panic button 24 is pressed by the user and the

camera 36 may remain activated for a predetermined time thereafter (e.g., for 30-60 seconds) prior to automatically shutting off itself. The camera lens may rotate within the housing 26 to “cover” a circular view angle of (or approximate) 360°. The video information provided by images shot by the camera 36 may be helpful in, for example, medical treatment of the user of the IP device 20, in law enforcement (e.g., when the user activates the panic button 24 in response to a burglary attempt or in response to a threat to the user’s physical safety), etc.

EX1008, 7:65-8:14.



EX1008 at FIG. 6.

202. *Zellner* also discloses that the “IP device 20” is capable of video conferencing and transmitting the “user’s voice” and “audio files” to an emergency services center:

Furthermore, *the user’s voice may also be sent to the ESC as one or more TCP/IP data packets* over the internet.

Id. 3:21-23.

For example, in the case of routine e-mail or “chat” messages, more latency may be tolerated. However, the IP-based network may establish that certain emergency messages (e.g., messages originating from the IP device 20) or other messages (e.g., video conferencing data) requiring instant transmission of the message without delay may be assigned the highest priority or “class of service” when the IP network has to allocate its data transmission bandwidth among the competing data packets.

Id. 6:46-54.

The user of the IP device may speak into the microphone 34 to transmit the user’s voice over the Internet 22.

Id. 9:22-23.

203. *Zellner*’s description is consistent with how the ’404 patent describes this feature:

In another embodiment, the present invention provides a self-defense device including a self-defense mechanism which is integrated with a mobile phone/device such that *when the self-defense mechanism is activated, a camera built into the mobile phone/device takes an image of*

the attacker, and the mobile phone/device sends image data and audio data to the authorities along with specific information such as, for example, the name and description of the owner of the self-defense device, location information, a time and date stamp, etc. In this way, the present invention utilizes a built-in camera to take still or moving images of the attacker and send the image and/or audio data to the authorities along with the specific information. The self-defense mechanism can be a vial containing pepper spray or mace, for example, or simply a separate panic button located on the device which activates the above-mentioned processes. Of course, the present invention is not limited to the examples discussed herein.

EX1001, 3:4-15

204. In my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood “snapshots” and “motion pictures” comprise “image data.” A person of ordinary skill in the art would have also understood the “user’s voice” and “audio files” to comprise “audio data.”

205. Accordingly, in my opinion, a person of ordinary skill in the art would have understood that *Zellner* discloses or suggests a portable or wearable unit (“mobile device”) with a camera (“camera unit”) that captures pictures,

videos, and/or sound (“adapted to obtain at least one of image data and audio data.”)

c. 9[b] a location unit, adapted to obtain location data

206. In my opinion, *Zellner* discloses or suggests “a location unit, adapted to obtain location data.”

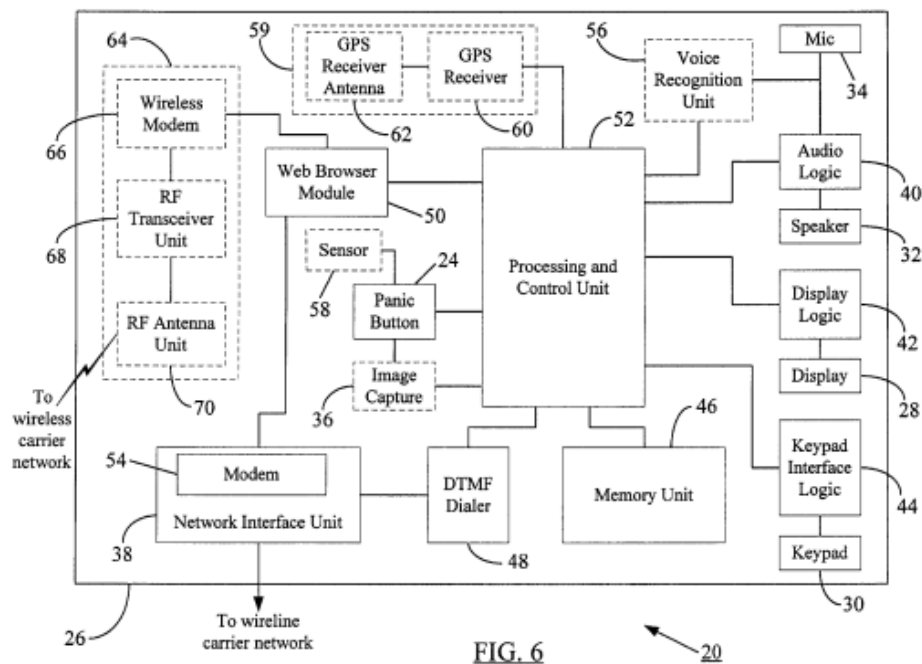
207. *Zellner* discloses that the portable device includes “a user location identifier 59” which further includes “a GPS receiver 60 and a GPS receiver antenna 62”:

[A] user location identifier 59 including a GPS (Global Positioning System) receiver 60 and a GPS receiver antenna 62; and a wireless data communication module 64 including a wireless modem 66, an RF (Radio Frequency) transceiver unit 68 and an RF antenna unit 70.

EX1008, 13:17-23.

In one embodiment, ***the device may include a location identifier unit that supplies the current location of the device (and, hence, of the user operating the device) to the processing unit to be included as part of the help request message so that ESC personnel may efficiently locate the user who requested the emergency help.***

Id. 3:34-38.



Zellner FIG. 6

208. Zellner discloses that the GPS receiver antenna receives “location signals” and transfers those signals to the GPS receiver 60, and identifies the current location of the device:

The user location identifier 59 within the housing 26 is shown to include a GPS receiver 60 and a GPS receiver antenna 62. *The GPS receiver antenna 62 may be provided on the housing 26 to continuously receive location signals from geostationary satellites and transfer those signals to the GPS receiver 60 to identify the current location of the IP device 20 and, hence, of the user carrying the IP device 20.* Instead of a built-in location identifier 59, the housing 26 may be provided with a port (not

shown) to receive an external location identifier (with or without the receiver antenna 62) that may be attached to the port when needed. The GPS location identifier 59 may perform better in an outdoor environment. This may be useful when the user is on the road or at a remote location where access to a telephone may not be easily available. In that case, the user's location may be transmitted along with the emergency help request message to the ESC 12. ***The user location identifier 59 may supply the PCU 52 with the requisite location information and the PCU 52, with the help of an appropriate web browser module 50 and the wireless data communication module 64 (described hereinbelow), may send the emergency help request message along with the user location information over the Internet 22 to the ESC 12.*** The commercially available Megellan GPS receiver may be included as part of the user location identifier 59.

Id. 14:14-38. To note, although *Zellner* describes receiving location signals from “geostationary satellites,” I know based my own experience that a person having ordinary skill in the art would have understood that GPS satellites are not geostationary. This is a common enough error that a person having ordinary skill in the art would have understood *Zellner* to be referring to the Medium Earth Orbits (MEOs) actually used by the GPS satellites. And regardless, a person

having ordinary skill in the art would have understood *Zellner* to disclose a GPS receiver that would receive and process GPS signals to produce the location of a GPS receiver, using the GPS satellites, as was well-known in the art at the time of *Zellner's* invention, even though *Zellner's* description of the satellite orbits is not technically correct. I also note that *Zellner* refers to a “Megellan GPS receiver,” but a person having ordinary skill in the art would have understood that to be a typo and that *Zellner* meant to refer to “Magellan,” a company which was a major producer of GPS receivers at the time of the *Zellner* patent.

209. *Zellner's* disclosure is consistent with the '404 patent's description of this feature, as described in §X.A.1.c. The '404 patent states:

The present invention can obtain location information in a number of different ways, for example through a tower-based location system. As is well known in the art, cell towers triangulate to figure out where a person is. As another example, *the present invention can also obtain location information through a form of GPS (Global Positioning System) on the device (GPS or AGPS, which is assisted GPS). Location information for the present invention can be an x-y coordinate or close to it that the phone obtains and transmits to 911.*

EX1001, 6:64-7:6

210. In my opinion, and based on my background and experience, a person having ordinary skill in the art would have understood that “location signals” and the “location information” constitute “location data.”

211. Accordingly, in my opinion, *Zellner* discloses or suggests that the portable device includes a user location identifier (“location unit”) that is used to identify the location of the device (“adapted to obtain location data.”).

d. 9[c] a transmitting unit, adapted to transmit as emergency information the image data, the audio data, and the location data along with the specific information including owner identification information; and

212. In my opinion, *Zellner* discloses or suggests “a transmitting unit, adapted to transmit as emergency information the image data, the audio data, and the location data along with the specific information including owner identification information.”

213. *Zellner* discloses that the data is transmitted to an emergency services center (“ESC”) via the internet through various transmission technologies. For example, *Zellner* discloses that the portable device includes “a wireless data communication module” for communication over a cellular network:

The RF antenna 70 provides the necessary signaling interface between a wireless carrier network 14 and the web browser module 50 that needs to access the wireless network 14.

The wireless data communication module 64 employs wireless devices to transfer data and information between the IP device 20 and the ESC 12 over the Internet 22. An antenna, e.g., an RF (radio frequency) antenna 70, may be provided on the housing 26 of the butt set 74 to allow wireless data communication. In the event of wireless data communication, the NIU 38 (including the wireline data modem, i.e., the modem 54) may remain inactive. Furthermore, when the IP device 20 is equipped with cellular telephone features or paging device features, the housing 26 for that IP device 20 may include only the wireless data communication module 64 and may omit the NIU 38. Here, data communication may be accomplished via a wireless modem 66 using a wireless carrier network 14. If the wireless carrier network 14 is a cellular network (e.g., a TDMA-based wireless network or a CDMA-based (Code Division Multiple Access) wireless network, or a GSM-based (Global System for Mobile Communications) wireless network), then the wireless modem 66 may be capable of data transfer using the message format supported by the given cellular network.

The web browser module 50 in the housing 26 may be configured to transfer data over a wireless carrier network 14 and, hence, the web browser module 50 may be connected to the wireless modem 66. The web browser module 50 may include a WAP (Wireless Application Protocol) browser to access the Internet 22. The WAP browser in the web browser module 50 may transfer

data over the Internet 22 using a WAP-supported data format, e.g., the WML (Wireless Markup Language) format. In one embodiment, the web browser module 50 may be configured to responsively connect to a wireline data modem (e.g., the modem 54) or a (wireless modem 66 depending on the desired mode of data communication. A web browser module 50 with an HTML browser may be similarly configured to perform data transmission and reception operations using wireless devices (similar to, for example, the wireless data communication module 64).

Id. 14:39-15:9.

214. *Zellner* further discloses an additional example where the portable device communicates wirelessly with a base unit that is physically connected to a wireline carrier network:

When the IP device 20 is portable, it may have an associated base unit (not shown) to transmit appropriate signals to the carrier network 14. ***For example, the IP device 20 may communicate wirelessly with its corresponding base unit and the base unit may be physically connected to a telephone line to forward messages received from the IP unit 20 to the carrier network 14, which, here, may be the PSTN.***

Id. 6:63-7:2.

215. *Zellner* further discloses that the portable device uses the TCP/IP protocol, and email or instant messaging to transmit the data:

Furthermore, *the user's voice may also be sent to the ESC as one or more TCP/IP data packets over the Internet.*

Id. 3:21-23.

The images captured by the digital camera 36 *may be transmitted as TCP/IP data packets to the ESC 12* upon activation of the panic button 24.

Id. 8:15-17.

The ESC 12 may be configured to *automatically transmit pre-recorded audio information over the Internet 22 (via TCP/IP message packets)* when the ESC 12 receives an emergency request message from the IP device 20.

Id. 9:17-21.

Upon activation of the panic button 24, the PCU 52 may retrieve the personal information from the memory 46 and *may transmit it to the web browser module 50, which, in turn, may immediately send the information to the ESC 12 via TCP/IP packets sent over the Internet 22.*

Id. 9:39-44.

Activation of the panic button by a user in need of emergency help results in *automatic transmission of one or more TCP/IP messages over the Internet to an emergency service center requesting emergency help* and identifying the user in need of such help.

Id. 19:29-34.

1. A device for requesting emergency assistance, comprising: a processing unit, a panic button coupled to the processing unit, wherein the panic button is configured to send a first indication to the processing unit, wherein the sending of the first indication is in response to a user of said device activating the panic button; and *a web browser module coupled to the processing unit, wherein the processing unit is configured to send a second indication to said web browser module, wherein the sending of the second indication is in response to the first indication, and wherein said web browser module is configured to deliver a help request message in a TCP/IP (Transmission Control Protocol/Internet Protocol) format to an emergency service center (ESC), wherein the delivering of the help request message is in response to the second indication.*

Id. claim 1

11. *The device of claim 1, further comprising a memory unit coupled to the processing unit, wherein the memory unit is configured to store therein said help request message in one of said TCP/IP format and a non-TCP/IP format.*

Id. claim 11

The IP device 20 may communicate with the ESC 12 using, for example, *the instant messaging functionality supported by an IP-based network, e.g., the Internet 22. The instant messaging feature allows the IP device 20 to establish a direct session or a virtual connection with the remote ESC 12 via the Internet 22.* In one embodiment, the IP-based network (here, the Internet 22),

and preferably the carrier network 14 as well, may employ “classes of service” or “quality of service” classification schemes for data packets handled by the network. Some parameters that affect a network's classification scheme include, for example, the data bandwidth required, the latency to be tolerated during a message transmission and the acceptable error-rate during a message transmission. For example, in the case of routine e-mail or “chat” messages, more latency may be tolerated. *However, the IP-based network may establish that certain emergency messages (e.g., messages originating from the IP device 20) or other messages (e.g., video conferencing data) requiring instant transmission of the message without delay may be assigned the highest priority or “class of service” when the IP network has to allocate its data transmission bandwidth among the competing data packets.*

Id. 6:33-54.

The user may “program” the IP device 20 with pertinent data about the ESC 12 including, for example, the name of the ESC 12, the IP address of the ESC 12, the telephone number and name of the contact person at the ESC 12, *the e-mail address of the ESC 12*, etc. These data may be entered using various keys on the keypad 30. The web browser module 50 may need a portion of such data to determine how to access the ESC 12 over the Internet 22.

Id. 10:3-11

It is noted that the discussion given hereinbefore with respect to carrier network 14 applies equally to one or both of the carrier network A 78 and carrier network B 80. *For example, carrier*

network B 80 may be a wireless carrier network (e.g., a cellular phone network) whereas the carrier network A 78 may be a wireline carrier network (e.g., the PSTN).

In one embodiment, the carrier network B 80 may also include the Internet 22. *In other words, the SSP18 may first receive the emergency help request message from the IP device 20 and may, in turn, forward that message (with or without additional information) to the ESC 12 over the Internet 22 (i.e., via the carrier network B 80).* This may be helpful to prevent confusion and flooding of TCP/IP messages at the ESC 12 when different users directly contact the ESC 12. *Instead, the SSP 18 may function like a “hub” that receives messages from all of its subscribers and then forwards them to the ESC 12.*

Id. 17:27-44

216. *Zellner’s* disclosure is consistent with how the ’404 patent describes the “transmitting unit” as discussed in §X.A.1.d.

217. A person of ordinary skill in the art would have understood that cellular telephones have cellular communications equipment, and that TCP/IP is a standard internet protocol.

218. In view of the above, in my opinion, a person having ordinary skill in the art would have understood that *Zellner* to disclose or suggest a “transmitting unit.”

219. *Zellner* also discloses that the portable device transmits various data including image, audio, and location data:

The images captured by the digital camera 36 may be transmitted as TCP/IP data packets to the ESC 12 upon activation of the panic button 24.

Id. 8:15-17.

As depicted in FIG. 4, the housing 26 may include built therein a speaker 32 and a microphone 34. In one embodiment, after invoking the emergency help functionality by pressing the panic button 24, ***the user of the IP device 20 may additionally speak into the microphone 34. The IP device 20 may be configured to transmit the user's voice over the Internet and to the ESC 12 by using known voice-over-IP methods.*** The user may also be able to listen to voice responses from the operator at the ESC 12 via the speaker 32. These voice responses may be transmitted over the Internet.

Id. 7:46-55.

Furthermore, ***the user's voice may also be sent to the ESC as one or more TCP/IP data packets*** over the Internet.

Id. 3:21-23.

The audio logic unit 40 may be connected to the microphone 34 and the speaker 32. The speaker 32 may be activated by the audio logic unit 40 when the PCU 52 informs the audio logic unit 40 that the panic button 24 has been pushed. Voice messages sent by, for example, the service personnel at the ESC 12, may first be received by the PCU 52 (via the NIU 38) and the PCU 52 may

transmit these signals to the audio logic unit 40 to be sent to the speaker 32 for generating audible sound. Alternatively, any digital audio files received by the IP device 20 (using the NIU 38) over the Internet 22 may first be sent to the web browser module 50 to retrieve the audio file data therefrom. The browser module 50 may then send the audio data to the PCU 52, which, in turn, forwards the audio data to the audio logic unit 40 and eventually to the speaker 32. ***The ESC 12 may be configured to automatically transmit pre-recorded audio information over the Internet 22 (via TCP/IP message packets) when the ESC 12 receives an emergency request message from the IP device 20.***

The user of the IP device 20 may speak into the microphone 34 to transmit the user's voice over the Internet 22. The audio logic unit 40 receives the electrical audio signals from the microphone 34 and sends them to the PCU 52, which, in conjunction with the browser module 50, transmits the user's voice over the Internet 22 using the NIU 38. ***In one embodiment, the user may store the user's personal identification information as a digital audio file in the memory unit 46 by speaking into the microphone 34.*** The PCU 52 may convert the audio electrical signals received from the audio logic unit 40 into the predetermined digital audio file format and store the user's personal information in the memory unit 46. The personal information may include the user's name, address, any known medical condition, contact information in case of emergency, etc. The digital audio file formats for the user's personal information may include file extensions such as, for example, “.WAV” (wave file), “.AIFF”(Audio Interchange File

Format), “.AU”(audio file), etc. *Upon activation of the panic button 24, the PCU 52 may retrieve the personal information from the memory 46 and may transmit it to the web browser module 50, which, in turn, may immediately send the information to the ESC 12 via TCP/IP packets sent over the Internet 22.*

Id. 9:3-44.

The GPS location identifier 59 may perform better in an outdoor environment. This may be useful when the user is on the road or at a remote location where access to a telephone may not be easily available. In that case, *the user's location may be transmitted along with the emergency help request message to the ESC 12. The user location identifier 59 may supply the PCU 52 with the requisite location information and the PCU 52, with the help of an appropriate web browser module 50 and the wireless data communication module 64 (described hereinbelow), may send the emergency help request message along with the user location information over the Internet 22 to the ESC 12.*

Id. 14:25-36.

In one embodiment, the *device may include a location identifier unit that supplies the current location of the device (and, hence, of the user operating the device) to the processing unit to be included as part of the help request message* so that ESC personnel may efficiently locate the user who requested the emergency help.

Id. 3:34-39.

220. *Zellner* discloses that the image, audio, and location data are transmitted to an ESC for the purposes of requesting help:

Activation of the panic button by the user results in the device ***automatically transmitting one or more TCP/IP messages over the Internet to an emergency service center requesting emergency help and identifying the user requesting such help.***

Id. Abstract

The foregoing describes exemplary embodiments of an IP device having a built-in panic button that may be implemented in hardware or software. Activation of the panic button by a user in need of emergency help results in automatic transmission of one or more TCP/IP messages over the Internet to an ***emergency service center requesting emergency help and identifying the user in need of such help.***

Id. 19:27-34.

221. A person of ordinary skill in the art would have therefore understood that the transmitted image, audio, and location data therefore related to an ongoing emergency, and that *Zellner*'s disclosure is consistent with how the '404 patent describes "emergency information," as discussed in §X.A.1.d.

222. Thus a person of ordinary skill in the art would have understood *Zellner* to disclose or suggest that the transmitting unit of the portable device is

“adapted to transmit emergency information the image data, the audio data, and the location data.”

223. In addition to transmitting image, audio, and location information, *Zellner* discloses transmitting personal information about the user such as a name or address, which can be recorded in text or audio. In particular, *Zellner* details transmitting a pre-recorded audio file which includes a recording of the user providing his/her personal information. *Zellner* also explains that the user can input the personal information in text using a keyboard:

The device may further include a memory unit to store the help request message to be sent to the ESC. *The memory may also store various personal information about the user, e.g., the identity of the user, the location or address of the user, any known medical condition the user is suffering from, etc. Such additional information may be included by the processing unit as part of the help request message sent to the ESC.*

Id. 3:14-21.

In one embodiment, *the user may store the user's personal identification information as a digital audio file in the memory unit 46 by speaking into the microphone 34.* The PCU 52 may convert the audio electrical signals received from the audio logic unit 40 into the predetermined digital audio file format and store the user's personal information in the memory unit 46. *The personal information may include the user's name, address, any known medical condition, contact information in case of*

emergency, etc. The digital audio file formats for the user's personal information may include file extensions such as, for example, “.WAV” (wave file), “.AIFF”(Audio Interchange File Format), “.AU”(audio file), etc. ***Upon activation of the panic button 24, the PCU 52 may retrieve the personal information from the memory 46 and may transmit it to the web browser module 50, which, in turn, may immediately send the information to the ESC 12 via TCP/IP packets sent over the Internet 22.***

Id. 9:27-44.

These data may be entered using various keys on the keypad 30. The web browser module 50 may need a portion of such data to determine how to access the ESC 12 over the Internet 22. ***Furthermore, the user may also prefer to enter personal information about the user, e.g., the user's name, the address of the user's contact location, any known medical condition, name and contact information about the user's family physician, etc.***

The keypad interface 44 transmits the signals received from the keyboard 30 to the PCU 52 for further processing. The PCU 52 decodes the received signals and accordingly instructs the appropriate circuit elements for necessary action. For example, when the user enters the user's personal information and the data pertaining to the ESC 12, the keypad interface logic 44 may send all the data to the PCU 52, which may instruct the memory unit 46 to store the received data therein. ***The PCU 52 may store the user's identification information, the ESC 12 access data, etc.,***

in the memory 46 using one of a number of digital text formats, e.g., HTML (Hyper Text Markup Language) format, ASCII (American Standard Code for Information Interchange) format, XML (Extensible Markup Language) text file format developed by W3C (World Wide Web Consortium), etc.

Id. 10:8-30.

The memory or storage unit 46 provides memory for storage of data, such as the user's personal information as discussed hereinbefore. The data stored locally in the memory unit 46 may be text, audio or video data and may include a number of digital file formats as described hereinbefore. For example, data that may be sent over the Internet 22 may be in the HTML or the WML (Wireless Markup Language) formats depending on whether the web browser module 50 is used with a wireline carrier network or a wireless carrier network respectively as described hereinbelow.

Id. 10:59-11:2.

The memory unit 46 may include volatile and/or non-volatile memory, such as RAM (Random Access Memory), ROM (Read Only Memory), EEPROM (Electrically Erasable Programmable Read Only Memory), flash memory, or other similar memory units. A volatile memory may lose the data stored therein if the power applied thereto is removed. *The personal information about the user (as an audio file or as a text file) as well as the contact information about the ESC 12 may be stored in the non-volatile portion of the memory 46.* On the other hand, a paging message may be stored in the volatile portion (or temporary

storage) of the memory 46 for an IP device 20 that may also function as a wireless pager.

Id. 11:7-19.

Furthermore, the web browser module 50 may also be automatically activated once the panic button 24 is pressed by the user of the IP device 20. ***In that case, the web browser 50 may retrieve (via the PCU 52) relevant locally-stored information (e.g., the web address of the ESC 12 or the personal information about the user) from the memory unit 46 and transmit an appropriate portion of that information over the Internet 22 in response to the activation of the panic button 24.*** The web browser module 50 interacts with the PCU 52 to execute necessary software routines for Internet access. The software routines, upon execution, activate the modem 54 in the NIU 38 to establish an electrical connection with a wireline carrier network (e.g., via a telephone line (not shown)) to accomplish dialed Internet access. In one embodiment, the web browser module 50 (including its hardware and/or software elements) may be a part of the PCU 52 and the PCU 52 may directly perform web browsing or information delivery over the Internet 22

Id. 11:64-12:15.

224. In my opinion, and based on my experience and background, a person of ordinary skill in the art would have understood that the user of the device is, at least sometimes, the owner of the device. In other words, a person having ordinary skill in the art would have appreciated that in practical

circumstances, the user of the device is the owner of the device. Thus, although *Zellner* describes transmitting information about the “user,” a person having ordinary skill in the art would have understood that same information is at least sometimes information about the “owner” of the device.

225. *Zellner* further discloses all four of the image, audio, location data, and personal information in response to the user pressing the panic button. More particularly, *Zellner* discloses transmitting captured images upon activation of the panic button:

The images captured by the digital camera 36 may be transmitted as TCP/IP data packets to the ESC 12 ***upon activation of the panic button 24.***

Id. 8:15-17.

226. *Zellner* discloses transmitting the audio data upon activation of the panic button:

In one embodiment, after invoking the emergency help functionality by pressing the panic button 24, the user of the IP device 20 may additionally speak into the microphone 34. ***The IP device 20 may be configured to transmit the user's voice over the Internet and to the ESC 12 by using known voice-over-IP methods.*** The user may also be able to listen to voice responses from the operator at the ESC 12 via the speaker 32.

Id. 7:46-55;

Furthermore, the user's voice may also be sent to the ESC as one or more TCP/IP data packets over the Internet.

The panic button may be implemented in hardware or software. In a hardware implementation, the panic button may be provided as a button on the face of the housing that can be pushed by the user when in need of emergency help. In a software implementation, a panic button icon may be displayed on a touch-sensitive display screen provided on the housing. ***The user may touch the icon to activate the panic button functionality, i.e., to transmit the help request message to the ESC.***

Id., 3:21-32

The audio logic unit 40 may be connected to the microphone 34 and the speaker 32. The speaker 32 may be activated by the audio logic unit 40 when the PCU 52 informs the audio logic unit 40 that the panic button 24 has been pushed. Voice messages sent by, for example, the service personnel at the ESC 12, may first be received by the PCU 52 (via the NIU 38) and the PCU 52 may transmit these signals to the audio logic unit 40 to be sent to the speaker 32 for generating audible sound. Alternatively, any digital audio files received by the IP device 20 (using the NIU 38) over the Internet 22 may first be sent to the web browser module 50 to retrieve the audio file data therefrom. The browser module 50 may then send the audio data to the PCU 52, which, in turn, forwards the audio data to the audio logic unit 40 and eventually to the speaker 32. ***The ESC 12 may be configured to automatically transmit pre-recorded audio information over the***

Internet 22 (via TCP/IP message packets) when the ESC 12 receives an emergency request message from the IP device 20.

The user of the IP device 20 may speak into the microphone 34 to transmit the user's voice over the Internet 22. The audio logic unit 40 receives the electrical audio signals from the microphone 34 and sends them to the PCU 52, which, in conjunction with the browser module 50, transmits the user's voice over the Internet 22 using the NIU 38. In one embodiment, the user may store the user's personal identification information as a digital audio file in the memory unit 46 by speaking into the microphone 34. The PCU 52 may convert the audio electrical signals received from the audio logic unit 40 into the predetermined digital audio file format and store the user's personal information in the memory unit 46. The personal information may include the user's name, address, any known medical condition, contact information in case of emergency, etc. The digital audio file formats for the user's personal information may include file extensions such as, for example, ".WAV" (wave file), ".AIFF" (Audio Interchange File Format), ".AU" (audio file), etc. Upon activation of the panic button 24, the PCU 52 may retrieve the personal information from the memory 46 and may transmit it to the web browser module 50, which, in turn, may immediately send the information to the ESC 12 via TCP/IP packets sent over the Internet 22.

Id. 9:3-44.

227. *Zellner* discloses transmitting the location data upon activation of the panic button:

The GPS location identifier 59 may perform better in an outdoor environment. This may be useful when the user is on the road or at a remote location where access to a telephone may not be easily available. *In that case, the user's location may be transmitted along with the emergency help request message to the ESC 12. The user location identifier 59 may supply the PCU 52 with the requisite location information and the PCU 52, with the help of an appropriate web browser module 50 and the wireless data communication module 64 (described hereinbelow), may send the emergency help request message along with the user location information over the Internet 22 to the ESC 12.*

Id. 14:25-36.

In one embodiment, *the device may include a location identifier unit that supplies the current location of the device (and, hence, of the user operating the device) to the processing unit to be included as part of the help request message* so that ESC personnel may efficiently locate the user who requested the emergency help.

Id., 3:34-39.

3. The device of claim 1, further comprising a user location identifier coupled to the processing unit, *wherein the user location identifier is configured to ascertain a location of the user activating said panic button.*

Id. claim 3

228. *Zellner* discloses transmitting personal information about the user such as a name or address upon activation of the panic button:

The device may further include a memory unit to store the help request message to be sent to the ESC. *The memory may also store various personal information about the user, e.g., the identity of the user, the location or address of the user, any known medical condition the user is suffering from, etc. Such additional information may be included by the processing unit as part of the help request message sent to the ESC.*

Id. 3:14-21.

In one embodiment, *the user may store the user's personal identification information as a digital audio file in the memory unit 46 by speaking into the microphone 34.* The PCU 52 may convert the audio electrical signals received from the audio logic unit 40 into the predetermined digital audio file format and store the user's personal information in the memory unit 46. The personal information may include the user's name, address, any known medical condition, contact information in case of emergency, etc. The digital audio file formats for the user's personal information may include file extensions such as, for example, “.WAV” (wave file), “.AIFF”(Audio Interchange File Format), “.AU”(audio file), etc. *Upon activation of the panic button 24, the PCU 52 may retrieve the personal information from the memory 46 and may transmit it to the web browser module 50, which, in turn, may immediately send the*

information to the ESC 12 via TCP/IP packets sent over the Internet 22.

Id. 9:27-44.

These data may be entered using various keys on the keypad 30. The web browser module 50 may need a portion of such data to determine how to access the ESC 12 over the Internet 22. Furthermore, the user may also prefer to enter personal information about the user, e.g., the user's name, the address of the user's contact location, any known medical condition, name and contact information about the user's family physician, etc.

The keypad interface 44 transmits the signals received from the keyboard 30 to the PCU 52 for further processing. The PCU 52 decodes the received signals and accordingly instructs the appropriate circuit elements for necessary action. For example, when the user enters the user's personal information and the data pertaining to the ESC 12, the keypad interface logic 44 may send all the data to the PCU 52, which may instruct the memory unit 46 to store the received data therein. *The PCU 52 may store the user's identification information, the ESC 12 access data, etc., in the memory 46 using one of a number of digital text formats, e.g., HTML (Hyper Text Markup Language) format, ASCII (American Standard Code for Information Interchange) format, XML (Extensible Markup Language) text file format developed by W3C (World Wide Web Consortium), etc.*

Id. 10:8-30.

The memory or storage unit 46 provides memory for storage of data, *such as the user's personal information as discussed hereinbefore*. The data stored locally in the memory unit 46 may be text, audio or video data and may include a number of digital file formats as described hereinbefore. For example, data that may be sent over the Internet 22 may be in the HTML or the WML (Wireless Markup Language) formats depending on whether the web browser module 50 is used with a wireline carrier network or a wireless carrier network respectively as described hereinbelow.

Id. 10:59-11:2.

The memory unit 46 may include volatile and/or non-volatile memory, such as RAM (Random Access Memory), ROM (Read Only Memory), EEPROM (Electrically Erasable Programmable Read Only Memory), flash memory, or other similar memory units. A volatile memory may lose the data stored therein if the power applied thereto is removed. *The personal information about the user (as an audio file or as a text file) as well as the contact information about the ESC 12 may be stored in the non-volatile portion of the memory 46*. On the other hand, a paging message may be stored in the volatile portion (or temporary storage) of the memory 46 for an IP device 20 that may also function as a wireless pager.

Id. 11:7-19.

Furthermore, *the web browser module 50 may also be automatically activated once the panic button 24 is pressed by the user of the IP device 20. In that case, the web browser 50 may*

retrieve (via the PCU 52) relevant locally-stored information (e.g., the web address of the ESC 12 or the personal information about the user) from the memory unit 46 and transmit an appropriate portion of that information over the Internet 22 in response to the activation of the panic button 24. The web browser module 50 interacts with the PCU 52 to execute necessary software routines for Internet access. The software routines, upon execution, activate the modem 54 in the NIU 38 to establish an electrical connection with a wireline carrier network (e.g., via a telephone line (not shown)) to accomplish dialed Internet access. In one embodiment, the web browser module 50 (including its hardware and/or software elements) may be a part of the PCU 52 and the PCU 52 may directly perform web browsing or information delivery over the Internet 22

Id. 11:64-12:15.

229. In view of the above, a person of ordinary skill in the art would have understood *Zellner* to disclose transmitting all four items in response to the user pressing the panic button, and this disclosure of *Zellner* is consistent with how the '404 patent describes transmitting emergency information “along with” owner identification information, as described in §X.A.1.d. Thus, in my opinion, a person of ordinary skill in the art would have understood *Zellner* to disclose transmitting image, audio, and location data “along with” the personal information.

230. To the extent that Patent Owner argues or that the Board finds that *Zellner* does not disclose or suggest transmitting the image, audio, and location data “along with” personal information, then at a minimum, a person having ordinary skill in the art would have considered it obvious to modify *Zellner* to transmit the image, audio, and location data “along with” personal information.

231. In my opinion, *Zellner*, transmitting the image, audio, and location data “along with” personal information would neither be inconsistent with *Zellner*’s disclosure nor otherwise require a redesign of *Zellner*’s operating principles because *Zellner* already discloses that each of the item may be transmitted. In addition to this, there is no suggestion that the portable device can transmit only one item to the exclusion of another.

232. *Zellner* discloses a need for simple operation and efficient communication in emergency situations:

In one embodiment, the device may include a location identifier unit that supplies the current location of the device (and, hence, of the user operating the device) to the processing unit to be included as part of the help request message so that ESC personnel may efficiently locate the user who requested the emergency help. An image capture device may also be included to allow the processing unit to transmit to the ESC one or more images of the physical vicinity of the user when the user activated the panic button. ***Such a transmission may help the ESC personnel to identify potential***

cause of the emergency request from the user and also to obtain evidence that may be needed in future law enforcement efforts.

Id. 3:34-45.

The device according to the present invention *advantageously harnesses the resources of the Internet to allow users to request emergency help over the Internet by simply pushing a panic button provided on the device. Internet-based emergency message delivery may be useful in many situations, for example, when the person in need of help is speech-impaired, disabled or in a situation that prevents that person from orally requesting emergency help.*

Id. 4:38-46.

In that case, *the user of the IP device 20 may simply touch an emergency help or panic button icon* provided on the display screen 28 to activate the software panic button to transmit the emergency help request message.

Id. 7:42-45.

233. A person of ordinary skill in the art would have understood that transmitting all four items in response to pressing the panic button would have advanced *Zellner*'s objective of simply and efficiently communicating the emergency information to the ESC personnel, and that it would better facilitate the emergency response if all the available information is provided.

234. For example, *Kumar*, describes an objective similar to the '404 patent and *Zellner*. *Kumar* discloses that in including the "location of the

wireless device” and “multimedia data,” “the transmitted MMS message may be quite useful and/or efficient in notifying an emergency contact of the situation at the local vicinity of the wireless device:

It should be appreciated that by including the location of the wireless device as well as multimedia data from the local vicinity of the wireless device, *the transmitted MMS message may be quite useful and/or efficient in notifying an emergency contact of the situation at the local vicinity of the wireless device.* The location of the wireless device and the multimedia data, including the emergency profile information that may be provided in the MMS message, may combine to provide an efficient notification of the circumstances surrounding an emergency to an emergency contact. In some instances, the emergency contact may be able to respond to the emergency situation in an appropriate manner based on the breadth of information (e.g., audio, video, and image data) provided in the MMS message.

EX1013 ¶[0054].

235. *Kumar* further discloses that the multimedia message may include the “emergency profile information” which is information associated “with a user of the wireless device”:

In some embodiments herein, the emergency profile includes information that may be associated with a user of the wireless device 100, 200. For example, the emergency profile may include information associated with the user of the wireless device such as

the user's: name, home address, home telephone number, work address, work address, emergency contact, social security or other identification number/information (e.g., passport information), blood type, medical conditions, allergies, medical insurance information (e.g., insurance plan, plan number, contact(s), deductible, etc.), automobile insurance information (e.g., insurance plan, plan number, contact(s), deductible, etc.), home insurance information (e.g., insurance plan, plan number, contact(s), deductible, etc.), etc.

In some embodiments, the emergency profile information may be categorized or include information related to particular types of situations, persons, users, etc. For example, the emergency profile may include a number to contact in the instance of a medical emergency and yet another number to contact in the instance of an automobile emergency. That is, the emergency profile may be customized for a user, a type of service provided with the wireless device, etc.

Id. ¶¶[0039], [0040].

In some embodiments, the content or combination of multimedia data included in the MMS message may vary or be specified by a user, an emergency profile, the wireless device or other controlling mechanisms. For example, in some embodiments the MMS message multimedia content may be determined or specified by a user, the emergency profile, the emergency contact, a configuration of the wireless device or the mobile network providing service for the wireless device.

Id. ¶[0053].

236. A person of ordinary skill in the art would have understood that there would have been a reasonable expectation of success in making a modification to *Zellner* because a person of ordinary skill in the art would have known how to configure the device to transmit all of the image, audio, location, and personal information. By the early 1990s, it was considered “obvious,” to transmit all four items of information from the portable device to the police. For example, *Coles* discloses:

Any activation of the system will immediately cause the following to happen. *One--calculation of the exact position of the portable locatable portable electronic camera image transmission unit 1 via the position location apparatus module 4. Two--activate as necessary the electronic camera module 2 to photograph the immediate area. Three--store all this information electronically within the internal electronic memory while at the same time transmitting, via the combined electronic memory and electronic transmitter module 5, name and address of the user, date, time of day, exact location, a photograph of the immediate area plus preferably sound.*

EX1015, 2:18-29.

The proposed use of such electronics may seem of itself to be obvious, but the resulting small package creates a range of completely new products and markets. For example, a child or young girl on the way to or from school will be able to alert his or

her parents to any potential danger en route. An attractive and vulnerable young woman walking home at night can alarm the police (or indeed any convenient person) of potential as well as actual danger.

Id. 2:63-3:3.

237. Accordingly, in view of the above, *Zellner* discloses or suggests a portable device with various transmission technologies (a “transmitting unit”) which in response to the user pressing the panic button transmits images, the user’s voice and audio recordings, and location information for the purpose of seeking emergency help (“adapted to transmit as emergency information the image data, the audio data, and the location data”) in addition to personal information of the user (“along with specific information including owner identification information”).

e. 9[d] & 9[e]

(i) “a panic button...wherein the panic button is activated by a series of depressings of the panic button”

238. In my opinion, *Zellner* in combination with *Kim* discloses or suggests this feature.

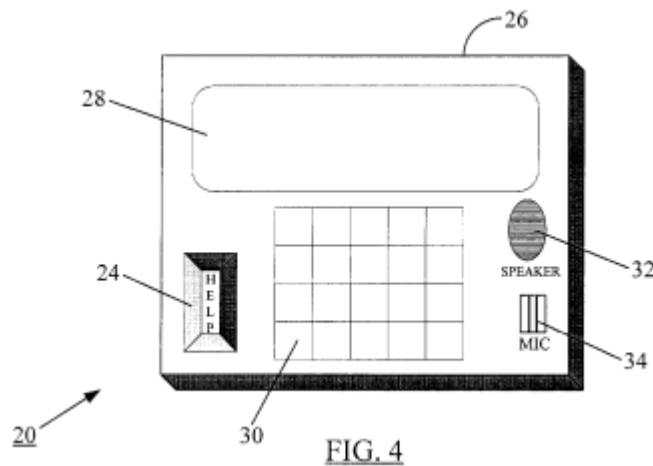
239. *Zellner* discloses that the portable device includes a “panic button”:

FIG. 4 is an illustration of an embodiment of the *IP device 20 of the present invention wherein the IP device 20 has a physically built-in panic button 24*. The IP device 20 may be a portable or wearable unit.

EX1008, 6:55-57.

The foregoing describes exemplary embodiments of an IP device having *a built-in panic button* that may be implemented in hardware or software.

Id. at 19: 27-29.



Zellner FIG. 4

240. *Zellner*'s description of the panic button is consistent with how the '404 patent describes a "panic button" as described in §X.A.1.e(i), and *Zellner* does not ascribe any non-panic-related functions to its panic button. Thus, in my opinion a person of ordinary skill in the art would have understood *Zellner*'s panic button to be a "panic button."

241. *Zellner* further discloses that the panic user may only need to push the panic button 24 once to request assistance:

The present invention contemplates a device for requesting emergency assistance, comprising a processing unit; a panic button coupled to the processing unit, ***wherein the panic button is configured to send a first indication to the processing unit when a user of the device activates the panic button;***

Id. 2:66-3:4.

The panic button may be implemented in hardware or software. In a hardware implementation, the panic button may be provided as ***a button on the face of the housing that can be pushed by the user when in need of emergency help.*** In a software implementation, a panic button icon may be displayed on a touch-sensitive display screen provided on the housing. ***The user may touch the icon to activate the panic button functionality, i.e., to transmit the help request message to the ESC.***

Id. 3:24-33.

The user of the IP device 20 may need to push the panic button 24 only once to transmit the emergency request message in the TCP/IP form.

Id. 7:28-30.

242. By 2005, a person of ordinary skill in the art would have been aware of the need to implement techniques that reduce the risk of false activation in panic button devices like *Zellner*'s. This is confirmed, for example, by prior

art disclosures that I discussed in §X.A.1.e(i) that describe reducing accidental activations. *Zellner* itself recognizes the need to avoid false activation in the context of its voice-activation embodiment:

Such an arrangement may be necessary to avoid false transmission of emergency help request messages (or “false alarms”) to the ESC 12.

EX1008, 13:40-42. But *Zellner* does not explicitly disclose a technique to minimize accidental activation when using the panic button.

243. As detailed in §X.A.1.e(i), *Kim* is a device similar to the ’404 patent and *Zellner*. *Kim* discloses an emergency mode that may be executed if the emergency key button 32 is manipulated a plurality of times, e.g., three times, within a set period of time. A person of ordinary skill in the art would have understood that pressing the panic button comprises activating the panic button, as this is consistent with how the ’404 patent describes it. *See* §X.A.1.e(i). In addition, as detailed in §X.A.1.e(i), *Kim*’s disclosure of “activating” the panic button is consistent with how the ’404 patent describes that the panic button may be activated by a “series” of depressions.

244. A person of ordinary skill in the art would have recognized the importance of implementing a technique to minimize accidental activation of a panic button in portable or wearable devices like those disclosed by *Zellner*.

That is because the risk of inadvertent presses would be expected to be higher in

a wearable form factor because such devices are more prone to being fumbled or, for example, activated by clutter in a pocket or purse.

245. *Kim* does not expressly describe that the purpose of requiring the user to manipulate or press the emergency key button a plurality of times (e.g., three times) within a time period was for the purpose of reducing accidental or false activations, but a person having ordinary skill in the art would have understood that the reason for *Kim*'s design was to reduce the risk of accidental or false activation, as explained in §X.A.1.e(i).

246. Thus, a person of ordinary skill in the art would have been motivated to combine *Zellner* and *Kim* and would have considered the combination to amount to the use of known technique (*Kim*'s technique of reducing accidental activation by requiring that the key be pressed a plurality of times (e.g., three times)) to improve similar devices (*Zellner*'s device having a panic button) in the same way (to reduce the risk of false activation).

247. In addition, a person of ordinary skill in the art also would have considered the combination to amount to applying a known technique (*Kim*'s technique of reducing accidental activation by requiring that the key be pressed a plurality of times (e.g., three times)) to a known device (*Zellner*'s device having a panic button) ready for improvement to yield predictable results (*Zellner*'s

device that requires a plurality of button presses to activate, thus reducing the chances of accidental activation).

248. In my opinion, a person of ordinary skill in the art would have had a reasonable expectation of success in modifying *Zellner*'s panic button to require three presses, with predictable results. There are several examples of prior art disclosing panic buttons similarly configured to be activated by a plurality of presses. For example, *Berger* discloses, holding or pressing the button "repeatedly":

In an emergency situation, a user would either hold the emergency button 214 or press the button repeatedly. If the person that the user is communicating with does not appear to be able to assist the user, *then the user may continue to activate the emergency button 214 in attempt to contact the emergency response center.* Thus, if the emergency button 214 is still activated at step 414, then the processor 302 terminates the existing call at step 418 and dials an emergency number associated with the emergency response center or otherwise contacts the center via the transceiver 323 at step 410. Thereafter, after the call is terminated by the mobile communication device 300 or the emergency response center at step 412, the processor returns to monitoring the emergency button or buttons 214 of the accessory 200 at step 404.

EX1019 ¶[0026].

249. Another example is *Cobb*, which discloses that the “emergency button 64 is pressed twice”:

When the emergency button 64 is pressed twice the electronic transmitter 41 sends the signal to the cellular relay station 12.

EX1017, 4:12-14.

250. *Smith* discloses pressing the “panic button 36 three times in quick succession”:

When armed by using the first button 24 as described above in relation to the first embodiment, ***a user can press the panic button 36 three times in quick succession.*** This will cause the device to automatically send a text message to a set cellphone. The device may be used by a child, for example, to send a text message to a parent's cellphone.

EX1018, 9:1-8.

251. *Wade* also discloses depressing “the pendent button 50, 3 times”:

In the case of an emergency situation the emergency caller should depress the pendent button 50, 3 times, step 226, the 3 button depressions minimize the occurrence of a false alarm or accidental emergency call being made. The first pendent push button depression activates the pendant 40 power circuit to latch on and subsequently causes the pendant transmitter 58 to send an identity code to the base 38, step 230. Subsequent pendant 40 button 50 pushes, being the second button push and higher allow the base to verify the identity code of pendent 40, step 232.

EX1016 ¶[0317].

252. Accordingly, in my opinion, the *Zellner-Kim* combination discloses or suggests a portable device with a panic button (“a panic button”) that, when pressed a plurality of times (e.g., three times), triggers the collection and transmission of emergency information (“wherein the panic button is activated by a series of depressings of the panic button”).

- (ii) **the panic button is “adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location when the panic button is activated”**

253. In my opinion, *Zellner* in combination with *Kim* discloses or suggests the panic button is “adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location when the panic button is activated.”

254. *Zellner* discloses “activat[ing]” the camera when the panic button is pressed:

The camera 36 may be activated when the panic button 24 is pressed by the user and the camera 36 may remain activated for a predetermined time thereafter (e.g., for 30-60 seconds) prior to automatically shutting itself off.

EX1008, 8:3-6.

255. *Zellner* also discloses a user location identifier that “ascertain[s] location of the user activating said panic button”:

In one embodiment, the device may include *a location identifier unit that supplies the current location of the device (and, hence, of the user operating the device) to the processing unit to be included as part of the help request message* so that ESC personnel may efficiently locate the user who requested the emergency help.

Id. 3:34-39;

3. The device of claim 1, further comprising a user location identifier coupled to the processing unit, *wherein the user location identifier is configured to ascertain a location of the user activating said panic button.*

Id. claim 3.

256. And as previously detailed in §X.A.1.d, *Zellner* discloses capturing and transmitting image, audio, and location data, along with personal information about the user in response to the user pressing the panic button.

257. The above disclosures are consistent with how the '404 patent describes “activating” the components of the device, as previously described in §X.A.1.e(ii).

258. As explained in §X.D.1.e(i), in the *Zellner-Kim* combination, *Zellner* is modified in view of *Kim* such that the same data and information is

captured and transmitted when *Zellner*'s panic button is pressed a plurality of times (e.g., three times).

259. In addition to this, *Zellner* discloses that the information is transmitted to a specific location (i.e., the ESC) as opposed to being merely broadcast. The user may program the portable IP device with information about the ESC:

The user may “program” the IP device 20 with pertinent data about the ESC 12 including, for example, the name of the ESC 12, the IP address of the ESC 12, the telephone number and name of the contact person at the ESC 12, the e-mail address of the ESC 12, etc.

Id. 10:3-8.

260. Based on my experience and background, a person of ordinary skill in the art would have understood such programming to comprise specifying the ESC to which the information is transmitted. As previously described in §X.A.1.e(ii), *Zellner*'s disclosure is consistent with how the '404 patent describes transmitting to a “specified location.” Thus, a person of ordinary skill in the art would have understood *Zellner* to disclose sending the data and information to a “specified location.”

261. Accordingly, in my opinion, the *Zellner-Kim* combination discloses or suggests a portable device with a panic button (“a panic button”) that activates

the camera, obtains the location of the user, and transmits images, the user's voice and an audio recording, location information, and user personal information to the programmed number/address for the emergency service center ("adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location") in response to pressing the panic button a plurality of times (e.g., three times) ("when the panic button is activated").

2. CLAIM 10: The mobile device as set forth in claim 9, wherein when the panic button is activated a public or private network for emergency purposes is dialed.

262. In my opinion, *Zellner* in combination with *Kim* discloses or suggests "[t]he mobile device as set forth in claim 9, wherein when the panic button is activated a public or private network for emergency purposes is dialed."

263. As previously detailed in §X.D.1.d, *Zellner* discloses that if the data is transmitted to the ESC via a wireline network, then the device communicates wirelessly with its corresponding base unit that is physically connected to the a wireline carrier network 14:

When the IP device 20 is portable, it may have an associated base unit (not shown) to transmit appropriate signals to the carrier network 14. *For example, the IP device 20 may communicate wirelessly with its corresponding base unit and the base unit may*

be physically connected to a telephone line to forward messages received from the IP unit 20 to the carrier network 14, which, here, may be the PSTN.

Id. 6:63-7:2.

264. In addition to this, *Zellner* discloses that the web browser module interacts with DTMF dialer 48 and NIU 38 to establish dial-up internet access over a telephone wireline via a base unit:

The web browser 50 may be activated using one or more keys on the keypad 30 and may be used for surfing the world wide web portion of the Internet. Furthermore, the web browser module 50 may also be automatically activated once the panic button 24 is pressed by the user of the IP device 20. In that case, the web browser 50 may retrieve (via the PCU 52) relevant locally-stored information (e.g., the web address of the ESC 12 or the personal information about the user) from the memory unit 46 and transmit an appropriate portion of that information over the Internet 22 in response to the activation of the panic button 24. The web browser module 50 interacts with the PCU 52 to execute necessary software routines for Internet access. ***The software routines, upon execution, activate the modem 54 in the NIU 38 to establish an electrical connection with a wireline carrier network (e.g., via a telephone line (not shown)) to accomplish dialed Internet access.*** In one embodiment, the web browser module 50 (including its hardware and/or software elements) may be a part of the PCU 52

and the PCU 52 may directly perform web browsing or information delivery over the Internet 22.

Id. 11:62-12:15

The IP device 20 may be connected to the carrier network 14 via a regular telephone line. In one embodiment, *a base unit (not shown) for the IP device 20 may be connected to the telephone line and the IP device 20 may be carried on the user's person. Any TCP/IP messages generated by the IP device 20 may be wirelessly transmitted first to the base unit, which, in turn, may forward them to the carrier network 14 using the telephone line.*

The TCP/IP messages may then be routed to the ESC 12 via the Internet 22. In another embodiment, the IP device 20 may utilize a wireless telephone network (e.g., the TDMA (Time Division Multiple Access) cellular network) as the carrier network 14 to initially transmit TCP/IP message packets to. Thereafter, the wireless network, in combination with the PSTN and the Internet 22, may route the TCP/IP packets to the ESC 12. In such an event, the carrier network 14 may be construed to include the PSTN and the wireless network.

Id., 5:48-64

When the IP device 20 is portable, it may have an associated base unit (not shown) to transmit appropriate signals to the carrier network 14. *For example, the IP device 20 may communicate wirelessly with its corresponding base unit and the base unit may be physically connected to a telephone line to forward messages*

received from the IP unit 20 to the carrier network 14, which, here, may be the PSTN.

Id. 6:63-7:2.

The network interface unit 38 provides an electrical interface for Signals travelling between various circuit elements inside the housing 22 and a wireline carrier network, e.g., the carrier network 14 in FIG. 3, connected to the IP device 20 either directly *or via a base unit (not shown)* associated with the IP device 20 as discussed hereinbefore.

Id. 8:53-58

In one embodiment, the DTMF (Dual Tone Multi Frequency) dialer 48 communicates with the PCU 52 and receives the telephone number sent to the PCU 52 by the web browser module 50 for dial-in Internet access. The telephone number may be for direct access to the ESC 12 or it may be for an ISP (Internet Service Provide) through which the emergency request message may be sent to the ESC 12 over the Internet 22. *The DTMF dialer 48, in turn, generates corresponding DTMF signals to be sent to the local telephone switching office in the carrier network 14 via the NIU 38. The DTMF signals may be sent over a telephone line either directly from the IP device 20 or from a corresponding base unit (not shown) for the IP device 20 as discussed hereinbefore.*

Id. 11:20-33

265. Further, *Zellner* particularly discloses that in response to the panic button being pressed a plurality of times (e.g., three times), the web browser module 50 interacts with a processing unit to “activate the modem 54 in the NIU 38 to establish an electrical connection with a wireline carrier network ... to accomplish dialed Internet access.”

266. *Zellner* also discloses that the web browser module provides a telephone number to the DTMF dialer for “dial in Internet access;” “the telephone number may be for direct access to the ESC 12 or it may be for an ISP (Internet Service Provide[r]). As *Zellner* further explains, this “DTMF dialer 48, in turn, generates corresponding DTMF signals to be sent to the local telephone switching office in the carrier network 14 via the NIU 38,” and “[t]he DTMF signals may be sent ... from a corresponding base unit ... for the IP device 20”:

In one embodiment, the DTMF (Dual Tone Multi Frequency) dialer 48 communicates with the PCU 52 and receives the telephone number sent to the PCU 52 by the web browser module 50 for dial-in Internet access. The telephone number may be for direct access to the ESC 12 or it may be for an ISP (Internet Service Provide) through which the emergency request message may be sent to the ESC 12 over the Internet 22. The DTMF dialer 48, in turn, generates corresponding DTMF signals to be sent to the local telephone switching office in the carrier network 14 via the NIU 38. The DTMF signals may be sent over a telephone line either directly from the IP device 20 or from a corresponding

base unit (not shown) for the IP device 20 as discussed hereinbefore.

Id. 11:20-33.

267. In view of the above, a person of ordinary skill in the art would have understood *Zellner* to disclose or suggest that the portable IP device may connect to the ESC or to the internet via dial-up access when the panic button is pressed. Additionally, because the ESC is an emergency services center and the purpose of the transmission is to request emergency help, a person of ordinary skill in the art would have understood it is being dialed for “emergency purposes.”

268. Accordingly, in my opinion, the *Zellner-Kim* combination discloses or suggests a portable device with a panic button that, when pressed a plurality of times (e.g., three times) (“wherein when the panic button is activated”) initiates a dial-up connection to the ESC or the Internet (“a public or private network for emergency purposes is dialed”).

3. CLAIM 11: “A mobile device as set forth in claim 9, wherein the specific information includes a pre-recorded emergency message.”

269. In my opinion, *Zellner* in view of *Kim* discloses “[a] mobile device as set forth in claim 9, wherein the specific information includes a pre-recorded emergency message.”

270. *Zellner* discloses that the user can pre-record a digital file which can include the user's personal information. *Zellner* further discloses that when the panic button is activated, the personal information is retrieved from memory 46 and may be transmitted to the web browser module 50, which in turn transmits the information to the ESC 12:

The user of the IP device 20 may speak into the microphone 34 to transmit the user's voice over the Internet 22. The audio logic unit 40 receives the electrical audio signals from the microphone 34 and sends them to the PCU 52, which, in conjunction with the browser module 50, transmits the user's voice over the Internet 22 using the NIU 38. ***In one embodiment, the user may store the user's personal identification information as a digital audio file in the memory unit 46 by speaking into the microphone 34.*** The PCU 52 may convert the audio electrical signals received from the audio logic unit 40 into the predetermined digital audio file format and store the user's personal information in the memory unit 46. The personal information may include the user's name, address, any known medical condition, contact information in case of emergency, etc. The digital audio file formats for the user's personal information may include file extensions such as, for example, ".WAV" (wave file), ".AIFF"(Audio Interchange File Format), ".AU"(audio file), etc. ***Upon activation of the panic button 24, the PCU 52 may retrieve the personal information from the memory 46 and may transmit it to the web browser module 50, which, in turn, may immediately send the***

information to the ESC 12 via TCP/IP packets sent over the Internet 22.

Id. 9:22-44.

271. *Zellner's* disclosure is consistent with how the '404 patent describes this feature:

In another embodiment the present invention allows the user to pre-record a personal warning message which is transmitted to the emergency personnel in the event of an attack during a specific time period. For example, if one is traveling to a meeting at 2 pm, she could program the device to transmit a specific warning message if the panic button is activated between the hours of 2 pm-4 pm. For example: "It is now Sunday, January 15th. I will be traveling to Sherborn, Mass. for a 2 pm meeting with Mr. John Smith who lives on Gray Road."

EX 1001 7:41-50.

272. In view of the above, a person of ordinary skill in the art would have understood that *Zellner's* disclosure of including, for example, "contact information in case of emergency" is analogous to the example provided in the '404 patent because the example also provides information about who may be contacted in an emergency (i.e., "Mr. John Smith who lives on Gray Road.").

273. Accordingly, the *Zellner-Kim* combination discloses or suggests pre-recording a digital audio file including personal information such as "the user's name, address, any known medical condition, contact information in case

of emergency, etc.” (“wherein the specific information includes a pre-recorded emergency message.”).

4. CLAIM 12: “The mobile device of claim 9, wherein a number of depressings of the panic button to activate the panic button is three.”

274. In my opinion, *Zellner* in combination with *Kim* discloses or suggests “[t]he mobile device of claim 9, wherein a number of depressings of the panic button to activate the panic button is three” for the reasons previously detailed in §X.A.1.e(i).

5. CLAIM 13

275. *Zellner* in combination with *Kim* discloses or suggests claim 13. With respect to 13[pre], 13[a], 13[b], and 13[e], see sections X.D.1.a, X.D.1.b, X.D.1.c, and X.D.1.e(i), respectively.

a. 13[c] a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location, along with specific information including owner identification information; and

276. Limitation 13[c] requires “a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location, along with specific information including owner identification information.” This is the same as 9[c] except that it further requires that the transmitting unit is adapted to transmit data and information to a “specified location.”

277. *Zellner* discloses or suggests 9[c] for the reasons previously detailed in §X.D.1.d. As previously discussed in §X.D.1.e(ii), a person of ordinary skill in the art would have understood *Zellner* to disclose transmitting the data to a programmed number/address for the emergency service center (i.e., a “specified location”). Thus, a person having ordinary skill in the art would have also understood the web browser module that interacts with a wireless data communication module and/or other transmission technologies (“transmitting unit”) transmits the data to a specified location.

278. Accordingly, in my opinion, the *Zellner-Kim* combination discloses or suggests a portable device with a web browser module that interacts with a wireless data communication module and/or other transmission technologies (“transmitting unit”) that in response to the user pressing the panic button transmits images, the user’s voice and audio recordings, and location information for the purpose of seeking emergency help to the emergency service center (“adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location”), in addition to personal information of the user (“along with specific information including owner identification information”).

b. 13[d] a panic button, which, when activated, performs the following panic button functions: (1) activating the camera unit, the location unit, and the transmitting unit to send the emergency information

***and the specific information to the specified location,
and (2) dialing a public or private network for
emergency purposes;***

279. Limitation 13[d] is the same as limitation 9[d] except that it also requires the dialing function described in claim 10. The *Zellner-Kim* combination discloses or suggests 9[d] as explained in §X.D.1.e. And the *Walker-Kim* combination discloses or suggests claim 10 as explained in §X.D.2.

280. Accordingly, in my opinion, the *Zellner-Kim* combination discloses or suggests a portable device with a panic button (“a panic button”) that activates the camera, obtains the location of the user, and transmits images, the user’s voice and an audio recording, location information, and personal information to the programmed number/address for the emergency service center (“performs the following panic button functions: (1) activating the camera unit, the location unit, and the transmitting unit to send the emergency information and the specific information to the specified location”) and initiates a dial-up connection to the emergency services center or the Internet (“and (2) dialing a public or private network for emergency purposes”).

6. CLAIM 14: “The mobile device of claim 13, wherein a number of depressings of the panic button to activate the panic button is five.”

281. In my opinion, *Zellner* in combination with *Kim* discloses or suggests “[t]he mobile device of claim 13, wherein a number of depressings of the panic button to activate the panic button is five.”

282. As previously detailed in §X.D.1.e(i), the *Zellner-Kim* combination discloses or suggests a portable device with a panic button that is activated by being pressed a plurality of times, e.g., three times. For the reasons previously described in §X.A.5, this disclosure overlaps and encompasses the 5 presses required by claim 14 and the ’404 patent does not disclose that there is something special or critical about five button presses.

283. Thus, in my opinion, the *Zellner-Kim* combination discloses or suggests that the panic button is pressed a plurality of times to activate the panic button (“wherein a number of depressings of the panic button to activate the panic button is five.”).

E. GROUND 3B: ZELLNER IN COMBINATION WITH KIM AND DIXIT RENDERS CLAIM 14 OBVIOUS

284. As previously explained in §X.D.6, the *Zellner-Kim* combination discloses or suggests claim 14.

285. To the extent that the Board disagrees, then in my opinion, claim 14 would have been obvious in view of *Zellner*, *Kim*, and *Dixit*. Particularly, for the

same reasons detailed in §X.B addressing Ground 1B, a person having ordinary skill in the art would have considered it obvious to modify the *Zellner-Kim* combination to implement *Dixit*'s technique of five button presses.

**F. GROUND 4A: MARTIN IN COMBINATION WITH KIM
RENDERS OBVIOUS CLAIMS 9, 10, 12-14**

1. CLAIM 9

a. 9[pre] A mobile device, comprising

286. In my opinion, to the extent the preamble is limiting, *Martin* discloses or suggests “[a] mobile device.”

287. *Martin* discloses a “wireless device” implemented as a “wireless telephone,” “handheld computer,” or “personal digital assistant”:

The wireless device may be any apparatus with telecommunication capabilities. For example, the wireless device may be a *wireless telephone, an interactive pager, a handheld computer, or a personal digital assistant*.

EX1009, 2:1-4

288. Accordingly, in my opinion, a person having ordinary skill in the art would have understood *Martin* discloses or suggests a wireless device implemented as a handheld computer or a personal digital assistant (“mobile device”).

b. 9[a] a camera unit, adapted to obtain at least one of image data and audio data;

289. In my opinion, *Martin* discloses or suggests “a camera unit, adapted to obtain at least one of image data and audio data.”

290. *Martin* discloses that the wireless device includes a “sensing device” implemented as “one or more of a microphone [and] a camera” that “can capture content” including “sound, still or moving images”:

Sensing device 160 may be, for example, one or more of a microphone, a camera, a thermometer, and a barometer. Sensing device 160 can capture content. The content can include one or more of sound, still or moving images, temperature, and pressure, depending on the type of sensing device used.

EX1009, 3:36-42

Sensing device 160 may be one of several instruments. *For example, a microphone may be used as sensing device 160 to capture sound as the content. Similarly, if the content comprises images, the appropriate sensing device would be a camera.* A thermometer and a barometer are appropriate sensing devices for temperature and pressure, respectively. The content can be transmitted to called party 200 in step 322.

Id., 5:39-47

291. *Martin* describes a method of using the mobile device that begins with pressing a “keystroke sequence” and results in capturing video and sound with the integrated camera:

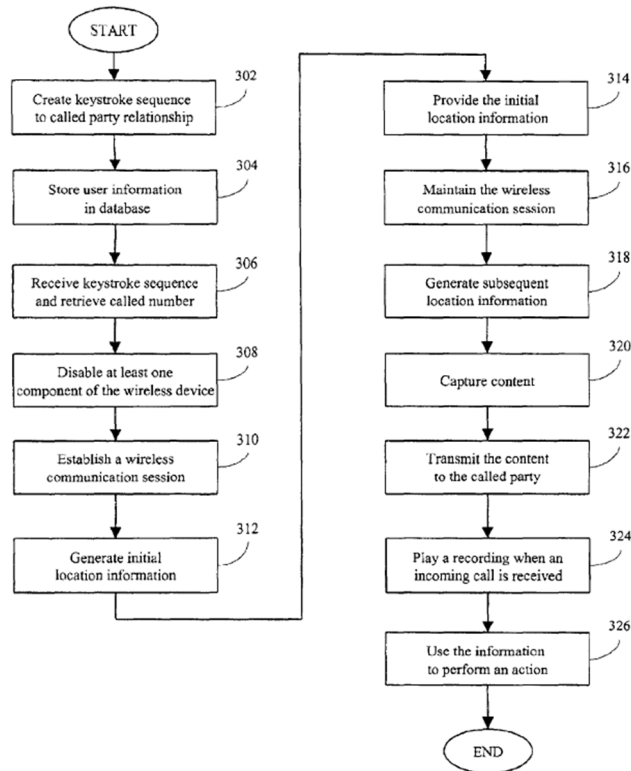


Figure 3

Id., Fig. 3

In step 310, microprocessor 110 can use the called number to establish a wireless communication session with called party 200.

Id., 4:64-66

In step 320, content surrounding wireless device 100 can be captured by sensing device 160.

Id., 5:38-39.

292. This is consistent with how the '404 patent describes this feature, as described in §X.A.1.b. In my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood that

still or moving images comprise “image data,” and “sound” comprises “audio data.”

293. Accordingly, in my opinion, a person having ordinary skill in the art would have understood that *Martin* discloses or suggests a wireless device with a sensing device implemented as a camera and microphone (“camera unit”) that captures sound and still or moving images (“adapted to obtain at least one of image data and audio data”).

c. 9[b] a location unit, adapted to obtain location data

294. In my opinion, *Martin* discloses or suggests “a location unit, adapted to obtain location data.”

295. *Martin* discloses that the wireless device includes location system 180, implemented as a “Global Positioning System (GPS) receiver” that generates “location information” such as “position coordinates of wireless device 100”:

For example, *location system 180 may be a Global Positioning System (GPS) receiver that is in communication with a constellation of GPS satellites, which produces position coordinates of wireless device 100.*

EX1009, 3:59-62

In step 312, initial *location information can be generated by at least one location system*, which may be one or more of location systems 180, 280, and 380. The initial location

information can pinpoint the location of wireless device 100 at the time the initial location information is generated. ***The initial location information may be generated using any of the known methods discussed above.*** In step 314, the initial location information can be provided to called party 200 during the wireless communication session. The initial location information is preferably provided to called party 200 as soon as it is generated.

Id., 5:4-14.

296. This is consistent with how the '404 patent describes this feature, as described in §X.A.1.c. In my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood the “location information” such as “position coordinates” to comprise “location data.”

297. Accordingly, in my opinion, a person having ordinary skill in the art would have understood that *Martin* discloses or suggests a wireless device with a GPS location system (“location unit”) that generates location information (for example, position coordinates) of a wireless device to pinpoint its location (“adapted to obtain location data”).

- d. 9[c] a transmitting unit, adapted to transmit as emergency information the image data, the audio data, and the location data along with specific information including owner identification information; and***

298. In my opinion, *Martin* discloses or suggests “a transmitting unit, adapted to transmit as emergency information the image data, the audio data, and the location data along with specific information including owner identification information.”

299. *Martin* discloses establishing a wireless communication session with a called party and that the “wireless communication session can be established using a number of components of wireless device 100, including [digital signal processor] 140 and antenna 150”:

The wireless communication session can be established using a number of components of wireless device 100, including DSP 140 and antenna 150.

EX1009, 5:1-3

Wireless device 100 can ***establish a wireless communication session with called party 200 through wireless network 300***. The present invention can further comprise one or more of location system 180, location system 280, and location system 380, which are associated with wireless device 100, called party 200, and wireless network 300, respectively.

Id., 3:48-54

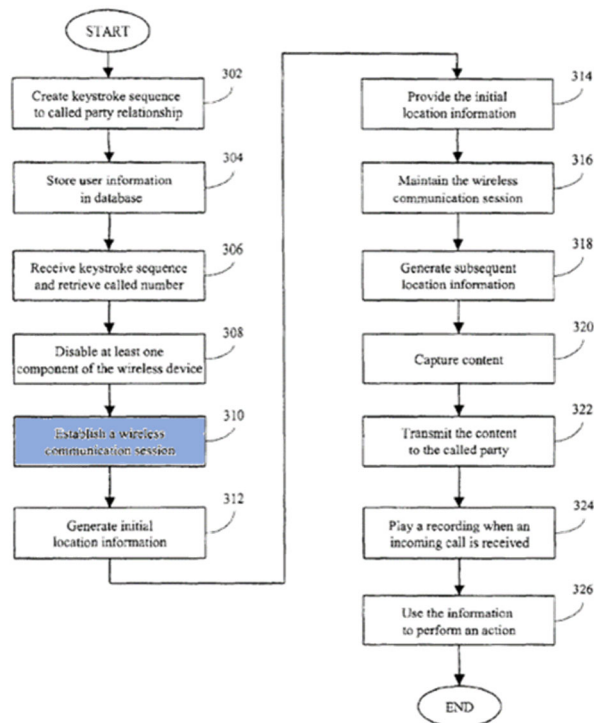


Figure 3

EX1009, Fig. 3 (annotated)

In step 310, microprocessor 110 can use the called number to establish a wireless communication session with called party 200.

In the first specific example, the microprocessor can use "911" as the called number to call a PSAP as called party 200.

Id., 4:64-5:1

300. This is consistent with how the '404 patent describes a "transmitting unit," as described in §X.A.1.d. Thus, in my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood that *Martin* discloses or suggests a "transmitting unit."

301. *Martin* also discloses capturing content (such as sound and images) and transmitting it and location information during a communication session.

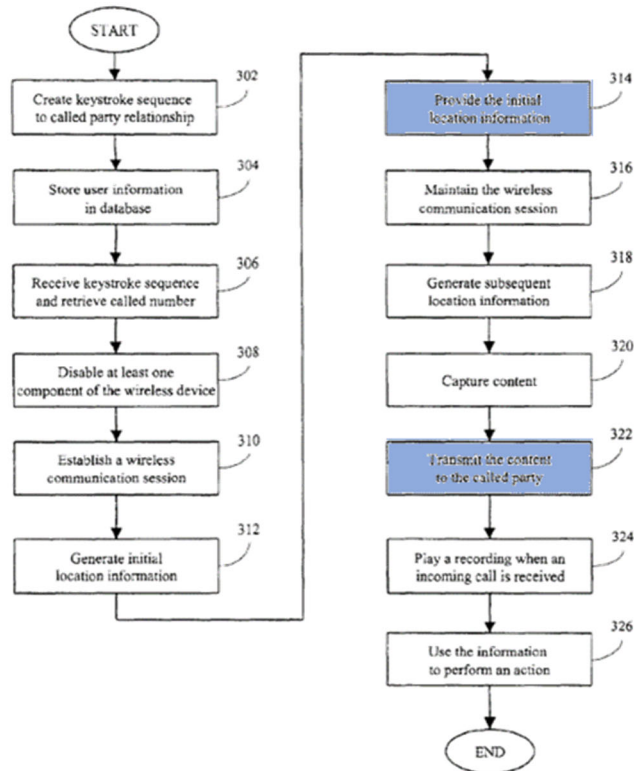


Figure 3

EX1009 at Fig. 3 (annotated)

The content can include one or more of sound, still or moving images, temperature, and pressure, depending on the type of sensing device used.

Id., 3:39-42

In step 314, the initial location information can provided to called party 200 during the wireless communication session. The initial location information is preferably provided to called party 200 as soon as it is generated.

Id., 5:10-14

The content can be transmitted to called party 200 in step 322.

Id., 5:46-47

302. In my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood images, sound, and location information to comprise image data, audio data, and location data, respectively. *See* X.F.1.b, X.F.1.c.

303. *Martin* discloses that the captured content (such as images and sound), and location information relates to an “emergency situation” and may be used by the called party for “dispatching an emergency response team to the location”:

The present invention is a ***system and method for reporting an emergency situation*** to a called party a using a wireless device.

EX1009 at Abstract

In step 326, called party can use one or more of the user information, the location information, and the content to perform an action. ***The action may comprise, for example, dispatching an emergency response team to the location***, and/or using the content as evidence in a litigation.

EX1009, 5:58-62

304. *Martin*’s disclosure is consistent with the ’404 patent’s description of “emergency information,” as described in §X.A.1.d. In my opinion, and based on my experience and background, a person having ordinary skill in the art

would have understood that *Martin* discloses or suggests transmitting the image, sound, and location information as “emergency information.”

305. *Martin* also discloses a “user profile” which includes “the name of the user of wireless device 100” and that it is sent “to establish the wireless communication session” or during the communication session”:

The user profile may comprises [sic], for example, the name of the user of wireless device 100, the medical record of the user, the type of vehicle owned by the user, and/or the vehicle's license plate number. The information can be provided to called party 200 when the keystroke sequence is used to establish the wireless communication session.

EX1009, 4:36-42

43. The method of claim 42, ***further comprising the step of transmitting the user profile to the called party during the wireless communication session.***

Id., claim 43

306. As also explained in §X.D.1.d, in my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood that the user of the device is, at least sometimes (if not most times), the owner of the device.

307. *Martin*’s disclosure of transmitting the image, audio, location data, and the user profile in connection with or during the communication session is

consistent with how the '404 patent describes transmitting emergency information “along with” owner identification information, as described in X.A.1.d. In my opinion, and based on my experience and background, a person having ordinary skill in the art would have understood that *Martin* discloses or suggests transmitting the images, sound, and location data “along with” the user profile.

308. Accordingly, in my opinion, a person having ordinary skill in the art would have understood that *Martin* discloses or suggests a wireless device with a DSP, antenna, and wireless network telecommunications (“a transmitting unit”) to transmit captured content (such as images and sound) and location information relating to an emergency situation (“adapted to transmit as emergency information the image data, the audio data, and the location data”) and a user profile including the user’s name, all during a communication session (“along with specific information including owner identification information”).

e. 9[d] & 9[e]

(i) “a panic button ... wherein the panic button is activated by a series of depressings of the panic button”

309. In my opinion, *Martin* in combination with *Kim* discloses or suggests “a panic button ... wherein the panic button is activated by a series of depressings of the panic button.”

310. *Martin* discloses that the wireless device includes a “keyboard,” and that when a “keystroke sequence” is entered using the keyboard, the wireless device establishes a communication session, and then captures and transmits various information:

The wireless device comprises *a keyboard* and a microprocessor. In one embodiment, *when a specific keystroke sequence is entered using the keyboard, the wireless device performs the following tasks:* (1) disabling one or more components of the wireless device; (2) *establishing a wireless communication session with the called party*; (3) communicating with a location system to generate location information pinpointing the location of the wireless device; and (5) providing the location information to the called party. In other embodiments, the wire device performs additional tasks, including: (6) *capturing content during the wireless communication*; (7) communicating with the location system to generate subsequent location information; and (8) *providing one or more of the subsequent location information and the content to the called party.*

EX1009, Abstract

FIG. 2 is a schematic diagram showing the system architecture of an embodiment of the present invention. The system of the present invention comprises microprocessor 110, *keyboard 120*, and display130, each of which is a component of wireless device 100. Microprocessor 110 is preferably a RISC (reduced instruction set

computer) microprocessor. *Keyboard 120 is an example of an input device.* Display 130 is an example of an output device.

Id. 3:17-24

311. *Martin* discloses various examples of such a “keystroke sequence.”

In one example, *Martin* discloses pressing “one special key”:

The specific keystroke sequence may comprise, for example, pressing *one special key on keyboard 120.*

Id., 7:18-20

312. In another example, *Martin* discloses including pressing any key, such as the “power-off” key, on the keyboard a number of times:

A second specific example of the keystroke sequence may comprise *pressing the “power-off”* key a number of times.

Id., 4:28-31

For example, when the owner is being forced by a carjacker to turn off wireless device 100, she can hold the "*" key down while *pressing the “power off” key on keyboard 120* of wireless device 100 to enter the specific keystroke sequence defined in step 502.

Id., 6:30-34

6. The wireless device of claim 1, *wherein the keystroke sequence comprises one of pressing a plurality of keys in seriatim, pressing one key one or more times*, and pressing a first key while holding down a second key.

Id., claim 6

41. The method of claim 35, *wherein the keystroke sequence comprises one of pressing a plurality of keys in seriatim, pressing one key one or more times*, and pressing a first key while holding down a second key.

Id., claim 41

313. *Martin*'s description of the "one special key" is consistent with how the '404 patent describes the "panic button" as a button with a dedicated panic function, as I described in §X.A.1.e(i). That *Martin* describes it as "one special key" and does not ascribe any other functions to it would have informed a person of ordinary skill that it was a dedicated key. *Martin* does not expressly describe a technique for reducing accidental or false activations of the "special key."

314. But, as explained in §X.D.1.e(i), by 2005, a person having ordinary skill in the art would have been aware of the need to reduce the risk of false activations of panic buttons like *Martin*'s special key, and would have been aware of various techniques for doing so. For example, *Kim* is similar to the '404 patent and *Martin*, and as detailed in X.A.1.e(i), *Kim* discloses a mobile phone with a dedicated emergency key button 32 and that an emergency mode may be executed if the "emergency key button 32 is manipulated a plurality of times (e.g., three times) within a set period of time":

At this time, although the controller 60 is allowed to execute the emergency mode according to the manipulation of the emergency key button 32 for a few seconds continuously, e.g., three seconds, it should be apparent that the *emergency mode may be allowed to be executed if the related emergency key button 32 is manipulated a plurality of times, e.g., three times, within a set period of time.*

Id., 13:1-6.

315. As explained in X.A.1.e(i), a person having ordinary skill in the art would have understood that *Kim*'s technique of requiring a plurality of presses served the purpose of reducing false activations of the emergency key.

316. And as I also explained above in §X.A.1.e(i), *Kim*'s disclosure related to emergency key button 32 is consistent with how the '404 patent describes a panic button that is activated by a series of presses.

317. A person having ordinary skill in the art would have been motivated to combine *Martin* and *Kim* and would have considered the combination to amount to the use of known technique (*Kim*'s technique of reducing accidental activation by requiring that the key be pressed a plurality of times (e.g., three times)) to improve similar devices (*Martin*'s device having a special key) in the same way (to reduce the risk of false activation).

318. A person having ordinary skill in the art also would have considered the combination to amount to applying a known technique (*Kim*'s

technique of reducing accidental activation by requiring that the key be pressed a plurality of times (e.g., three times)) to a known device (*Martin*'s device having a special key) ready for improvement to yield predictable results (*Martin*'s device that requires a plurality of "special key" presses (e.g., three presses) to activate, thus reducing the chances of accidental activation).

319. For the same reasons a person having ordinary skill in the art would have had a reasonable expectation of success in modifying *Zellner* discussed in §X.D.1.e(i), a person having ordinary skill in the art would have had a reasonable expectation of success in modifying *Martin*'s special key to require three presses, and the result would have been predictable. Moreover, as noted above in ¶312, *Martin* already discloses that its device is capable of initiating the communication session and transmitting data in response to a key being pressed one or more times.

320. To note, even though *Martin* discloses that the keystroke sequence may be any key pressed one or more times (e.g., the power-off key), a person having ordinary skill in the art would have understood that using a dedicated button like *Martin*'s special key that required being pressed a plurality of times was advantageous over using any key for the same reasons discussed above in §X.A.1.e(i).

321. Accordingly, in my opinion, the *Martin-Kim* combination discloses or suggests a wireless device with a special key (“panic button”) that, when pressed a plurality of times (e.g., three times) activates the special key to trigger establishing a wireless communication session, and capturing, generating, and transmitting data (“wherein the panic button is activated by a series of depressings of the panic button”).

- (ii) **the panic button is “adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location when the panic button is activated”**

322. In my opinion, *Martin* in combination with *Kim* discloses or suggests the panic button is “adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location when the panic button is activated.”

323. *Martin* discloses that entering the keystroke sequence with a keyboard key triggers the device to perform several operations.

324. With reference to the exemplary method in Figure 3, *Martin* discloses:

- Entering a keystroke sequence at the wireless device to establish a wireless communication session with the called party:

In step 306, when a user of wireless device 100 *inputs the keystroke sequence on keyboard 120, microprocessor 110 can retrieve the called number from memory 112*. In a specific example, if the user presses the "power-off" key while holding down the "*" key, microprocessor 110 knows that 911 is to be used as the called number. Other keystroke sequences can associate other telephone numbers with other called parties.

EX1009, 4:46-53

In step 310, *microprocessor 110 can use the called number to establish a wireless communication session with called party 200*. In the first specific example, the microprocessor can use "911" as the called number to call a PSAP as called party 200. The wireless communication session can be established using a number of components of wireless device 100, including DSP 140 and antenna 150.

Id., 4:64-5:3

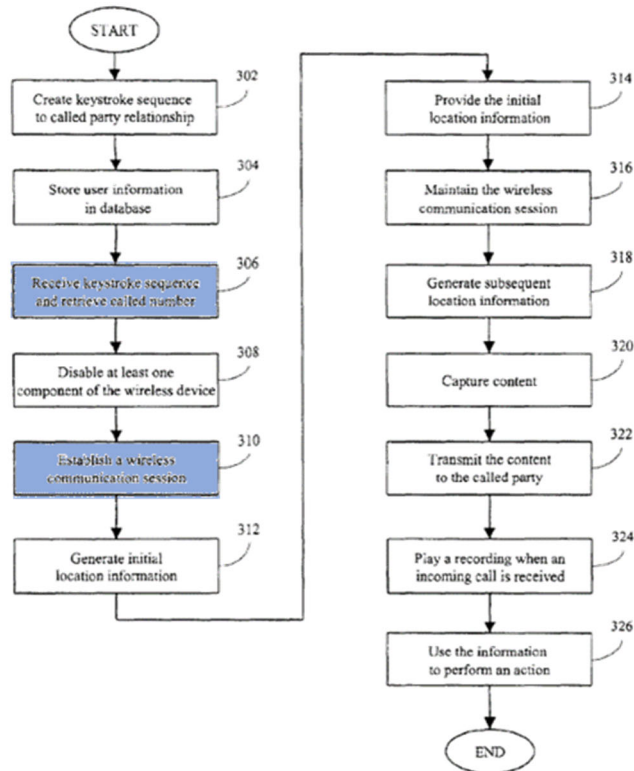


Figure 3

EX1009 at Fig. 3 (annotated)

- Generating and providing location information of the wireless device to the called party:

In step 312, initial location information can be generated by at least one location system, which may be one or more of location systems 180, 280, and 380. The initial location information can pinpoint the location of wireless device 100 at the time the initial location information is generated. The initial location information may be generated using any of the known methods discussed above. In step 314, the initial location information can be provided to the called party 200 during the wireless communication session. The

initial location information is preferably provided to called party 200 as soon as it is generated.

Id., 5:4-14

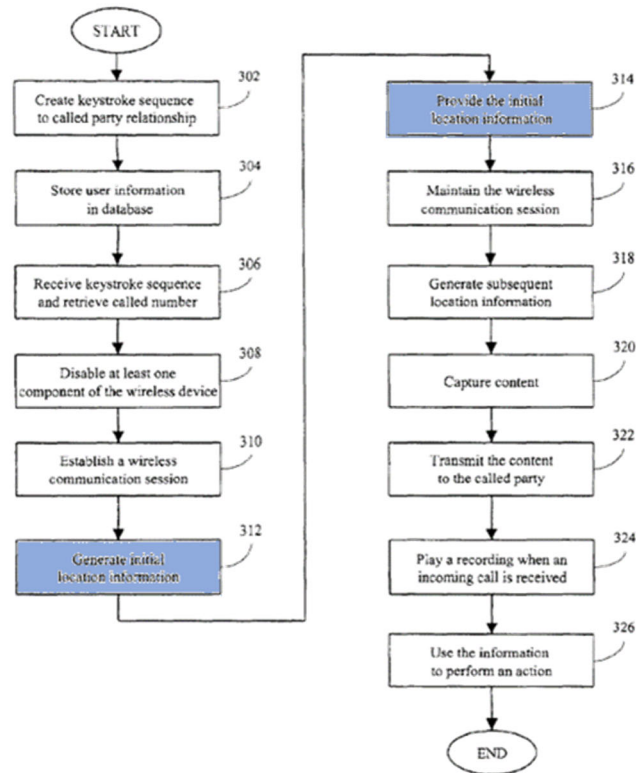


Figure 3

EX1009 at Fig. 3 (annotated)

- Capturing content (such as images and sound) and transmitting that content to the called party:

In step 320, content surrounding wireless device 100 can be captured by sensing device 160. Sensing device 160 may be one of several instruments. For example, a microphone may be used as sensing device 160 to capture sound as the content. Similarly, if the content comprises images, the appropriate sensing device would be a camera. A thermometer and a barometer are

appropriate sensing devices for temperature and pressure, respectively. The content can be transmitted to called party 200 in step 322.

Id., 5:39-47

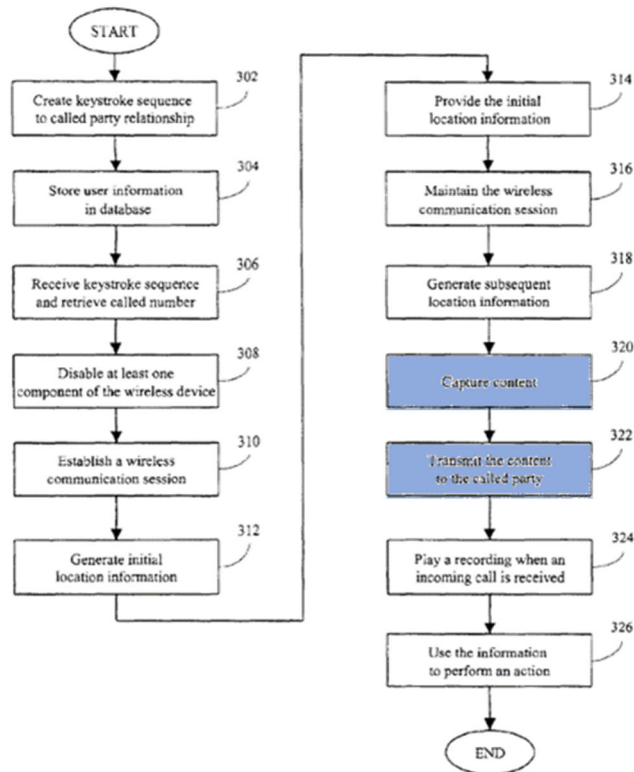


Figure 3

EX1009 at Fig. 3 (annotated)

325. This is consistent with how the '404 patent describes this feature, as described in §X.A.1.e(ii).

326. As I discussed above in §X.F.1.e(i), in the *Martin-Kim* combination, *Martin*'s special key is pressed a plurality of times (e.g., three times) to initiate the same operations when the special key is pressed once.

327. *Martin* further discloses that data from the mobile device is transmitted to a specified location as opposed to merely broadcast. *Martin* discloses defining or creating a relationship between keystroke sequence and a called party (i.e., the called number), for example, “911”:

A preferred method for using the present invention comprises the following steps. *First, a relationship between a telephone number that is associated with the called party (the called number) and a sequence of keystrokes is created, and the relationship is programmed into the wireless device.*

EX1009, 2:23-27

In step 302, at least one *relationship between a keystroke sequence and a telephone number associated with called party 200 (the called number) can be defined or created.* The relationship may be stored in memory 112 shown in FIG. 2.

Id., 4:22-25

In step 306, when a user of wireless device 100 inputs the keystroke sequence on keyboard 120, microprocessor 110 can retrieve the called number from memory 112. *In a specific example, if the user presses the “power-off key while holding down the “*” key, microprocessor 110 knows that 911 is to be used as the called number.*

Id., 4:45-50

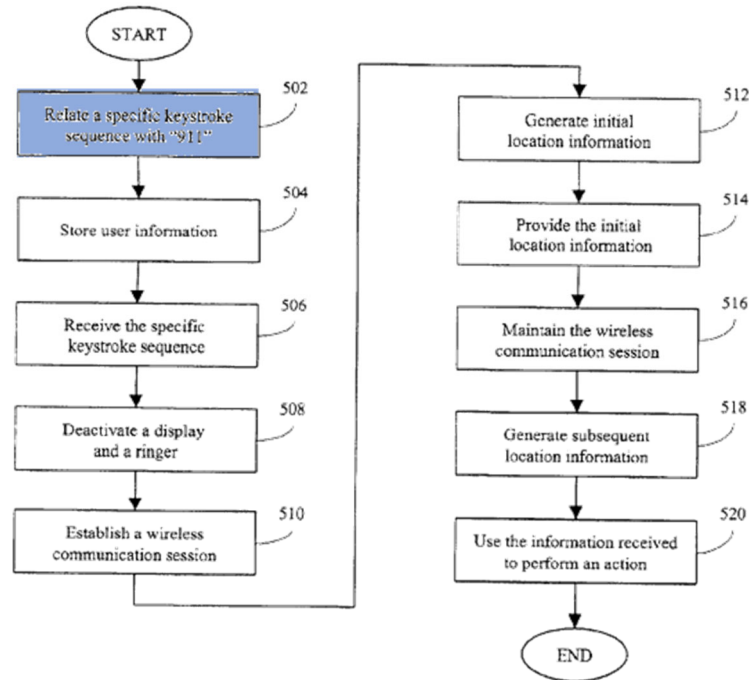


Figure 5

EX1009 at Fig. 5 (annotated)

328. The called party may be a public safety answering point (PSAP), an undercover law enforcement operation center, and/or other parties.

In step 506, the specific keystroke sequence is received by wireless device 100. *For example, when the owner is being forced by a carjacker to turn off wireless device 100, she can hold the “*” key down while pressing the “power off” key on keyboard 120 of wireless device 100 to enter the specific keystroke sequence defined in step 502.*

Id., 6:29-34

The wireless communication session *can be initiated by microprocessor 110 that dials 911 because it had recognized the specific keystroke sequence to be related to 911.*

Id., 6:43-46

The specific keystroke sequence may comprise, for example, pressing one special key on keyboard 120. In step 704, the keystroke sequence and the telephone number of operation center 600 can be stored in memory 112. ***In step 706, when the undercover officer presses the special key on keyboard 120, the keystroke sequence is received by microprocessor 110.***

Id., 7:18-25

329. More particularly, *Martin* discloses that to establish the communication session, the microprocessor, for example, “dials 911” when the keystroke sequence is entered:

The wireless communication session ***can be initiated by microprocessor 110 that dials 911 because it had recognized the specific keystroke sequence to be related to 911.***

Id., 6:43-46

330. A person having ordinary skill in the art would have understood that the step of defining or creating the relationship between the keystroke sequence and the called number to comprise the user or system designer specifying the location to which the various data would be transmitted.

331. Accordingly, in my opinion, the *Martin-Kim* combination discloses or suggests a mobile device with a special key (“a panic button”) that triggers various operations, including capturing images and sound, generating location information, and establishing a communication session and transmitting the data

and a user profile to a specified number (“adapted to activate the camera unit, the location unit, and the transmitting unit, and send the emergency information and the specific information to a specified location”) when the special key is pressed a plurality of times (e.g., three times) (“when the panic button is activated.”)

2. CLAIM 10: The mobile device as set forth in claim 9, wherein when the panic button is activated a public or private network for emergency purposes is dialed.

332. In my opinion, *Martin* in combination with *Kim* discloses or suggests “[t]he mobile device as set forth in claim 9, wherein when the panic button is activated a public or private network for emergency purposes is dialed.”

333. As I discussed above in X.F.1.e(ii), a person having ordinary skill in the art would have understood the *Martin-Kim* combination to disclose or suggest that pressing the special key a plurality of times (e.g., three times) causes the device to establish a communication session. More particularly, *Martin* discloses that to establish the communication session, the microprocessor “dials 911” when the keystroke sequence is entered:

The wireless communication session can be initiated by microprocessor 110 that dials 911 because it had recognized the specific keystroke sequence to be related to 911.

EX1009, 6:43-46

334. *Martin* further discloses that party may be a PSAP, 911, an undercover law enforcement operation center, and/or other parties:

In step 506, the specific keystroke sequence is received by wireless device 100. *For example, when the owner is being forced by a carjacker to turn off wireless device 100, she can hold the “*” key down while pressing the “power off” key on keyboard 120 of wireless device 100 to enter the specific keystroke sequence defined in step 502.*

Id., 6:29-34

The wireless communication session *can be initiated by microprocessor 110 that dials 911 because it had recognized the specific keystroke sequence to be related to 911.*

Id., 6:43-46

The specific keystroke sequence may comprise, for example, pressing one special key on keyboard 120. In step 704, the 20 keystroke sequence and the telephone number of operation center 600 can be stored in memory 112. *In step 706, when the undercover officer presses the special key on keyboard 120, the keystroke sequence is received by microprocessor 110.*

Id., 7:18-25

335. A person having ordinary skill in the art would have recognized these as public network emergency services entities because *Martin* discloses that a PSAP is a “Public Safety Answering Point” and calls routed to it are

governed by federal government Federal Communications Commission (“FCC”) telecommunications policies:

The widespread use of the wireless telephones in the United States has prompted the Federal Communications Commission (FCC) to promulgate new rules related to emergency call processing. The FCC's wireless Enhanced 911 (E911) rules require certain Commercial Mobile Radio Services (CMRS) carriers to begin transmission of enhanced location and identity information in two phases. The first phase, started on Apr. 1, 1998, required wireless service providers to transmit a 911 caller's number and section of the cell site from which the call is originated to a Public Safety Answering Point (PSAP). The second phase, starting on Oct. 31, 2001, requires all wireless service providers to locate two-thirds of all 911 callers within 125 meters of their physical locations. In other words, for all 911 calls received, a PSAP must be able to pinpoint 67% of the callers within 125 meters.

Under the FCC rules, wireless communication networks and wireless telephones (or any wireless devices that can be used to call 911), must provide both the identity and location of the caller to a 911 dispatcher.

Id., 1:23-42

336. This is consistent with how the '404 patent describes this feature, as described in §X.A.2 above.

337. Accordingly, in my opinion, the *Martin-Kim* combination discloses or suggests that when the special key is pressed a plurality of times (e.g., three times) (“wherein when the panic button is activated”), the microprocessor dials a called party, e.g., 911, a PSAP, or an undercover law enforcement center (“a public or private network for emergency purposes is dialed”).

3. CLAIM 12: The mobile device of claim 9, wherein a number of depressings of the panic button to activate the panic button is three.

338. In my opinion, *Martin* in combination with *Kim* discloses or suggests this feature for the reasons discussed in §X.F.1.e(i).

4. CLAIM 13

a. 13[pre], 13[a], 13[b], 13[e]

339. In my opinion, *Martin* in combination with *Kim* discloses or suggests claim 13. With respect to 13[pre], 13[a], 13[b], and 13[e], see sections X.D.1.a, X.D.1.b, X.D.1.c, and X.F.1.e(i), respectively.

b. 13[c]: a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location, along with specific information including owner identification information; and

340. Limitation 13[c] requires “a transmitting unit, adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location, along with specific information including owner identification information.” This is the same as 9[c] except that it further

requires that the transmitting unit is adapted to transmit data and information to a “specified location.”

341. *Martin* discloses or suggests 9[c] for the reasons explained in §X.F.1.d. As explained in §X.F.1.e(ii), a person having ordinary skill in the art would have understood *Martin* to disclose or suggest defining or creating the relationship between the keystroke sequence and the called number to comprise the user or system designer specifying the location to which the various data would be transmitted. Thus, a person having ordinary skill in the art would have also understood that *Martin*’s DSP and antenna (“transmitting unit”) transmit the data to a specified location.

342. Accordingly, in my opinion, the *Martin-Kim* combination discloses or suggests a wireless device using a DSP, antenna, and wireless network telecommunications (“a transmitting unit”) to transmit various data relating to an emergency situation including image, sound, and location information to a called party (“adapted to transmit the image data, the audio data, and the location data as emergency information to a specified location”) in addition to a user profile (“along with specific information including owner identification information”).

- c. **13[d]: a panic button, which, when activated, performs the following panic button functions: (1) activating the camera unit, the location unit, and the transmitting unit to send the emergency information and the specific information to the specified location, and (2) dialing a public or private network for emergency purposes,**

343. Limitation 13[d] is the same as limitation 9[d] except that it also requires the dialing function described in claim 10. The *Martin-Kim* combination discloses or suggests 9[d] as explained in §X.D.1.e(ii). The *Martin-Kim* combination discloses or suggests claim 10 as explained in §X.F.2.

344. Accordingly, in my opinion, the *Martin-Kim* combination discloses or suggests that when the special key is pressed a plurality of times (e.g., three times) (“when the panic button is activated”) it triggers various operations, including capturing images and sound, generating location information, and establishing a communication session and transmitting the data and a user profile to a specified number (“performs the following panic button functions: (1) activating the camera unit, the location unit, and the transmitting unit to send the emergency information and the specific information to the specified location”); and to cause the microprocessor to dial a called party, e.g., 911, a PSAP, or an undercover law enforcement center (“and (2) dialing a public or private network for emergency purposes”).

5. CLAIM 14: The mobile device of claim 13, wherein a number of depressings of the panic button to activate the panic button is five.

345. In my opinion, *Martin* in combination with *Kim* discloses or suggests “[t]he mobile device of claim 13, wherein a number of depressings of the panic button to activate the panic button is five.”

346. As discussed above in §X.F.1.e(i), the *Martin-Kim* combination discloses or suggests a mobile device with a special key (“panic button”) that, when pressed a plurality of times (e.g., three times), triggers the collection and transmission of emergency information (“wherein the panic button is activated by a series of depressings of the panic button”).

347. For the reasons previously described in §X.A.5, this disclosure overlaps and encompasses the 5 presses required by claim 14 and the ’404 patent does not disclose that there is something special or critical about five button presses.

348. Accordingly, in my opinion, the *Martin-Kim* combination discloses or suggests that the special key is pressed a plurality of times to activate the special key (“wherein a number of depressings of the panic button to activate the panic button is five.”).

G. Grounds 4B: *Martin* in view of *Kim* and *Dixit* renders claim 14 obvious

349. As I explained in §X.F.5, the *Martin-Kim* combination discloses or suggests claim 14.

350. To the extent the Board disagrees, then claim 14 would have been obvious in view of *Martin*, *Kim*, and *Dixit*. In particular, for the same reasons discussed above in §X.B with respect to Ground 1B, it would have been obvious to modify the *Martin-Kim* combination to implement *Dixit*'s technique of five button presses.

XI. CONCLUSION

351. The findings and opinions set forth in this declaration are based on my work and examinations to date.

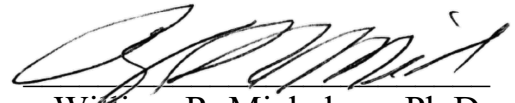
352. I may continue my examinations. I may also receive additional documentation and other factual evidence over the course of this IPR that will allow me to supplement and/or refine my opinions. I reserve the right to add to, alter, or delete my opinions and my declaration upon discovery of any additional information. I reserve the right to make such changes as may be deemed necessary.

353. In signing this declaration, I recognize that the declaration will be filed as evidence in an IPR before the PTAB. I also recognize that I may be subject to cross-examination in the 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.

354. I hereby 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 are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: 1 November 2023



William R. Michalson, Ph.D.