(12) UK Patent Application (19) GB (11) 2 401 752 (13) A

(43) Date of A Publication 17.11.2004

(21) Application No: 0312170.4

(22) Date of Filing: 28.05.2003

(30) Priority Data:
(31) 0310885 (32) 13.05.2003 (33) GB

(71) Applicant(s):
Guy Frank Howard Walker
Flat 1, 88 Fitzjohns Avenue, Hampstead,
LONDON, NW3 6NP, United Kingdom

(72) Inventor(s):
Guy Frank Howard Walker

(74) Agent and/or Address for Service:
Guy Frank Howard Walker
Flat 1, 88 Fitzjohns Avenue, Hampstead,
LONDON, NW3 6NP, United Kingdom

(51) INT CL[7]:
H04M 11/04

(52) UK CL (Edition W):
H4L LEAA L201 L209 L213 L215

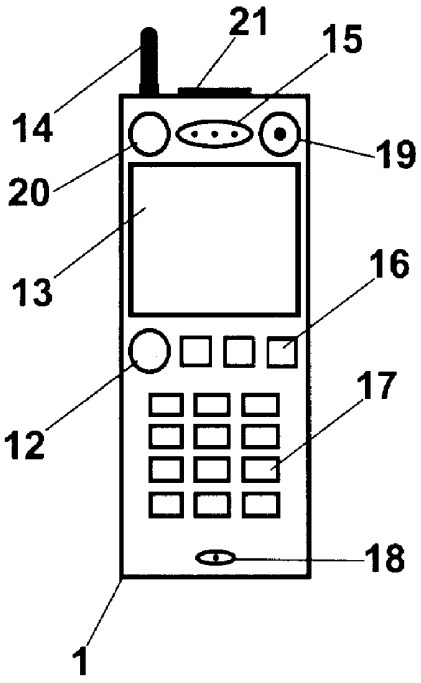
(56) Documents Cited:
WO 2003/040995 A2
BE 001013205 A6
DE 010128728 A1
DE 010061593 A1
JP 2003134258 A
US 6278884 B1

(58) Field of Search:
UK CL (Edition V) H4L
INT CL[7] H04M
Other: ONLINE: WPI, EPODOC, JAPIO, INSPEC

(54) Abstract Title: **Mobile personal security eyewitness device**

(57) A cellular handheld 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.

Fig 2



GB 2 401 752

Original

Samsung v. Fendgo
IPR2024-00113
Exhibit 1007

EXHIBIT 1007
Page 1 of 56

Fig 1

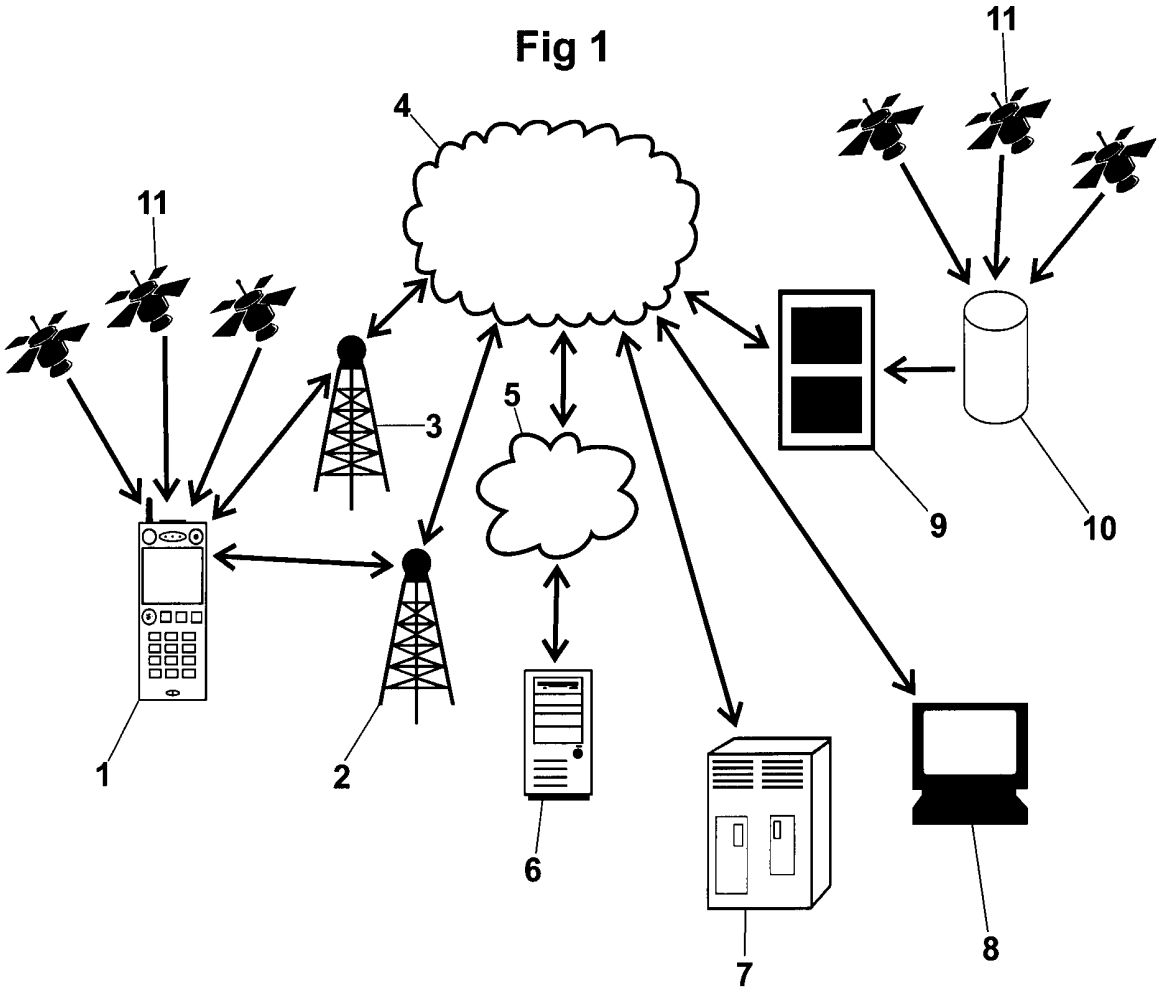


Fig 2

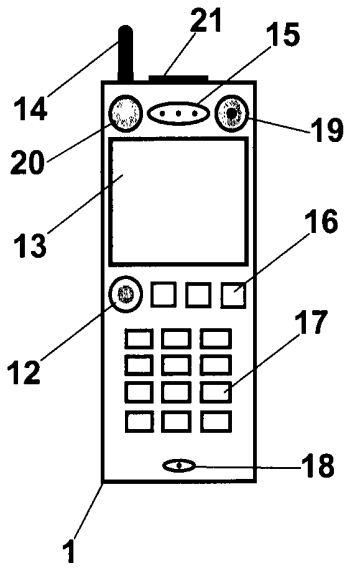
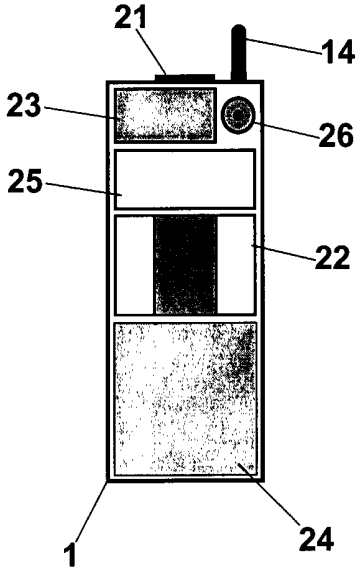


Fig 3



2401752

3G CELLULAR MOBILE COMMUNICATIONS PERSONAL SECURITY EYEWITNESS DEVICE AND REMOTE DATA STORAGE CRIME PREVENTION SYSTEM

BACKGROUND

[0001] 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.

[0002] 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, 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.

PRIOR ART

[0003] Prior art exists, relating to the various technologies combined and incorporated into this invention, including:

[0004] GB2364481 Communication device with provision for remote data storage (Applicant: ERICSSON TELEFON AB L M (SE))

[0005] US6188887 Distributed data storage and delivery in a cellular telephone network (Applicant: ERICSSON TELEFON AB L M (US))

[0006] WO02082108 Reverse link handoff mechanism with Hybrid-ARQ and cell site selection in CDMA2000 1XEV-DV systems (Applicant: NOKIA CORP (FI); HSU LIANGCHI ALAN (US); NOKIA INC (US); CHENG MARK W (US))

[0007] GB2377587 Mobile telecommunications system (Applicant: VODAFONE GROUP PLC (GB))

[0008] US2003005127 Method and system for the distributed IP object persistent storage in a large scale network (Applicant: IBM (US))

[0009] DE10061593 (Applicant: PAETZOLD MAIKA (DE)) This describes a mobile protection system incorporating a mobile video telephone device, and aims to act as a crime deterrent through enabling the user to sound an audible alarm for a number of seconds and transmit video and sound data to police. The device is designed to summon police to the scene of an incident and is designed to be operated by a victim on coming under attack. The invention describes how the user may be fined or sued for misuse leading to emergency services being called out unnecessarily. Users will therefore only use this invention once they are certain that it is absolutely necessary to contact police, and will delay using this invention in many cases, potentially putting themselves at risk in potentially dangerous situations and providing opportunity for attackers to snatch the device before the user feels sufficiently threatened to attempt activation of the invention.

[0010] DE10061593 specifies that audio and visual information is transmitted to the nearest police station. Such specification requires recording equipment to be installed at every police station, meaning that considerable expense would be incurred in developing a system to automatically determine which police station was nearest and route data to that particular station. DE10061593 does not transmit data other than audio and visual data, meaning that much potential evidence relating to a situation is not captured or documented by this invention.

[0011] DE10061593 specifies that situations should be documented but does not provide any means for avoiding time delays in documentation and does not provide any means for accurately determining the timeline of such documentation. Time delays may therefore occur in the documentation of such situations, meaning that the precise time of a situation may be impossible to determine from such documentation, and the safety of the user may be compromised during such time delays, as an attacker may potentially destroy the device during such delays.

[0012] DE10061593 does not link a documented individual or individuals to a specific place at a specific time, as timeline data are not generated or transmitted, or recorded.

[0013] DE10061593 specifies that an odour dispenser may be incorporated into the mobile device so that odour may be emitted by the device as a deterrent, but DE10061593 does not provide any means of detecting odours at the scene, or any means of identifying the odour profiles of an attacker or attackers.

[0014] DE10061593 specifies that the mobile device should have GPS functionality but does not claim that GPS location coordinates are transmitted together with sound and video data. GPS data is therefore not documented, according to DE10061593. Emergency services would therefore only be aware of the location of the user providing that the device remains operational, and that emergency services are able to track the device whilst the device remains operational. Emergency services would therefore have difficulty in relating documented sound and video information to the precise location of the device according to a timeline.

[0015] DE10061593 involves the contact and callout of emergency services, and may therefore put considerable strain upon emergency services, leading to significant increases in false alarms and in unnecessary calls to emergency services.

[0016] DE10061593 does not provide any particular means for documentation, and does not provide any means which might enable such documented situations to be automatically compared against other documented situations, and does not provide any means of automatically extracting useful crime detection information from such documented information, meaning that much potential criminal evidence may remain undiscovered.

[0017] DE10061593 does not prevent an attacker from deactivating the device, by switching the device off or removing the batteries for example, and does not prevent an attacker from forcing the victim to deactivate the device, and does not provide any means for activating the invention in the event that the device is snatched from the victim before the victim has had an opportunity to activate the device.

[0018] DE10061593 does not provide any means for capturing video images at night or in total darkness, meaning that DE10061593 is only operational where suitable light conditions exist.

[0019] Published papers:

The Storage and Supply of Data within a Cellular Framework for a Variety of Mobility and Usage Patterns. Justin Champion (J.C.Champion@staffs.ac.uk), Dr John Rees (S.J.Rees@staffs.ac.uk), Ian Sunley (G.I.Sunley@staffs.ac.uk), Staffordshire University, Stafford, Staffordshire, England.

[0020] A QoS Management Architecture for Packet Switched 3rd Generation Mobile Systems. (O. Lataoui, T. Rachidi, L. G. Samuel, S. Gruhl, and Ran Hong Yan, Bell Laboratories, Lucent Technologies, Al Akhawayn University in Ifrane, Morocco) http://www.bell-labs.com/org/physicalsciences/pubs/lataoui.pdf

[0021] THE PROBLEMS ADDRESSED BY THIS INVENTION

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.

[0022] Many women feel apprehensive about meeting men in isolated circumstances, and crimes including date rape often occur inside the victim's own home. In such circumstances criminals know it can be claimed that the victim consented, and should police become involved it will then be the word of the criminal against that of the victim. In many cases such reported rapes do not reach the courts due to insufficient evidence, and statistics show that where the matter is taken to court, in many such cases sufficient doubt often exists in the minds of judges and jurors that the case ends in the acquittal of the accused. For this reason many victims choose not to report such crimes against them, for fear that they will not be believed or that police will be unable to prove that the crime took place.

[0023] Criminals most fear their identity being linked to their crimes. Successful prosecutions depend on police obtaining sufficient reliable evidence linking the identity of criminals to their crimes. The stronger the evidence linking a criminal to a crime, the more likely it is that the criminal will be brought to justice for that crime. Criminals are much less likely to proceed with criminal activity in a particular location when they believe their identity is clearly connected to that particular location at that particular time. Closed circuit television systems help to achieve this but crimes are often committed out of sight of such systems, and in many cases where images of crimes are recorded by CCTV equipment, camera angles and low image resolutions prevent accurate or reliable identification of criminals.

[0024] In the event of a crime occurring in a specific location at a specific time, eyewitnesses often do not come forward and many are never traced, meaning that essential evidence is lost.

[0025] 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. The high incidence of mobile phone theft is testament to the fact that such devices currently act as an irresistible temptation to criminals.

[0026] A number of cellular based emergency services and mobile communications personal safety devices are presently in operation around the world, all essentially providing services similar to those detailed below, yet none of these services act as strong criminal deterrents or provide much protection against crimes of robbery or violence, or link the identity of criminals to their crimes:

[0027] Korea-Wide Child Safety Service (nGeleye);
Users connect directly to a Call Centre through their Geleye handset, and can have several numbers "hot key" programmed into the phone by the subscriber. The service enables parents to track the location of their children in possession of such a device and enables children to use the device to call a friend or relative or security service in an emergency, and reveal their location.

[0028] Japan-Wide Safety Service (SECOM EZ);

This cellular service uses GPS (Global Positioning System) to locate the position of persons needing assistance. Once located, SECOM informs the responsible subscriber of the person's position, and, if necessary, SECOM dispatches emergency personnel to provide assistance. Video recordings must be completed before they can be transmitted as email attachments. SECOM EZ currently provides a number of related services including; personal navigation, friend finder, stolen property recovery, asset tracking, mapping, restaurant guides, train schedules, town guides and weather information.

[0029] "HELPNET Mobile" is an emergency cellular service which allows GPS mobile phone users in Japan to report emergencies to an appropriate authority, such as the police, tow service, hospital, etc. Subscribers to this service are required to enter a few keypresses on a GPS mobile phone to contact a service centre, which detects the user's location and automatically reports to emergency public services. HELPNET Mobile was co-developed by Japan Mayday Service, Co., Ltd. and KDDI Corp

[0030] Various cellular emergency services exist in the United States, linking users to emergency services and providing location coordinates.

[0031] With present devices and technology, in the event that a young woman, for example, finds herself in a threatening circumstance, none of the current devices or services available through handheld mobile communications devices presently provide her with sufficient protection. In the event that she attempts to contact the emergency services there is a strong possibility that an attacker may take the device from her before she is able to explain her circumstances to the emergency services, or may hold a weapon against her, forcing her to inform the emergency services that she called in error.

[0032] In the event that she initiates a sound or video recording of threatening activity towards her, the probability is that the device will be snatched from her before she has had a chance to transmit the recorded images and/or sound. Such recordings are of little use if the handheld device is stolen or destroyed by the criminal. In the event that she attempts to transmit live streaming video of her circumstances to a friend, who could potentially act as an eyewitness to the circumstance, she must first look up her friend's number in the device memory, or dial her friend's number into the keypad. All such actions take up valuable

time and attention in an emergency situation. Should she succeed in initiating such a call, her friend may be unavailable to answer the call.

[0033] In the event that she calls a friend and her friend does answer the call, she may not be able to explain the circumstances of the situation that she faces, for fear of being overheard, and in the event of an attack against her, should the attack be witnessed by the recipient of her call, no recording of the video and sound images would exist following the event unless the recipient was in possession of equipment capable of recording such data, and took the necessary actions to initiate such recordings.

[0034] For these reasons, criminals to not currently view mobile communications handheld devices as a deterrent to criminal activity, on the contrary, they still see them as an attractive target.

[0035] Various devices and objects are presently available for the purpose of self-defence and personal security. Such devices include knives and firearms, stun guns, pepper sprays and personal attack alarms, but many such devices are illegal to carry or use within certain jurisdictions, and in jurisdictions where it is legal to carry and use such devices or objects in self-defence, these objects and devices are frequently taken from victims by their attackers during an attack and used against victims.

[0036] Personal attack alarms act as a deterrent to certain criminals in certain situations, but according to UK police many owners of such alarms forget to carry these devices with them on every occasion and these devices are of little use where the criminal is capable of destroying the device, or if the circumstance occurs in an isolated location out of audible range of others. In cases where a personal attack alarm is heard, the public often mistake such alarms as false alarms as the public are used to hearing car alarms and property burglar alarms and fire alarms trigger spontaneously and for no apparent reason.

[0037] US2002183037 combines a personal attack alarm with a mobile communications device, enabling pre-selected telephone numbers to be dialled automatically or emergency services contacted at the press of a button during an attack. In such circumstances the emergency services may record sound detected by the device's microphone once a successful connection has been made, providing that the high decibel alarm is not activated. This

invention does not capture any images of an attacker or link the identity of the attacker to the specific location at the specific time of the attack and does not capture any sound recordings or data which could be used to identify the attacker. The invention relies on the emergency services making a recording of sounds detected by the device's microphone only in the event that a successful connection is obtained to the emergency services. A major drawback of this invention is that unintentional calls can easily be made to the emergency services whenever the emergency button is accidentally pressed on any such mobile communications device.

WHAT THE INVENTION DOES

[0038] 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.

[0039] The invention further prevents criminals from deactivating the device by locking the device power source securely in place, and disabling all other functionality of the device, and provides a safe means for preventing criminals from forcing the user to deactivate the device.

[0040] 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.

[0041] 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 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.

[0042] In another embodiment of the invention, the device has a burglar alarm feature, incorporating an infrared sensor for detecting human or animal movement, and may be set to trigger the automatic series of actions mentioned above, upon detecting such movement beyond a preset threshold value, thereby capturing and transmitting video, sound and other data relating to a burglary.

[0043] 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.

[0044] 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).

[0045] 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.

[0046] 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.

[0047] 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.

[0048] 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.

[0049] 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.

[0050] In all cases, the user may select an option preventing location coordinates being regularly transmitted or otherwise regularly determined or recorded, thereby hiding the location of the user and preventing tracking of the user, except on pressing the eyewitness button.

[0051] The burglar alarm embodiment of the invention may be used, for example, in a hotel room. The device may be placed in the room with the infrared movement sensor facing into the room, and be set to trigger an audible alarm incorporated into the device and to trigger automatic transmission of audio and visual and other captured data and positioning data to the data storage facility, on detecting movement above a preset threshold value, thereby automatically transmitting and recording evidence relating to a burglary. The device may alternatively be set to operate silently, recording and transmitting data without activating an alarm.

[0052] ESSENTIAL FEATURES OF THE INVENTION

Accordingly, this invention provides 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 the simple trigger initiates a series of automatic parallel or sequential actions causing the handheld device to instantly power up the sensors, and to instantly activate the electronic locking mechanism, and to instantly generate and integrate accurate timeline data with data generated by the sensors as the sensors react to both the environmental conditions at the geographical location of the handheld device and to the behaviour and activities of any individuals present at the location within range of the sensors, wherein the integrated data are further integrated with regularly updating geographical positioning data, and wherein the handheld device instantly transmits all the data as one or more streams of data through one or more wireless connections to one or more telecommunications networks, wherein the data are routed to a data storage facility, wherein the data are automatically organised and stored as evidence linking the individuals to the location according to the timeline, and to the physical presence of the user of the handheld device.

[0053] The evidence is thus stored beyond reach of such individuals referred to and may not be destroyed by such individuals, even in the event that the handheld device is subsequently destroyed.

[0054] The sensors include one or more microphones and one or more digital video cameras with daylight and artificial light and low light sensitivity. 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.

[0055] The data storage facility incorporates computerised digital data recording equipment fully compatible with the handheld device transmissions, and is configured to communicate with a plurality of handheld devices in real time and to receive and to organise and to record mission critical data transmitted from a plurality of handheld devices in real time into a database or databases, controlled by a database application which automatically organises received data packets relating to handheld device transmissions into correct timeline order, against handheld device or user identities.

[0056] In another embodiment of the invention, the device has a burglar alarm feature, incorporating an infrared sensor for detecting human or animal movement, and may be set to trigger the simple trigger mentioned above, upon detecting such movement beyond a preset threshold value.

[0057] NON-ESSENTIAL FEATURES OF THE INVENTION

Sensors incorporated into the handheld device may also include any combination of the following sensors, each of which may possess automatically adjustable sensitivity, or may have directional or non-directional or specific frequency or response sensitivities, and such sensors may each be incorporated into one or more physical sides or surfaces of the handheld device, so that information may be captured by each sensor type simultaneously in all or multiple directions from the handheld device, thereby enabling the device to capture data relating both to the user on one side of the device and to other individuals who may be facing opposing sides of the device:

[0058]
a) One or more digital video cameras with night vision sensitivity
b) One or more digital video cameras with daylight and artificial light and low light and night vision sensitivity
c) One or more digital video cameras with infrared sensitivity
d) One or more digital video cameras with ultraviolet sensitivity
e) One or more infrared sensors
f) One or more ultraviolet sensors
g) One or more movement sensors
h) One or more temperature sensors
i) One or more air pressure sensors
j) One or more air humidity sensors
k) One or more odour sensors
l) One or more bio detectors
m) One or more smoke detectors
n) One or more ultrasound sensors
o) One or more wind speed sensors
p) One or more skin electrical property sensors
q) One or more heart monitor sensors
r) One or more accelerometers

s) One or more fingerprint detector pads

t) One or more iris scanners

u) One or more touch sensitive colour screens

v) One or more text scanners

[0059] The handheld device may also include:

1) A recessed button set to operate at a higher finger pressure than other device buttons, with this button configured to act as the simple trigger, or eyewitness button.
2) Infrared illumination for enabling digital video images to be captured in complete darkness by a digital video camera incorporated into the handheld device.
3) One or more light bulbs or torch lights or flashlights or combination thereof, for enabling video images to be captured automatically by the digital video camera in low light and night conditions and in complete darkness.
4) Quad-mode, quad-band CDMA2000 1xEV-DV Cell/PCS + GSM/GPRS + A-GPS + AMPS circuitry
5) Hybrid (AFLT and A-GPS) positioning and timing technologies
6) Technology for filtering speech sounds and frequencies from other sounds, frequencies, background sounds and background noise.
7) Software applications

[0060] 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.

[0061] INTRODUCTION TO THE DRAWINGS

A preferred embodiment of the invention will now be described with reference to the accompanying drawings in which:

[0062] FIGURE 1 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.

[0063] 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.

[0064] 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.

[0065] DETAILED DESCRIPTION

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.

[0066] 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).

[0067] 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.

[0068] 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.

[0069] 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.

[0070] 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.

[0071] 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.

[0072] 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.

[0073] CDMA2000 1xEV-DV thus provides effective enabling technology for this present invention.

[0074] 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 1 incorporating such technology may be set to automatically adjust mode of operation to suit the particular network it is operating within.

[0075] A software application running on the handheld device 1 is able to determine the maximum data transfer rate and bandwidth limitations of the wireless connection to the cellular network 1 to which the device is connected, and feeds this information into a video graphics application algorithm, which automatically adjusts the resolution and frames per second rate of photographic and or video images transmitted to the data storage facility 7, thereby transmitting images at the best resolution and rates possible at the time of the transmission, according to the particular network and network capacity, together with any required data defining the criteria for correct playback of such images at the data storage facility. Where cellular network resources do not provide sufficient bandwidth for image transmissions, transmissions are automatically restricted to sound and other data by the software application.

[0076] Advanced Forward Link Trilateration (AFLT) is a mobile-based positioning technology where a mobile device takes measurements on signals from several serving base stations 2 and 3 and reports them back to the cellular network 4. Positioning is achieved through timing the signals from the base stations 2 and 3.

[0077] 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.

[0078] 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.

[0079] 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.

[0080] Position Determining Entity (PDE) 9 software uses a handset-based Global Positioning System (GPS) receiver together with Wireless Assisted GPS (WAG) and Hybrid Position Location WAG technology at the network service control point to determine the user location, regardless of terrain. This technology enables high-availability performance and accuracy indoors, outdoors, and in urban and rural conditions where pure network or unassisted GPS solutions fail.

[0081] 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:

[0082] 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.

[0083] 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.

[0084] The following details the preferred embodiment of the data recording and storage facility 7:

[0085] 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.

[0086] Such data are automatically and/or manually organised within a database application residing on a server at the data storage facility 7 or web based server 6 or servers, so that such information may be accessed, retrieved and copied at a later date, according to various criteria, and/or mined for useful information and/or compared and/or combined with other data stored in other similar data storage facilities at other locations and/or against other databases. Such data mining and comparison may include face recognition, and voice recognition, and odour recognition, and fingerprint recognition and criminal profiling software or algorithms.

[0087] The preferred embodiment for data storage at the data storage facility 7 incorporates technology known as "InfiniBand," founded in 1999 by Compaq, Dell, Hewlett-Packard, IBM, Intel, Microsoft, and Sun Microsystems. InfiniBand is a unified interconnect fabric which can handle storage I/O, network I/O and interprocess communication (IPC). It can connect disk arrays, SANs, LANs, servers and server clusters to each other and to the outside world (e.g., a WAN, VPN or the Internet). It is designed primarily for enterprise data centres, where availability, reliability, scalability and performance are key. InfiniBand provides high-bandwidth, low-latency throughput over relatively short distances, and supports redundant I/O paths through a single fabric as well as multiple fabrics, so it can keep a data centre operational even if something fails.

[0088] InfiniBand uses a point-to-point, channel-based, message-passing model over a switched interconnect fabric that can offer many possible paths between two nodes. InfiniBand packets range in size from 256b to 4KB, and a single message (a series of data packets carrying an I/O transaction) can be as large as 2GB. InfiniBand thus provides suitable technology for this invention. The InfiniBand 1.0 specification, finalized in October 2000, allows a channel to use multiple links through a fabric for data rates of 4x (10Gb/s) and 12x (30Gb/s), and is bi-directional.

[0089] While databases have traditionally used block-based storage, there are significant advantages in file-level interfaces. Direct Access File System (DAFS) is a file access protocol based on Network File System (NFS), designed specifically to take advantage of the Direct (RDMA) and asynchronous I/O features of InfiniBand and Virtual Interface (VI) compliant interconnects in high-performance clustered environments. DAFS provides a fast, low latency and reliable file-based storage connection. Database data stored in a DAFS server's file system can then be managed using several types of data management products. In addition, by virtue of being a filing technology, DAFS has the potential to offload some of the internal storage processing that databases currently have to do.

[0090] The electronic locking device securing the removable electronic battery 24 and other components is a simple electronic lock with a time-delay feature, which operates a mechanical lock, and is operated through the handheld device keypad 17. Such technology is commonplace and many mechanisms and technologies presently exist which provide effective solutions for the incorporation of this feature.

[0091] 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.

[0092] 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:

[0093] 1) All other functionality of the handheld device 1 is immediately disabled, including the on/off button 21, meaning that the device cannot be switched off and the initiated process cannot be stopped until a deactivating code known only to the user is input through the keypad 17 or until the battery 24 fully discharges.

[0094] 2) An electronic locking mechanism is activated (not shown), locking the rechargeable battery 24 and other removable components of the handheld device, including the device SIM card (not shown), securely in place. The battery 24 and SIM Card may now only be removed by entering the correct deactivating code, through the keypad 17. The locking device has a time-delay feature, preventing the locking device from releasing the battery 24 immediately. In the event that an attacker forces the user to input the deactivating code, the user may instead input a bogus deactivating code known only to the user, which makes the device appear to have been deactivated or switched off, yet the device continues recording and transmitting images and data. The attacker has no way of knowing if the user has entered the correct deactivating code or the bogus deactivating code, as the device displays identical information and appears the same in each case, and as the battery 24 cannot be removed immediately in each case.

[0095] In the event that the eyewitness button 12 is pressed and the rechargeable battery 24 subsequently becomes fully discharged, the rechargeable battery may only be removed by connecting the device 1 to an electrical mains transformer and/or battery charger to power the device, enabling the unlocking code to be entered through the keypad 17, and enabling the deactivating voice command to be received and activated by the handheld device 1.

[0096] 3) The hybrid A-GPS circuitry built into the handheld device 1 is powered up.

[0097] 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.

[0098] 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.

[0099] 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.

[0100] 7) Electrical equipment operating at the data storage facility 7 or cellular network 4 compares the time displayed by the handheld device 1 against the precise time at the location of the handheld device as determined by precision clocks, and where necessary, the data storage facility 7 or cellular network 4 corrects the timestamp recorded by the handheld device 1 against recordings of data transmitted to the data storage facility 7, thereby ensuring the accuracy of the timestamp.

[0101] 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.

[0102] The invention thus firmly links the identities and behaviours of recorded individuals to particular locations at particular times, and to the physical presence of the user of the handheld device 1 on each occasion, regardless of light conditions.

[0103] 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.

[0104] 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.

[0105] 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.

[0106] 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.

[0107] 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.

[0108] In the event that the handheld device's 1 internal memory components or facilities are or become full to capacity before or during the course of recording such data, priority is given to the present recording. In this event, older data stored in the memory components or facilities of the device are erased, creating more space to enable the present recording to commence or continue.

[0109] 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.

[0110] The user may access and retrieve files which the user has created, by connecting the handheld device 1 to the data storage facility 7 and accessing the user account through an application or operator of the data storage facility 8 and/or 6, and/or access such files through a web site. The user may view a list of all files created by the user and either playback, download electronic copies of those files, email, fax or otherwise send electronic copies of those files to an internet address, or transmit copies of those files to another handheld device 1 or telecommunications device or electronic domain.

[0111] Users may also delete recorded files stored against their device ID or account at the data storage facility 7, but only after a certain time delay. Such a time delay prevents criminals

from forcing their victims to delete any potentially incriminating files relating to themselves. The length of the time delay is determined and set by the data storage facility operator 8 and/or 6.

[0112] The burglar alarm embodiment of the invention referred to above incorporates one or more high decibel audible alarms (operating through the earpiece 15) into the handheld device 1 and additionally incorporates one or more movement detectors in the form of passive infrared sensors 22 capable of sensing changes in thermal radiation caused by movement within a field of view, or incorporates other movement detector technologies for the purpose of detecting movement within a field of view. The infrared sensor or sensors 22 are set to trigger the alarm or alarms and simultaneously trigger the simple trigger and eyewitness commands upon detection of human or animal movement within a field of view of the infrared sensor or sensors exceeding a preset threshold value, thereby acting as a burglar alarm feature which instantly captures, records and transmits all data and evidence relating to a burglary to the data storage facility.

[0113] This feature is either set or disabled by pressing a button or series of buttons 16 & 17, and incorporates a variable preset time delay and flashing light or warning sound, allowing sufficient time to position the device or disable the device without triggering the alarm or eyewitness commands. Additional sensors or technology may be incorporated to detect the precise source and location of movement detected within the field of view. The device 1 may be positioned in a room with the infrared sensor/s 22 facing into the room. Setting the device into an electrical battery charger (not shown) connected to the electrical mains ensures that the batteries are not drained in operating this feature. A user might, for instance, find this embodiment of the invention useful when staying in hotels, or when leaving valuable possessions in a space which is unattended, or may simply use this feature as a domestic burglar alarm, and may incorporate additional remote sensors into the burglar alarm system as outlined in other embodiments detailed below.

[0114] The combined torch and electronic flashlight 25 may be activated by the eyewitness button 12 upon the light sensor detecting light levels below a preset threshold value, thereby providing illumination for capturing images in normal visible light frequencies in low light or dark conditions, and the torch and/or flashlight function may additionally be operated independently of the eyewitness button and eyewitness commands.

[0115] OTHER EMBODIMENTS

In another embodiment of the invention, the handheld device 1 incorporates a high decibel audible alarm and components and technology capable of detecting movement of the handheld device 1 itself. By pressing a button or series of buttons the feature is activated after a preset time delay, allowing sufficient time to position the device without triggering the alarm. Such embodiment enables the device to be used as a burglar alarm, which may, for example, be hung by a cord around a doorknob or window handle, where the alarm is triggered by detected movement of the device itself exceeding a preset threshold value. The trigger of the alarm may additionally be set to initiate the series of actions relating to the pressing of the eyewitness button 12, thereby capturing sound and video and other data relating to the event and to the environmental and geographical location.

[0116] In another embodiment of the invention sensors are detachable from the handheld device and may either remain connected to the handheld device within a certain distance of the handheld device by wire or by optical fibre or by radio or by microwave or by infrared or by other wired or wireless connection, and such sensors may be remotely operated and worn on clothing or placed in a room or rooms, and such sensors may possess a power supply independent of the handheld device or may possess an independent power connection for connecting such sensors to an electrical mains supply.

[0117] In another embodiment of the invention the handheld device 1 incorporates electronic components and circuitry enabling the device to receive transmissions made by domestic and commercial CCTV systems, and/or burglar alarm and fire alarm and smoke detection systems, by wire or by radio, or by telephone connection, or by microwave or infrared connection, for instant relay by the handheld device to the data storage facility 7 and/or to emergency services and/or private security services, on pressing the eyewitness button. Such embodiment improves the safety of data recorded through standalone security systems, preventing criminals from destroying the evidence at the location by removing and destroying tapes, disks or other such storage media. Such embodiment may be used by shop keepers and/or security staff as an additional safety and security measure.

[0118] In another embodiment of the invention the handheld device 1 incorporates an accelerometer component and the series of automatic actions initiated by pressing the eyewitness button are additionally set to initiate on a signal from the accelerometer being

detected by the device beyond a preset threshold value. Such embodiment enables eyewitness data to be automatically recorded in the event of a car crash or other such accident, and on exceptionally rough handling of the device.

[0119] In another embodiment of the invention the handheld device 1 incorporates an alarm and miniature fan or fans which draw air into, over or through an odour sensor or bio detector, and further incorporates chemical detection and/or identification and/or analysis technology. The equipment detects and records chemical profiles and concentrations of airborne atoms, molecules, particles and human odours entering the device, and compares such profiles against a database of known profiles relating to particular substances, compounds, elements, atoms, molecules, bacteria, viruses and other such microscopic materials, so as to identify such materials. Alternatively, analysis of such data may be performed by software and technology incorporated into the software application running at the data storage facility. Such embodiment enables odour profiles of individuals to be captured, particularly in the event that the handheld device is snatched from the hand of the user, and transmitted to the data storage facility as an additional part of the sequence of automatic actions occurring on pressing the eyewitness button 12 , thereby providing further evidence relating to the identification of the recorded individual or individuals, and to the conditions in the location at the time of the transmission.

[0120] Lab-on-a-chip biodetectors and "electronic nose" chips and products are presently available in small handheld devices for detecting decaying food, chemicals, bacteria and illnesses including pneumonia. Such devices have been shown able to detect organisms such as anthrax, and diseases such as cancer and illnesses such as pneumonia, and are capable of identifying human odour profiles. Such devices are able to detect and identify chemical profiles in seconds.

[0121] One example of such technology is Cyrano Sciences' propriety sensor technology, used in a small handheld device, the "Cyranose 320." The technology consists of individual thin-film carbon-black polymer composite chemiresistors configured into an array. The collective output of the array is used to identify an unknown analyte using standard data analysis techniques. The sensor array, along with data analysis algorithms, form the main components of Cyrano's electronic nose. This technology was originated in the labs of Professor Nathan Lewis at the California Institute of Technology.

[0122] This embodiment of the invention incorporates such electronic nose chips and/or other odour sensing technology into the handheld device. The device sensors may be set to automatically and regularly seek to detect certain known materials. When certain odours are detected by the device beyond preset threshold values, the alarm is triggered and information relating to the detected substance is accessed through the connection to the internet, and displayed on the screen of the device, providing the user with relevant safety and/or medical information. In particular, the alarm may be triggered by smoke particles, alerting the user to the possibility of a fire and acting as a smoke detector, and/or the alarm may be triggered by a specific type of smoke such as cigarette smoke or fumes above a particular threshold level, providing the user with information about the concentration of particles and level of health risk in that environment, and/or the alarm may be triggered by carbon monoxide, alerting the user to poisoning, and/or the alarm may be triggered by low levels of oxygen and/or high concentrations of carbon dioxide or ozone, and/or the alarm may be triggered by alcohol fumes, and/or by explosive gases or fumes, and/or poisonous gasses or fumes, and/or by air pollution, and/or by bacterial agents, and/or dust, and/or mites, and/or pollen, and/or or to viral particles, alerting the user to exposure to illnesses such as influenza, and enabling the user to assess the risks of allergic reaction. In all such cases where the alarm is triggered, the device displays information relating to the identification of chemical or substance or type of particle detected, and to the air concentration, and provides any relevant health warnings and/or health information, and provides the user with useful and/or automatic internet links which may immediately be connected to through the device, providing the user with useful and relevant information.

[0123] Through this embodiment, the handheld device 1 may also be operated manually to detect odours such as decaying meat, bad breath, alcohol levels within the breath thereby enabling the user to check his or her level of intoxication, and odours produced by sickness and disease including cancer, and odours produced by excessive or stale body odour, and odours relating to food safety such as salmonella, E.coli, and other such odours, enabling the user to check if food is still safe to eat, or if the user should pay attention to personal health or hygiene and other such concerns.

[0124] On detection of certain odours, the handheld device 1 may be set to automatically connect to authorities and transmit details of such detected substances and/or analysed data to the

authorities, including geographical coordinates and time of detection, thereby assisting the authorities in tracking events such as gas leaks, and/or bio terrorism, and/or influenza outbreaks, and/or other viral or bacterial outbreaks, and/or pollution, and/or other concerns of public and individual health and safety. Other relevant data captured by other sensors incorporated within the handheld device may additionally be included in such transmissions to such departments.

[0125] In another embodiment of the invention the handheld device incorporates components including any number of the following; ultrasound transmitter and sensor, movement sensor, high-sensitivity microphone, heart monitor sensor, and where the components are configured to detect unusual heart rhythms and conditions, cardiac arrest and foetal activity, analysed by software application running within the handheld device, and wherein the software and components may be activated by the user independently of the simple trigger or eyewitness button. Through such embodiment the device may be used in emergency situations to monitor, record and transmit such data to the relevant emergency services, simultaneously as the user conducts a video call and/or video conference communication with emergency services.

[0126] In another embodiment of the invention, pressing the eyewitness button 12 momentarily only records and transmits images and data to the data storage facility 7 for a limited period of time, that time period predetermined by the user or device supplier, and during that time period other functionality of the handheld device is suspended but at the end of that time period the normal functionality of the handheld device again becomes available to the user. In the event that a connection to the data storage facility is not obtained during such time period, the device continues recording data throughout the time period into its memory facilities and continues trying to make the connection beyond the time period, if necessary, until a connection has been made and the recorded data transmitted. Pressing the eyewitness button 12 and holding down this button beyond a preset time period initiates ongoing recording and transmission until the user inputs a code known only to the user into the keypad of the device, or until the battery or other power supply becomes completely discharged and is removed.

[0127] In another embodiment of the invention, pressing the eyewitness button additionally causes all captured data to be recorded inside the data storage facilities of the handheld device.

[0128] In another embodiment of the invention, two or more buttons of the handheld device 1 are pressed in sequence or simultaneously to initiate the automatic eyewitness recording and transmission of information, thereby preventing unnecessary calls to the data storage facility occurring as a result of accidental pressing of the eyewitness button 12.

[0129] In another embodiment of the invention, one or more buttons of the handheld device 1 are held down beyond a certain time period to initiate the automatic eyewitness recording and transmission of information, thereby preventing unnecessary calls to the data storage facility occurring as a result of accidental pressing of the eyewitness button.

[0130] 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 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.

[0131] In another embodiment of the invention the user of the handheld device may dial the telephone number of the device from another handheld device 1 or from any telephone device, or through other electronic means, and transmit a code to the device known only to the user, which triggers the electronic locking mechanism locking the device power source and identification components in place, and prevents any user from making or receiving any calls or communications through the device, or from accessing any data within the device, until a deactivating code known only to the user is entered through the device keypad, or transmitted to the device, or until a deactivating voice command is given.

[0132] 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.

[0133] In another embodiment of the invention the handheld device 1 connects temporarily or permanently to an internet 5 website address, and computerised data recording equipment operating through this website address acts as the data storage facility, having appropriate recording facilities to receive and record all data transmitted by the eyewitness button 12 or buttons of the handheld device 1.

[0134] 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.

[0135] In another embodiment of the invention the handheld device 1 incorporates one or more electronic credit and/or debit cards enabling the user to make purchases against such credit or debit cards through the handheld device, combined with a facility to record and transmit images and data relating to each purchase event as captured by the device sensors, together with financial transaction data communicated between the device and the retail point, thereby documenting interactions with retail and other staff or individuals in case of future disagreement, argument or conflict relating to the purchase or other matter. Such credit card information may be transmitted by the handheld device to a retail point through secure encrypted transmission either directly or indirectly or via a cellular telecommunications network or via a computer network or via a data or telecommunications network by radio or by infrared or by microwave or by email or by other wireless connection to a bank system or retailer system or other commercial system.

[0136] An electronic credit card may be an electronic file or electronic component or data storage device or software application or algorithm incorporated into the handheld device, which stores similar data to that which is stored on a magnetic strip built into plastic credit and debit cards, and communicates such data to retailers and/or other commercial or non commercial establishments upon a user making a purchase. Such communication of data may take place with both user and retailer present in a particular location, or with user and retailer in separate locations and in separate jurisdictions. In one particular embodiment an electronic credit card is a card with a built-in magnetic strip storing the relevant user and banking data designed to slot into a compatible socket or compartment in the handheld device. In another embodiment an electronic credit card is an electronic chip or a card containing an electronic chip which stores the relevant user identification information and banking data and is designed to slot into a compatible socket or compartment of the handheld device. In another embodiment an electronic credit card is an electronic data file stored in the electronic memory components of the handheld device and holds the relevant user information and banking data.

[0137] In another embodiment of the invention the cellular base stations 2 and 3 have data recording equipment at their locations able to receive and record mission critical transmissions from a plurality of handheld devices, acting as a distributed storage network, or acting as relays for later relay to said data storage facility

[0138] In another embodiment of the invention the handheld device 1 incorporates an alarm, temperature sensor, air pressure sensor, air humidity sensor and wind speed sensor. The temperature sensor is detachable and is able to function as a medical thermometer. The thermometer function may be set to sound the alarm above a preset temperature, thereby alerting the user to the need for medical attention in the event of high body temperature. The combined information received by temperature, air pressure, air humidity and wind speed sensors may be analysed by analysis software within the device or software existing on an external computer system to which the device is connected, and provide the user with information relating to current weather conditions and to predictions of future weather conditions. Such data may be combined with data received by the device through commercial weather forecasts, thereby providing the user with accurate information relating to the environmental conditions. Such embodiment enables important information relating to the environmental conditions at the time of an incident to also be captured and

transmitted to the data storage facility as an additional part of the sequence of automatic actions occurring on pressing the eyewitness button 12. Such information would be of particular use in helping to determine the cause of road accidents and other such incidents in which the weather can be a contributory factor to the occurrence or outcome of such an incident.

[0139] In another embodiment of the invention the handheld device 1 connects to a data storage facility 7 through wireless connection to the internet 5 or by wireless connection to an intranet or other external computer or telephone network, without first connecting through the cellular telecommunications network 4.

[0140] 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.

[0141] 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.

[0142] In another embodiment of the invention, pressing the eyewitness button 12 additionally initiates a feature accessing and receiving geographic information system (GIS) mapping information, displaying such information as a map or maps on the screen of the device 13, detailing the geographic area surrounding the device and highlighting the nearest emergency services, and enabling the user to view maps of the location at different scales and in both two dimensional and three dimensional virtual reality representations.

[0143] In another embodiment of this invention, a mapping application uses data stored in data files relating to handheld transmissions, to display the geographical positions and environmental conditions of users on a digital map, according to timeline and geographical positioning data, thereby enabling authorities to bring together all relevant data within a specified radius of any location and within a specified range of times, in a meaningful way,

combined with GIS mapping data relevant to the location and weather data captured by a plurality of handheld devices and available through commercial weather services.

[0144] In another embodiment of the invention the handheld device 1 does not have global positioning components or other geographical or mapping components and capabilities and in such embodiment the handheld device transmits digital images and/or video images and/or sound and/or other recorded data as described in the various embodiments of this invention to the data storage facility 7 without transmitting geographical coordinates.

[0145] In another embodiment of the invention the components of the handheld device 1 are reduced in size and/or fitted more compactly thereby enabling the device to be reduced in size and attached to a wrist strap, and enabling the device to be worn in a similar manner to a wristwatch, or clipped to a belt. The device may be made detachable from the wrist strap for convenient operation, or be a component part of the wrist strap itself. Such embodiment ensures that users always know where to find the device in an emergency and improves the convenience of carrying the device. The size of the device may be reduced through stacked Chip-Scale-Packaging for processor and memory devices, and flip-chip device attach technologies, which enable increased electronic sophistication within a given space.

[0146] In another embodiment of the invention the internal data storage facilities of the handheld device 1 are protected against destruction and physical shock by strong and watertight and fireproof and shock resistant materials, securing data in a similar manner to an aircraft black box recorder.

[0147] In another embodiment of the invention the outer casing and inner supports of the handheld device are made sufficiently robust to enable the device to remain operational following a vehicle weighing up to two tonnes running directly over the device when the device is placed on a hard concrete surface. Such embodiment helps prevent attackers from destroying the device, and common knowledge of such embodiment will act as a deterrent to any such attempt by attackers.

[0148] In another embodiment of the invention the handheld device 1 is made sufficiently watertight to withstand being thrown into water, and to remain operational after being thrown into water. Such embodiment helps prevent attackers from destroying the device

and knowledge of such embodiment acts as a further deterrent to any such attempt by attackers.

[0149] In another embodiment of the invention, the handheld device 1 is made sufficiently buoyant to float on water and sufficiently watertight to remain operational after being thrown into water, thereby protecting any recorded data which has not transmitted successfully, and protecting the device against any attempt at destruction made by throwing the device into water.

[0150] In another embodiment of the invention the handheld device 1 may be incorporated into a computer, or notebook computer, or laptop computer, or tablet computer, or palm computer or personal digital assistant, or other electronic device or built into an item of clothing or an item of luggage.

[0151] 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.

[0152] In another embodiment of the invention, the handheld device 1 incorporates a laser pointer, of the type frequently used by public speakers in making presentations, thereby enabling the user to signal for help or assistance to individuals or groups within line of sight of the device.

[0153] In another embodiment of the invention the handheld device 1 incorporates components enabling the device to receive regular or constant external time signals from high precision atomic clocks or other such high precision clocks other than GPS, broadcast by regular radio or satellite or other such broadcasts, and enabling the device to regularly and automatically correct the time as displayed by the device, thereby ensuring that the timestamp made by the handheld device against recordings of eyewitness data represents a precisely accurate timeline.

[0154] In another embodiment of the invention the timeline data are generated by the cellular network or data storage facility through high precision clocks and equipment able to determine the correct time at the specific location of the handheld device 1 at the time of

real time transmission, and such data are integrated with data transmitted by the handheld device 1 to represent the correct timeline for the transmission, and are set to override or replace any timeline data generated and transmitted by the handheld device.

[0155] In another embodiment of the invention the handheld device 1 incorporates a high-decibel alarm, enabling the device to be operated additionally or simultaneously as a personal attack alarm. This alarm function may be set to activate as part of the sequence of automatic actions which occur on pressing the eyewitness button, or be set to operate through an input or series of inputs and/or actions.

[0156] 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 removing a cord and/or pin from the device. Such initiated recording and transmission continues until the pin is replaced and the correct deactivating code known only to the user is then input through the keypad 17.

[0157] In another embodiment of the invention some or all of the handheld device sensors may be permanently activated and powered up, on powering up the handheld device, or may be powered down until activated and powered up on pressing the eyewitness button.

[0158] In another embodiment of the invention the device power source is a removable rechargeable hydrogen based fuel cell or cells. Such power source may be recharged with a hydrogen based charger.

[0159] 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 dialup connection.

[0160] In another embodiment of the invention the handheld device incorporates at least one or more fingerprint detector pads. Each pad is able to detect fingerprint physical characteristics, thermal characteristics, electrical characteristics, humidity characteristics, pressure characteristics and other such fingerprint or skin characteristics. Such pads may

be activated by the eyewitness button, or operated independently of the eyewitness feature. Such embodiment enables the fingerprints of an attacker or robber to be captured and instantly transmitted along with other data in the event that the handheld device is snatched from the hand of the user. Touch screens for displaying and inputting information into the handheld device may be configured to perform some or all of the features of a fingerprint pad.

[0161] In another embodiment of the invention the handheld device incorporates one or more ultraviolet sensors and/or light sensors, wherein the sensors and the device may be configured to detect the strength of the sun's ultraviolet rays, and alert the user to risk levels to health. This feature is operated independently of the simple trigger or eyewitness button.

[0162] Technologies other than those outlined in this document may be involved or applied to provide alternative means of implementation of the various embodiments of the invention. The invention is not limited to the embodiments described and illustrated above, but can be varied in many ways within the scope and spirit of the invention, which is defined in the appended claims.

CLAIMS

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.

2. A handheld device as claimed in Claim 1 wherein said sensors include one or more microphones and one or more digital video cameras with daylight and artificial light and lowlight sensitivity, and may also or alternatively include any combination of the following sensors:

   a) One or more digital video cameras with night vision sensitivity
   b) One or more digital video cameras with daylight and artificial light and low light and night vision sensitivity
   c) One or more digital video cameras with infrared sensitivity
   d) One or more digital video cameras with ultraviolet sensitivity
   e) One or more infrared sensors
   f) One or more ultraviolet sensors
   g) One or more movement sensors
   h) One or more temperature sensors
   i) One or more air pressure sensors
   j) One or more air humidity sensors
   k) One or more odour sensors
   l) One or more bio detectors
   m) One or more smoke detectors
   n) One or more ultrasound sensors
   o) One or more wind speed sensors
   p) One or more skin electrical property sensors
   q) One or more heart monitor sensors
   r) One or more accelerometers
   s) One or more fingerprint detector pads
   t) One or more iris scanners
   u) One or more touch sensitive colour screens

v) One or more text scanners

3. A handheld device as claimed in Claim 2 wherein each type of sensor may be incorporated into all or opposing physical sides or surfaces of said handheld device so that information may be captured by each sensor type simultaneously in all or multiple directions from said handheld device.

4. A handheld device as claimed in Claim 2 wherein some or all of said sensors may be permanently activated and powered up, on powering up said handheld device, or may be powered down until activated and powered up by said simple trigger or through said series of automatic parallel or sequential actions occurring on the triggering of said simple trigger, or on other input or action.

5. A handheld device as claimed in Claim 1 wherein said handheld device possesses a unique electronic identification and is contactable through one or more telephone numbers.

6. A handheld device as claimed in Claim 1 wherein said handheld device is contactable through one or more email addresses or through other such electronic domains or through wireless messaging services.

7. A telecommunications network as claimed in Claim 1 wherein said network is a cellular telecommunications network.

8. A handheld device as claimed in Claim 1, and cellular telecommunications network as claimed in Claim 7, wherein said data are captured as live data by said sensors and integrated and transmitted in real time as mission critical data through one or more always connected packet data wireless connections to one or more said cellular telecommunications networks.

9. Mission critical data as claimed in Claim 8 wherein said data are transmitted as secure encrypted data.

10. A telecommunications network or cellular telecommunications network as claimed in Claims 1 and 7 wherein said mission critical data are routed in real time to said data storage facility.

11. A data storage facility as claimed in Claim 10 wherein said mission critical data are automatically received and organised according to said timeline data and recorded and logged into a computer database or other such computerised data storage facility in real time.

12. Timekeeping technologies as claimed in Claim 1 wherein said handheld device regularly and automatically corrects the time as displayed by said handheld device through comparing the time as displayed by the timekeeping components of said handheld device to regular radio or satellite or other such broadcasts of precision time signals generated by atomic clocks or other such external high precision clocks, and adjusts the time as displayed by said timekeeping components to correspond with said precision time signals so as to ensure the accuracy and reliability of said timeline data.

13. A personal safety system as claimed in Claim 1 wherein said timeline data are checked by said cellular network or said data storage facility against precision clocks for accuracy and wherein said timeline data are corrected as necessary to reflect the correct time at the location of said handheld device at the time of said transmission.

14. A personal safety system as claimed in Claim 1 wherein said transmitted timeline data are generated by said cellular network or said data storage facility through high precision clocks and equipment able to determine the correct time at the specific location of said handheld device at the time of said real time transmission, and wherein said generated timeline data are integrated with data transmitted by said handheld device to represent the correct timeline for said transmission, and are set to override or replace any timeline data generated and transmitted by said handheld device.

15. A handheld device as claimed in Claim 1 wherein said handheld device incorporates one or more colour screens for displaying photographic images and video data and other data.

16. A handheld device as claimed in Claim 1 wherein said handheld device incorporates one or more touch sensitive colour screens for displaying data and for inputting data into said handheld device.

17. Removable components as claimed in Claim 1 wherein said components may include power source components and device identity components and device communications components and device memory components and device casing components, and wherein said power source components may include a rechargeable battery or batteries, or may include a rechargeable hydrogen based fuel cell or cells, and wherein said identity components may include a SIM card or UIM card and wherein said memory components may include memory chips and memory cards and data storage discs and hard drives and magnetic tapes and magnetic strips.

18. A handheld device as claimed in any proceeding claim possessing a light sensor and technology for automatically adjusting the mode of digital camera operation to suit light conditions.

19. A handheld device as claimed in any proceeding claim possessing at least one or more digital video cameras with low light and night vision sensitivity.

20. A handheld device as claimed in Claim 1 possessing one or more digital video cameras with automatically adjustable daylight and artificial light and low light and night vision sensitivity, wherein said handheld device automatically responds to location light intensities and adjusts mode of operation to maintain optimum performance in all light conditions.

21. A handheld device as claimed in any proceeding claim possessing one or more infrared illumination sources for enabling digital video images to be captured in

complete darkness by one or more digital video cameras incorporated into said handheld device and having infrared sensitivity.

22. A handheld device as claimed in any proceeding claim possessing one or more light bulbs or torch lights or flashlights or combination thereof for enabling video or photographic images to be captured automatically by said digital camera in normal visible light frequencies in low light and night conditions and in complete darkness.

23. A handheld device as claimed in Claim 22 wherein said torch and/or said flash functions may be operated independently of said simple trigger.

24. Sensors as claimed in Claim 2 having directional or non-directional or specific frequency or response sensitivities.

25. A handheld device as claimed in any proceeding claim possessing technology for filtering speech sounds and frequencies from other sounds and frequencies, or from background sound or noise.

26. A handheld device as claimed in any proceeding claim wherein said simple trigger is a single input into said device, which may be any button or input of said device nominated by said user, or may be a recessed button which may be set to operate at a higher finger pressure than other buttons incorporated into said device.

27. A handheld device as claimed in Claim 26 wherein the time duration of said single input beyond a certain preset time period triggers said simple trigger and wherein the time duration of said single input within said time period only triggers said simple trigger for a limited time period, that time period predetermined by said user or device manufacturer, wherein at the end of said time period normal communications functionality of said handheld device again becomes available to said user.

28. A handheld device as claimed in any proceeding claim wherein said simple trigger is a voice activated command.

29. A handheld device as claimed in any proceeding claim wherein said simple trigger is a series of inputs.

30. A handheld device as claimed in any proceeding claim wherein said simple trigger is a number of parallel inputs.

31. A handheld device as claimed in any proceeding claim wherein said simple trigger is triggered by removing a cord or pin from said device.

32. A handheld device as claimed in any proceeding claim wherein any button or navigation control or input feature or combination of such inputs of said device may be set to act as said simple trigger.

33. A handheld device as claimed in Claims 28, 29, 30, 31 and 32, wherein said inputs may require said user to perform actions beyond preset time periods, such as holding one or more buttons down beyond a certain number of seconds.

34. A handheld device as claimed in Claim 1 wherein said series of automatic parallel or sequential actions includes disabling all other functionality of said device including any on/off buttons, so that said device cannot be switched off and the series of said automatic parallel or sequential actions set in process cannot be stopped unless a deactivating code known only to said user is input through said device keypad or until a deactivating voice command is given by said user or until said power source of said handheld device fully discharges.

35. An electronic locking mechanism as claimed in Claim 1 wherein said electronic locking mechanism operates a mechanical lock, locking said power source of said handheld device and other said components securely in place.

36. An electronic locking mechanism as claimed in Claim 35 wherein said power source may only be removed following activation of said series of automatic parallel or sequential actions by entering a correct deactivating code known only to said user through said device keypad, or by a deactivating voice command given by said user and known only to said user.

37. An electronic locking mechanism as claimed in Claim 36 wherein said locking device has a time-delay feature preventing said locking device from immediately releasing said power source and other said components on entering said deactivating code or on giving said deactivating voice command.

38. A handheld device as claimed in Claim 1 wherein said user may input a bogus deactivating code known only to said user through the device keypad or give a bogus deactivating voice command known only to said user which makes said device appear to have been deactivated or switched off, yet said device continues transmitting said data.

39. A handheld device as claimed in Claim 1 wherein entering said bogus deactivating code causes said device to display identical information and appear the same as if the correct deactivating code had been entered, so that only the user is aware if the correct deactivating code has been entered or if said device is continuing to transmit data.

40. A handheld device as claimed in any proceeding claim where in the event that said power source subsequently becomes fully discharged following the triggering of said simple trigger, said power source may only be removed by connecting said device to an electrical mains transformer or battery charger or fuel cell charger to power said device, enabling said deactivating code to be entered through said device keypad, and enabling said deactivating voice command to be received and activated by said handheld device.

41. A handheld device as claimed in Claim 1 wherein said device additionally records all data produced by said automatic parallel or sequential actions into data storage facilities within said device.

42. A handheld device as claimed in Claim 41 wherein said handheld device records all data produced by said automatic parallel or sequential actions into data storage facilities within said handheld device only in the event that data transmission to said data storage facility as claimed in Claim 1 is unsuccessful due to a dropped wireless connection between said device and said telecommunications network.

43. A data storage facility as claimed in Claim 1 wherein said transmitted data are automatically and manually organised within a database application by executable computer code residing on a server or servers at said data storage facility or reside on an internet based server or servers, so that such data may be accessed, retrieved and copied at a later date, according to various criteria, and mined for useful information and compared and combined with other data stored in other similar data storage facilities at other locations or against other databases.

44. A handheld device as claimed in Claim 42 wherein said device constantly attempts to make a wireless connection with one or more cellular base stations in the event that a connection does not already exist, and upon successfully making such a connection to a cellular network connects to said data storage facility and transmits said data recorded inside said device together with live data in real time, so that all such data received at said data storage facility may be automatically organised by said database application, to provide a continuous and unbroken record of events consistent with a continuous timeline from the triggering of said simple trigger.

45. Cellular base stations as claimed in Claim 44 wherein said cellular base stations have data recording equipment at their locations able to receive and record mission critical transmissions from a plurality of handheld devices, acting as a distributed storage network, or acting as relays for later relay to said data storage facility.

46. Data storage facilities within said handheld device as claimed in Claim 41 wherein recording and storage of data relating to the triggering of said simple trigger is given priority over other data or earlier recorded data in the event that said data storage facilities become full to capacity during the course of data recordings initiated by said simple trigger, or are full to capacity prior to the triggering of said simple trigger.

47. Data storage facilities as claimed in Claim 41 wherein said data storage facilities are protected against destruction and physical shock by strong and watertight and fireproof and shock resistant materials, securing data in a similar manner to an aircraft black box recorder.

48. A data storage facility as claimed in Claim 1 wherein said data storage facility is embedded within said cellular telecommunications network architecture as claimed in Claim 7, or embedded within the internet or embedded within a data network architecture or embedded within a telecommunications network

architecture or embedded within the Public Switched Telephony Network or embedded within or connected to any combination of said infrastructures.

49. A data storage facility as claimed in Claim 1 wherein said data storage facility incorporates computerised data recording equipment fully compatible with said handheld device and capable of receiving and recording and storing mission critical data transmissions and communications in real time from a plurality of said handheld devices, and is configured within said architecture to communicate with said handheld devices to receive, record, store and log all mission critical data and communications transmissions in real time from said handheld devices into a database or databases.

50. A data storage facility as claimed in Claim 1 wherein InfiniBand technologies or iSCSI technologies or Fibre Channel Protocol (iFCP) technologies or Fibre Channel over IP (FCIP) technologies or DAFS technologies or Network File System (NFS) technologies or Storage Area Network (SAN) technologies or Network Attached Storage (NAS) technologies or Direct Attached Storage (DAS) technologies or distributed architecture of data storage technologies or any combination of such technologies are utilised.

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.

52. A data storage facility as claimed in Claim 1 wherein said data storage facility creates a unique electronic file within said database to hold all data recorded during said transmission from said handheld device.

53. A database as claimed in Claim 52 wherein said database is controlled by a database application which automatically organises received data packets relating to said electronic file into correct timeline order.

54. An electronic file as claimed in Claim 52 wherein a new file is created for each new transmission received by said data storage facility and wherein a database link between each file and said handheld device or said handheld device owner's identity or account is made.

55. A database application as claimed in Claim 53 wherein said application enables all said files relating to recordings and transmissions made by said user to be accessed by said user through said handheld device or accessed by said user through an internet website and played back or copied or emailed or faxed by said user to an email address or other electronic domain or transmitted by said user to a telephone number or downloaded by said user to a computerised device.

56. A database application as claimed in Claim 53 wherein said application enables users to delete recorded files stored against the electronic identification of said handheld devices related to said users at said data storage facility, following a certain time delay.

57. A database application as claimed in Claim 53 wherein said application enables all said files relating to recordings and transmissions made by said handheld devices within a selected radius of any chosen location and within a selected range of dates and times to be listed and accessed together with details of said handheld device user identities.

58. A mapping application incorporating executable computer code, using data stored in files as claimed in Claim 57 wherein the geographical positions of said users referred to in Claim 57 are displayed on a digital map of said location according to timeline and geographical positioning data.

59. A handheld device as claimed in Claim 1 wherein said user may prevent location coordinates of said handheld device from being transmitted or otherwise determined or recorded except upon triggering said simple trigger.

60. A data storage facility as claimed in Claim 44 wherein electronic equipment compares the present time as displayed and transmitted by said handheld device against the precise time at the location of said handheld device as determined by precision clocks, and corrects the recorded timeline data as generated by said handheld device and stored within the memory components of said handheld device during interrupted live transmissions to said cellular network, according to any time discrepancy between said time as displayed by said device and precise time at the location of said device as determined by precision clocks.

61. A cellular network as claimed in Claim 44 wherein electronic equipment compares the present time as displayed and transmitted by said handheld device against the precise time at the location of said device as determined by precision clocks and corrects the recorded timeline data as generated by said handheld device and stored within the memory components of said handheld device during interrupted live transmissions, according to any time discrepancy between the time as displayed by said device and the precise time at the location of said device as determined by precision clocks.

62. A handheld device as claimed in any proceeding claim wherein said handheld device includes technology enabling said device to connect to multiple protocol cellular networks with technology capable of automatically formatting and transmitting data according to each protocol, and including CDMA and WCDMA and UTMS and GSM and GPRS and AMPS protocols, and which may involve initiating a dialup connection.

63. A handheld device as claimed in any proceeding claim wherein executable computer code runs on said device, capable of determining the maximum data transfer rate and bandwidth limitations of said wireless connection to said cellular network to which said handheld device is connected, and capable of determining if sufficient bandwidth is available for transmission of image data, and capable of restricting the transmission of image data and other data where necessary.

64. A handheld device as claimed in Claim 63 wherein said executable computer code feeds said maximum data transfer rate and bandwidth limitations into a video graphics application algorithm which automatically adjusts the resolution and frames per second rate of photographic and video images transmitted to said data storage facility so as to transmit images at the best resolution and rates possible at the time of said transmission according to the particular cellular network and network capacity and together with any required data defining the criteria for correct playback of such images at said data storage facility.

65. A handheld device as claimed in any proceeding claim wherein said handheld device incorporates one or more high decibel audible alarms and additionally incorporates one or more movement detectors in the form of passive infrared sensors capable of sensing changes in thermal radiation caused by movement within a field of view, or incorporates other movement detector technologies for the purpose of detecting movement within a field of view.

66. A handheld device as claimed in Claim 65 wherein said infrared sensor or sensors are set to trigger said alarm or alarms and simultaneously trigger said simple trigger as claimed in Claim 1 upon detection of movement within range of said sensor or sensors exceeding a preset threshold value, or on detecting human or animal movement within a field of view, thereby acting as a burglar alarm feature.

67. A handheld device as claimed in Claim 66 wherein a time-delay feature enables said movement detector or detectors to be set to detect movement whilst allowing a user sufficient time to set and place said device and to move outside the field of view of said detector or detectors without the movement of said user in so doing triggering said burglar alarm feature.

68. A handheld device as claimed in Claim 66 wherein a time-delay feature provides said user with a sound and or flashing light alert together with a variable preset time period in which to deactivate said burglar alarm feature without triggering said burglar alarm feature.

69. A handheld device as claimed in Claim 67 wherein additional sensors and technology currently available and capable of automatically determining the precise source and location of movement detected within said field of view are incorporated into said device and generate further data for integration with said data transmitted to said data storage facility by said handheld device upon the triggering of said burglar alarm feature.

70. A handheld device as claimed in Claim 1 wherein said device incorporates movement detectors capable of detecting movement of said device, and acting as a burglar alarm feature wherein detection of said movement of said device beyond a preset threshold value triggers both said alarm and said simple trigger, and wherein a time delay feature is incorporated enabling said movement detector to be set and deactivated within a predetermined time period without movement of the device by the user in setting or deactivating said burglar alarm feature triggering said burglar alarm feature.

71. A handheld device as claimed in Claim 1 wherein geographical location determination technologies include Hybrid (AFLT and A-GPS) technologies supporting roaming among different countries onto different carrier networks and into different wireless infrastructures.

72. Geographical location determination technologies as claimed in Claim 1 wherein the calculation to determine the location of said handheld device is performed by said handheld device and wherein said calculation output data are integrated with said transmission data by said handheld device

73. Geographical location determination technologies as claimed in Claim 1 wherein the calculation to determine the location of said handheld device is performed by said cellular network and wherein said calculation output data are integrated with said transmission data by said cellular network.

74. A handheld device as claimed in Claim 2 wherein said fingerprint detector pads detect fingerprint physical characteristics, fingerprint thermal characteristics, fingerprint electrical characteristics, fingerprint humidity characteristics, fingerprint pressure characteristics, and other such fingerprint or skin characteristics, and wherein said fingerprint detector pads may be activated by said simple trigger or independently of said simple trigger.

75. A handheld device as claimed in Claim 15 wherein said screen or screens act as fingerprint detector pads as claimed in Claim 74.

76. A handheld device incorporating one or more odour sensors or bio detectors as claimed in Claim 2 wherein said handheld device incorporates a miniature fan or fans which draw air into, over or through said odour sensors or said bio detectors and where said sensors may be activated by said simple trigger or independently of said simple trigger.

77. A handheld device as claimed in Claim 76 wherein said handheld device incorporates chemical detection or chemical identification or chemical analysis technology capable of detecting and recording chemical profiles and concentrations of airborne atoms, molecules, particles and human odours entering said sensors.

78. A handheld device as claimed in Claim 77 wherein said handheld device incorporates technology capable of comparing said chemical profiles against profiles relating to known odours, substances, compounds, elements, atoms, molecules, bacteria, viruses, pollen and other such microscopic materials so as to identify such materials.

79. A database application as claimed in Claim 43 wherein said database application incorporates technology capable of comparing such profiles as claimed in Claim 77 against profiles relating to known odours, substances, compounds, elements, atoms, molecules, bacteria, viruses, pollen and other such microscopic materials so as to identify such materials.

80. A handheld device as claimed in Claim 77 wherein said handheld device incorporates an audible alarm and wherein said alarm is triggered upon said sensors detecting certain specified materials above certain preset threshold levels.

81. A handheld device as claimed in Claim 1 wherein said handheld device incorporates an audible alarm and wherein said odour and bio sensors as claimed in Claim 2 are configured to automatically and regularly seek to detect certain known odours, substances, compounds, elements, atoms, molecules, bacteria, viruses, pollen and other such microscopic materials, above preset threshold values, and where said handheld device may be set to sound said alarm upon any such detection exceeding preset threshold values and to provide information relating to detected concentrations and profiles, and to connect said user to internet information resources to provide said user with relevant health or safety or medical or other information relating to said microscopic materials.

82. A handheld device as claimed in Claim 81 wherein said microscopic materials include smoke, cigarette fumes, carbon monoxide, carbon dioxide, oxygen, ozone, explosive gasses or fumes, poisonous gasses or fumes, air pollution, dust, mites, bacterial agents, viral particles, pollen, decaying meat, bad breath, alcohol levels within the breath, sickness and disease including cancer and pneumonia, excessive or stale body odour, salmonella, escherichia coli (E.coli) and other such microscopic materials.

83. A handheld device as claimed in Claim 81 wherein said handheld device may be set to automatically alert authorities on detection of certain microscopic materials of concern to public health and safety departments, and automatically transmits data and profiles relating to said detected materials together with geographical coordinates and time of detection to said health and safety departments, and where additional data captured by other sensors incorporated within said handheld device may additionally be transmitted together with said data relating to said detected materials.

84. A handheld device as claimed in Claim 1 wherein said user may activate or deactivate said simple trigger and other device functionality remotely by dialling a telephone number related to said handheld device from another handheld device or from any telephone device connected to the international telephone network, or through connecting to said 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 said data storage facility, or through a cellular network, and entering a code known only to said user, and wherein said user may activate said simple trigger or other device functionality silently and without causing said device to sound a ringing tone or light up any illuminating components of said device on making a connection to said device.

85. A handheld device and data storage facility as claimed in Claim 1 wherein said handheld device connects temporarily or permanently to an internet website address, and wherein computerised data recording equipment operating through said website address acts as said data storage facility.

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.

87. Sensors as claimed in Claim 2 wherein said sensors are detachable from said handheld device and may either remain connected to said handheld device within a certain distance of said handheld device by wire or by optical fibre or by radio or by microwave or by infrared or by other wired or wireless connection, and wherein said sensors may be remotely operated and worn on clothing and placed in chosen locations and wherein said sensors may possess a power supply independent of said handheld device or may possess an independent power connection for connecting said sensors to an electrical mains supply.

88. A handheld device as claimed in Claim 2 wherein said handheld device incorporates an audible alarm and at least one or more of the following sensors: temperature sensor, air pressure sensor, air humidity sensor, wind speed sensor.

89. A handheld device as claimed in Claim 88 wherein said handheld device incorporates analysis software, or wherein an external computer system to which said device is connected incorporates said analysis software, and wherein said software analyses data generated by said sensors and provides said user with information relating to current weather conditions and with information relating to predictions of future weather conditions, and wherein said data and information may be combined with information received by said device or said computer system relating to local weather forecasts, and integrated and transmitted with data generated on the triggering of said simple trigger.

90. A handheld device as claimed in Claim 89 or external computer system as claimed in Claim 89 wherein said handheld device or said external computer system integrates said data relating to said weather conditions and said timeline data with received geographic information system (GIS) mapping data, or other such mapping data, enabling weather conditions and data captured by said handheld device sensors to be mapped according to said timeline, through a computer application incorporating executable computer code so as to produce a map of events following the triggering of said simple trigger.

91. A handheld device as claimed in Claim 90 wherein said integrated data may be displayed on a screen incorporated into said handheld device as a map or maps, or as graphs or charts or as 3D virtual reality representations, and may be configured to highlight nearest emergency services.

92. A handheld device as claimed in any proceeding claim wherein said handheld device connects to a data storage facility through wireless connection to the internet or through wireless connection to an intranet or other external computer or telephone network, without first connecting through a cellular telecommunications network.

93. A handheld device as claimed in any proceeding claim wherein said handheld device connects to a data storage facility through technology known as "Bluetooth" or other similar technologies.

94. A handheld device as claimed in any proceeding claim wherein said handheld device incorporates video conferencing technology, and enables said user to simultaneously take part in a video conference with emergency services and other organisations or individuals following the triggering of said simple trigger.

95. A handheld device as claimed in Claim 94 wherein said handheld device automatically transmits data to emergency services enabling emergency services to instantly locate and access said data file or files relating to the triggering of said simple trigger.

96. A handheld device as claimed in Claim 2 wherein said handheld device incorporates a detachable temperature sensor, which may function both as a medical thermometer and as an air temperature sensor.

97. A handheld device as claimed in Claim 96 wherein said handheld device incorporates an audible alarm and wherein said thermometer may be set to trigger said alarm upon detecting a temperature value above a predetermined body temperature value when held against or inserted into a human body.

98. A handheld device as claimed in Claim 2 wherein said handheld device is set to trigger said simple trigger in the event that said accelerometer component detects sudden acceleration beyond a preset threshold value.

99. A handheld device as claimed in Claim 2 wherein said handheld device incorporates components including any number of the following; ultrasound transmitter and sensor, movement sensor, high-sensitivity microphone, heart monitor sensor, and where said components are configured to detect unusual heart rhythms and conditions, cardiac arrest and foetal activity, analysed by executable computer code running within said handheld device or running on external computer systems, and wherein said computer code and said components may be activated by said user independently of said simple trigger.

100. A handheld device as claimed in Claim 99 wherein said handheld device incorporates an audible alarm and wherein said alarm is triggered by unusual heart rhythms, cardiac arrest, unusual foetal activity and other such health conditions upon pressing said handheld device against the body of an individual, and wherein said computer code provides said user with options to record data relating to said conditions and to contact emergency services and to transmit said data to emergency services whilst conducting conversations or video conferences with emergency services.

101. A handheld device as claimed in any proceeding claim wherein independent remote sensors, which may be part of a commercial or domestic CCTV or fire alarm or burglar alarm or smoke detection or wireless security system, may transmit data to said handheld device by wire or by radio, microwave or infrared

connection, for instant relay by said handheld device to said data storage facility on activating said simple trigger.

102. A handheld device as claimed in Claim 1 wherein said handheld device incorporates one or more electronic credit and/or debit cards enabling said user to make purchases at retail points against such credit or debit cards through said handheld device, and wherein said handheld device incorporates a facility to record and transmit data relating to each purchase event as captured by said sensors together with data generated through transfer of credit card data and financial data relating to said purchase event between said handheld device and said retail points.

103. A handheld device as claimed in Claim 102 wherein said credit card information may be transmitted by said handheld device to said retail point through secure encrypted transmission either directly or indirectly or via a cellular telecommunications network or via a computer network or via a data or telecommunications network by radio or by infrared or by microwave or by email or by other wireless connection to a bank system or retail system or other commercial system.

104. An electronic credit card as claimed in Claim 102 wherein said electronic credit card is an electronic file or an electronic component or a data storage device or executable computer code or algorithm incorporated into said handheld device, which stores similar data to that which is stored on a magnetic strip built into plastic credit and debit cards.

105. Purchases as claimed in Claim 102 where both user and retailer may be present in a particular location at the same time, or where said user and retailer may be in separate locations within a particular jurisdiction or in separate jurisdictions or in separate parts of the world.

106. An electronic credit card as claimed in Claim 102 wherein said electronic credit card is a card with a built-in magnetic strip storing necessary user and banking data, and is designed to slot into a compatible socket or compartment in said handheld device.

107. An electronic credit card as claimed in Claim 102 wherein said electronic credit card is an electronic chip or a card containing an electronic chip which stores the necessary user information and banking data and is designed to slot into a compatible socket or compartment of said handheld device.

108. An electronic credit card as claimed in Claim 102 wherein said electronic credit card is an electronic data file stored in the electronic memory components of said handheld device and holds the necessary user information and banking data.

109. A handheld device as claimed in any proceeding claim wherein the components of said handheld device are reduced in size or fitted more compactly through means such as stacked Chip-Scale-Packaging for processor and memory devices, and flip-chip device attach technologies, or other such means, enabling said device to be reduced in size and incorporated into or attached to a wrist strap,

and enabling said device to be worn in a similar manner to a wristwatch, or clipped to a belt.

110. A handheld device as claimed in any proceeding claim wherein the outer casing and inner supports of said handheld device are made sufficiently robust to enable said device to remain operational following a vehicle weighing up to two tonnes running directly over said device when said device is placed on a hard concrete surface.

111. A handheld device as claimed in any proceeding claim wherein said device is made sufficiently watertight to withstand being thrown into water, and to remain operational after being thrown into water.

112. A handheld device as claimed in any proceeding claim wherein said device is made sufficiently buoyant to float on water and sufficiently watertight to remain operational after being thrown into water.

113. A handheld device as claimed in any proceeding claim wherein said device is incorporated into a computer, or laptop computer, or tablet computer, or palm computer or personal digital assistant, or other such electronic device or built into an item of clothing or into an item of luggage.

114. A handheld device as claimed in any proceeding claim wherein said handheld device incorporates a laser pointer, of the type frequently used by public speakers in making presentations, or other such laser.

115. A handheld device as claimed in any proceeding claim wherein said handheld device incorporates a high-decibel alarm, triggered additionally on the triggering of said simple trigger, or operated independently as a personal attack alarm.

116. A handheld device as claimed in any proceeding claim wherein said user of said handheld device may dial the telephone number of said device from another handheld device or from any telephone device, or through other electronic means, and transmit a code to said device known only to the user, which triggers said electronic locking mechanism and prevents any user from making or receiving any calls or communications through the device, or from accessing any data within the device, until a deactivating code known only to the user is entered through said device keypad, or transmitted to said device, or until a deactivating voice command is given.

117. Data mining and data comparison as claimed in Claim 43 wherein said data may be analysed by face recognition, and voice recognition, and odour recognition, and fingerprint recognition and criminal profiling software or algorithms.

118. A handheld device incorporating an ultraviolet sensor as claimed in Claim 2 and or light sensor as claimed in Claim 18 wherein said sensors and said device are configured to detect the strength of the sun's light and ultraviolet rays, and alert said user to risk levels to health, and where the feature is operated independently of said simple trigger.

Application No: GB 0312170.4 **Examiner:** Robert Shorthouse
Claims searched: 1-118 **Date of search:** 13 October 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance	
Y	1 at least	DE 10061593 A1	(PAETZOLD) See whole document
Y, P	1 at least	WO 03/040995 A2	(BELLSOUTH) See whole document
Y	1 at least	US 6278884 B1	(KIM) See abstract and column 3 lines 13-50
Y	1 at least	JP 2003134258	(MATSUSHITA) See English language abstract, WPI accession number 2003-425370 [58]
Y	1 at least	BE 1013205	(BOUHY) See English language abstract, WPI accession number 2002-055904 [08]
Y	1 at least	DE 10128728 A1	(SIEMENS) See English language abstract, WPI accession number 2003-334323 [32]

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[V]:

H4L

Worldwide search of patent documents classified in the following areas of the IPC[7]:

H04M

The following online and other databases have been used in the preparation of this search report:

WPI, EPODOC, JAPIO, INSPEC

An Executive Agency of the Department of Trade and Industry