US 20160064036A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2016/0064036 A1**

(43) **Pub. Date: Mar. 3, 2016**

Chen et al.

(54) **CLOUD INFORMATION STORAGE, ACCESS, AND SECURITY**

(71) Applicant: **COBAN TECHNOLOGIES, INC.**, Houston, TX (US)

(72) Inventors: **Allan Chen**, Sugar Land, TX (US); **Yun Long Tan**, Sugar Land, TX (US)

(73) Assignee: **COBAN TECHNOLOGIES, INC.**, Houston, TX (US)

(21) Appl. No.: **14/715,742**

(22) Filed: **May 19, 2015**

Related U.S. Application Data

(60) Provisional application No. 62/044,139, filed on Aug. 29, 2014.

Publication Classification

(51) **Int. Cl.**

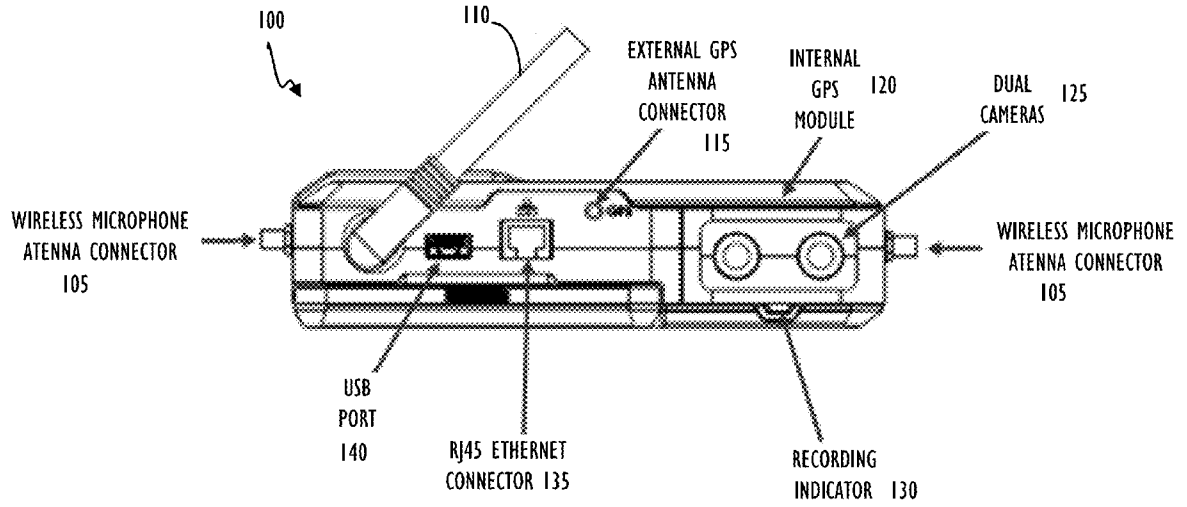
G11B 27/10	(2006.01)
H04N 21/235	(2006.01)
H04N 7/18	(2006.01)
H04N 21/239	(2006.01)
H04N 21/258	(2006.01)
H04N 21/2543	(2006.01)
H04N 21/2743	(2006.01)
H04N 21/214	(2006.01)

(52) **U.S. Cl.**

CPC ***G11B 27/10*** (2013.01); ***H04N 21/2743*** (2013.01); ***H04N 21/2353*** (2013.01); ***H04N 21/214*** (2013.01); ***H04N 21/239*** (2013.01); ***H04N 21/25816*** (2013.01); ***H04N 21/2543*** (2013.01); ***H04N 7/185*** (2013.01)

(57) **ABSTRACT**

Devices and methods for cloud based management of multimedia files and/or associated data files are presented. Methods for using the device(s) to implement different information management techniques for managing information obtained (e.g., recorded) by a plurality of recording devices are also described. A comprehensive use of multiple distinct surveillance systems in a coordinated manner is described. A set of surveillance devices configured for use by one or more law enforcement agencies or other government agencies may upload and share information using cloud information, storage, access, and security methods. Maintaining information using cloud based techniques allows for sharing access (securely and remotely) without redundant copies of information on physical media and may reduce bandwidth transmission requirements. Further, requirements for both chain of custody of evidence and confidentiality regarding digitally recorded evidence may be complied with.



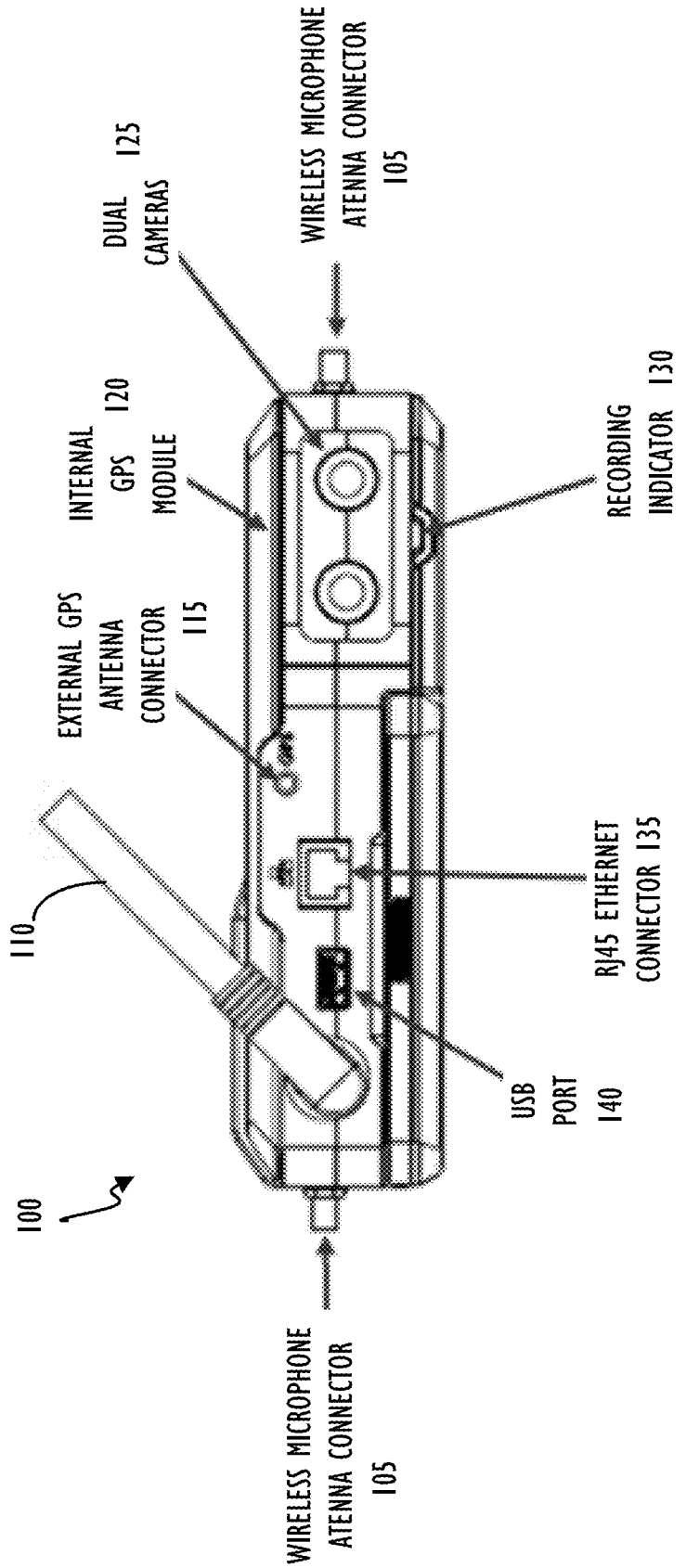

WIRELESS MICROPHONE ATENNA CONNECTOR 105
DUAL CAMERAS 125
WIRELESS MICROPHONE ATENNA CONNECTOR 105
INTERNAL GPS MODULE 120
RECORDING INDICATOR 130
EXTERNAL GPS ANTENNA CONNECTOR 115
110
RJ45 ETHERNET CONNECTOR 135
USB PORT 140
100

FIGURE 1A

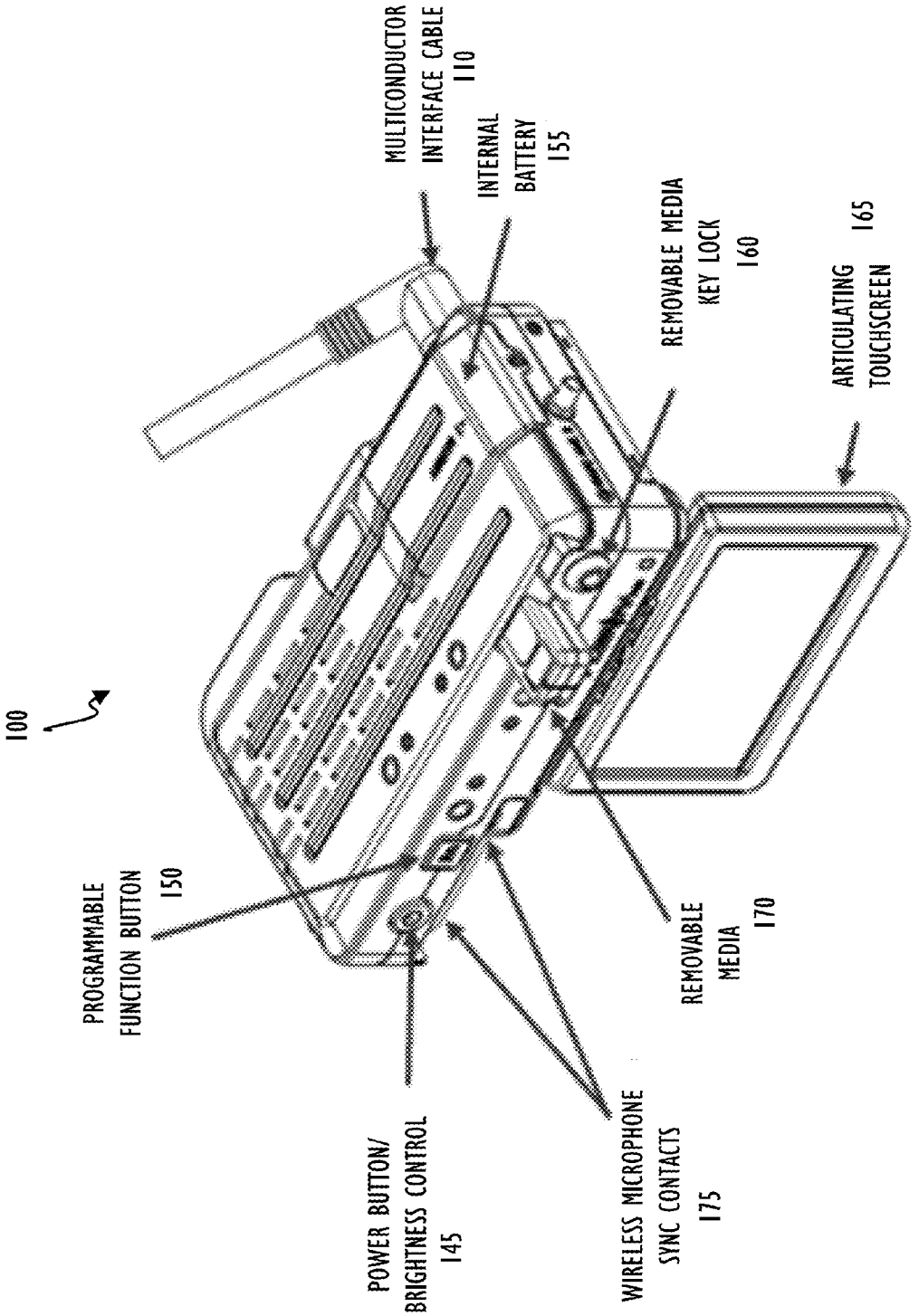

100
MULTICONDUCTOR INTERFACE CABLE 110
INTERNAL BATTERY 155
REMOVABLE MEDIA KEY LOCK 160
ARTICULATING TOUCHSCREEN 165
PROGRAMMABLE FUNCTION BUTTON 150
POWER BUTTON/ BRIGHTNESS CONTROL 145
WIRELESS MICROPHONE SYNC CONTACTS 175
REMOVABLE MEDIA 170

FIGURE 1B

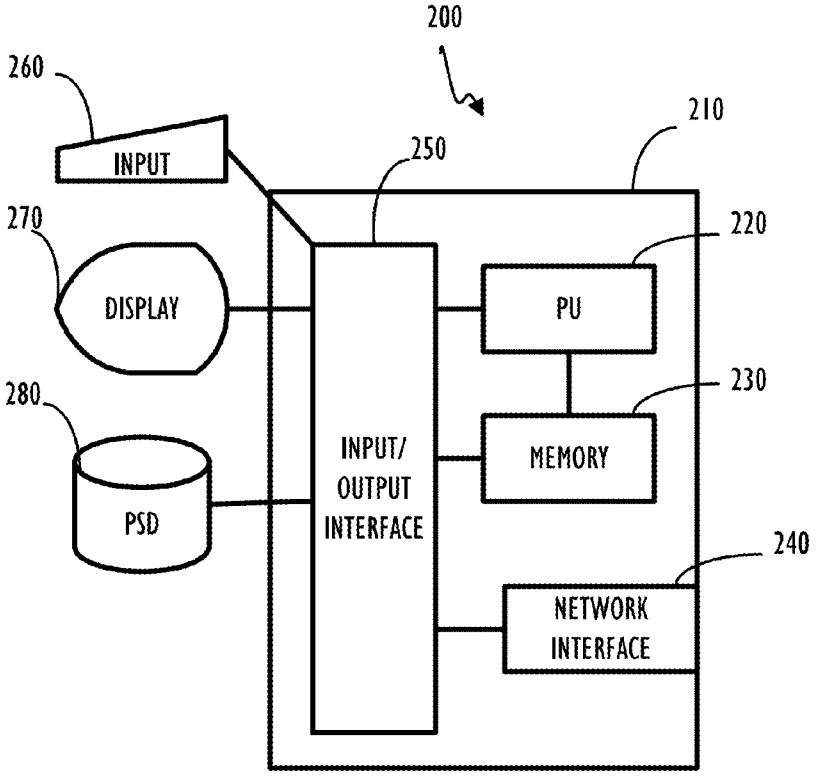


FIGURE 2A

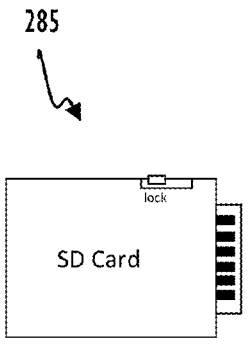


FIGURE 2B

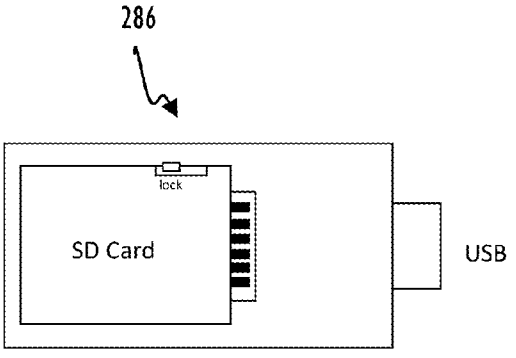


FIGURE 2C

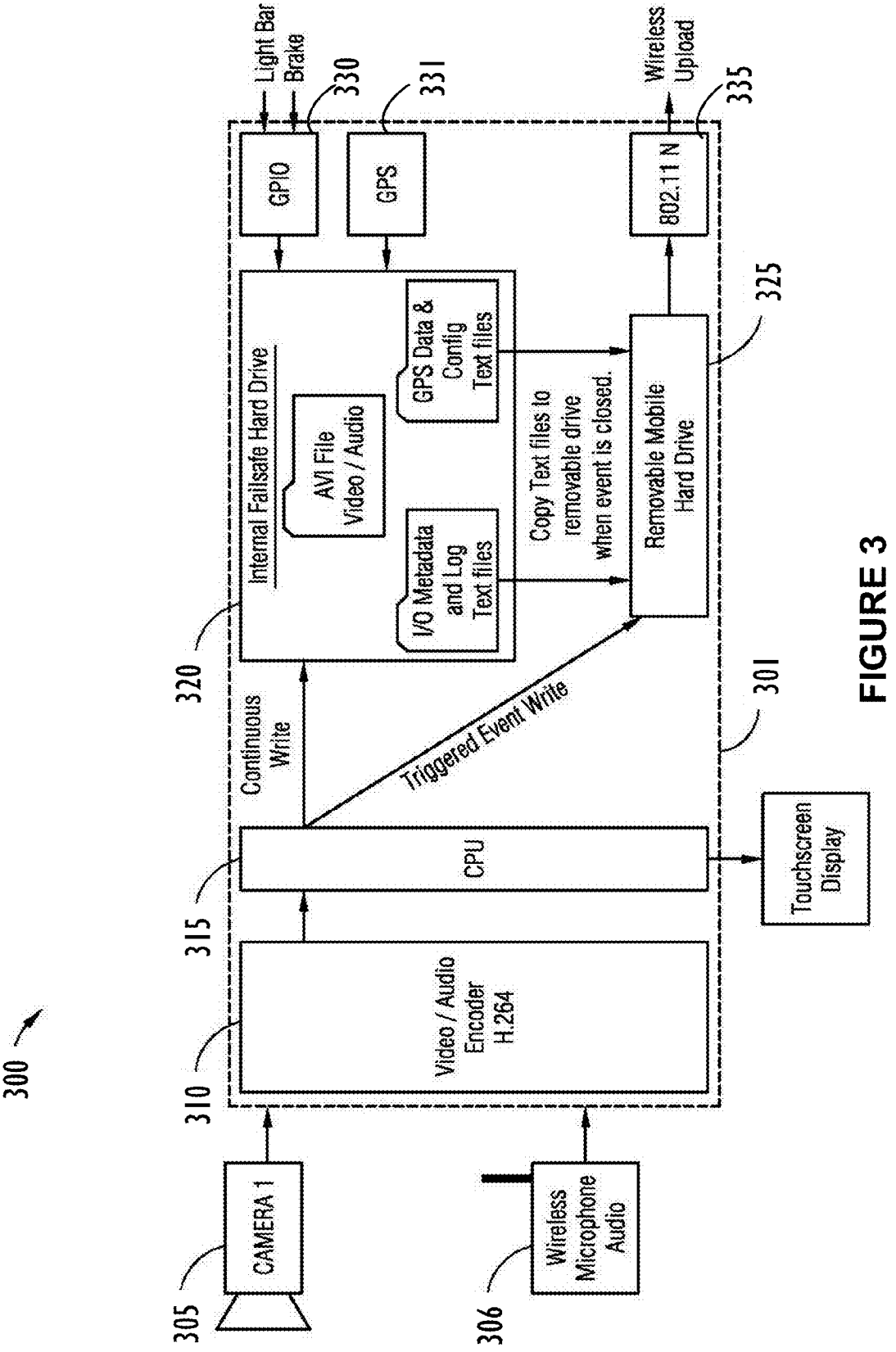

300
305
CAMERA 1
306
Wireless Microphone Audio
310
Video / Audio Encoder H.264
315
CPU
320
Internal Failsafe Hard Drive
AVI File Video / Audio
I/O Metadata and Log Text files
GPS Data & Config Text files
Continuous Write
Triggered Event Write
Copy Text files to removable drive when event is closed.
301
325
Removable Mobile Hard Drive
Touchscreen Display
GPIO
GPS
802.11 N
330
331
335
Light Bar Brake
Wireless Upload

FIGURE 3

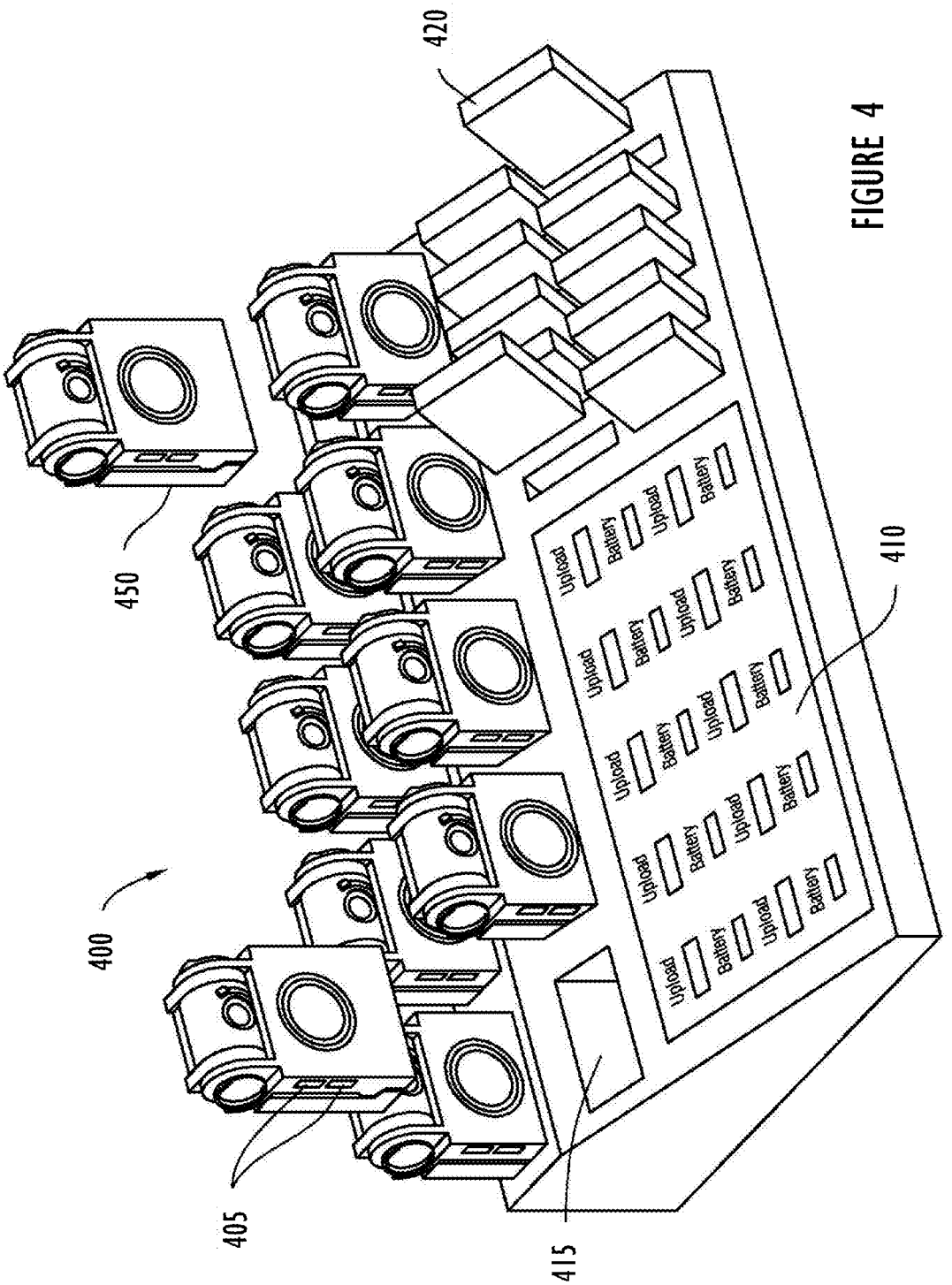


FIGURE 4

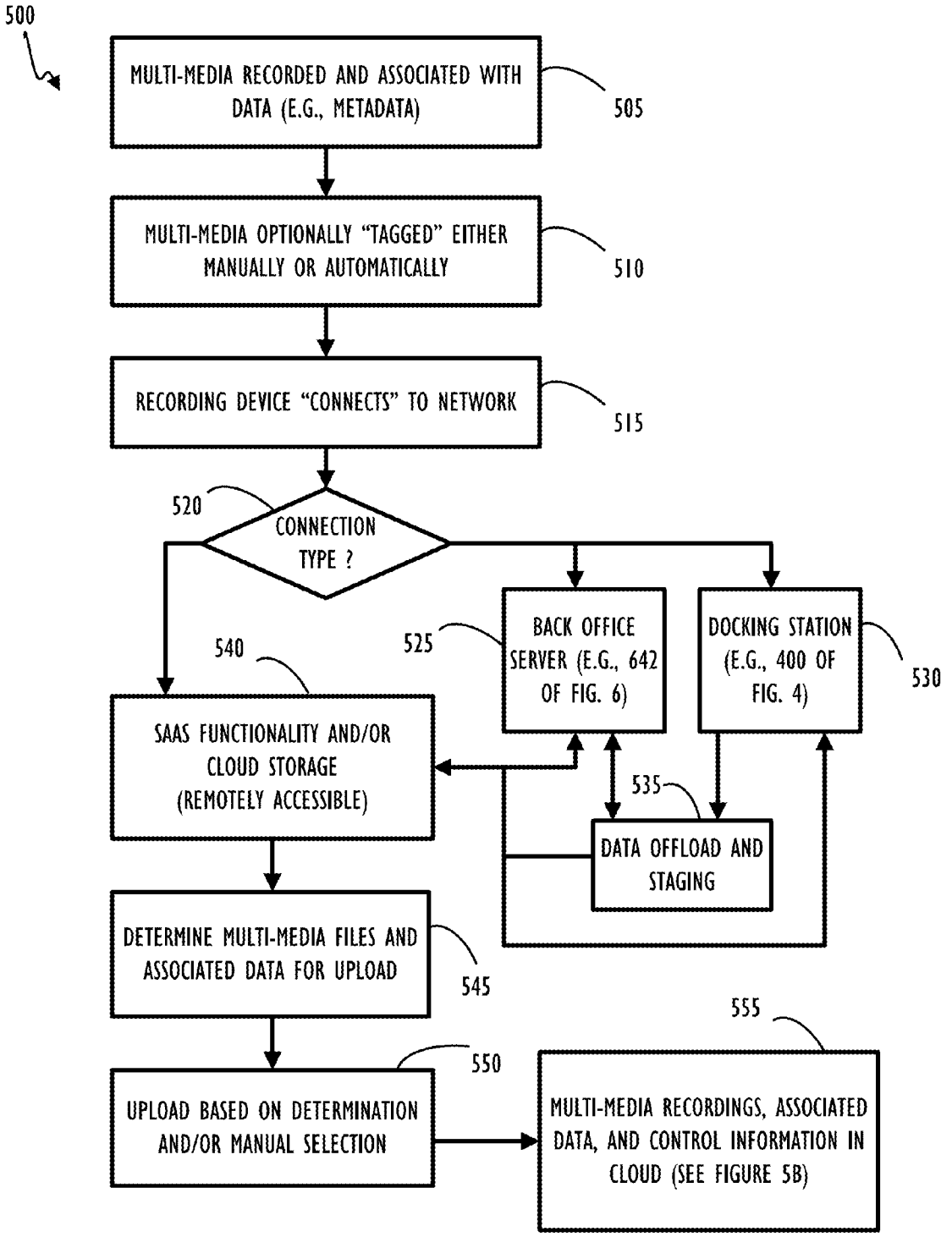

500
MULTI-MEDIA RECORDED AND ASSOCIATED WITH DATA (E.G., METADATA)
505
MULTI-MEDIA OPTIONALLY "TAGGED" EITHER MANUALLY OR AUTOMATICALLY
510
RECORDING DEVICE "CONNECTS" TO NETWORK
515
520
CONNECTION TYPE ?
525
BACK OFFICE SERVER (E.G., 642 OF FIG. 6)
530
DOCKING STATION (E.G., 400 OF FIG. 4)
540
SAAS FUNCTIONALITY AND/OR CLOUD STORAGE (REMOTELY ACCESSIBLE)
535
DATA OFFLOAD AND STAGING
DETERMINE MULTI-MEDIA FILES AND ASSOCIATED DATA FOR UPLOAD
545
555
550
UPLOAD BASED ON DETERMINATION AND/OR MANUAL SELECTION
MULTI-MEDIA RECORDINGS, ASSOCIATED DATA, AND CONTROL INFORMATION IN CLOUD (SEE FIGURE 5B)

FIGURE 5A

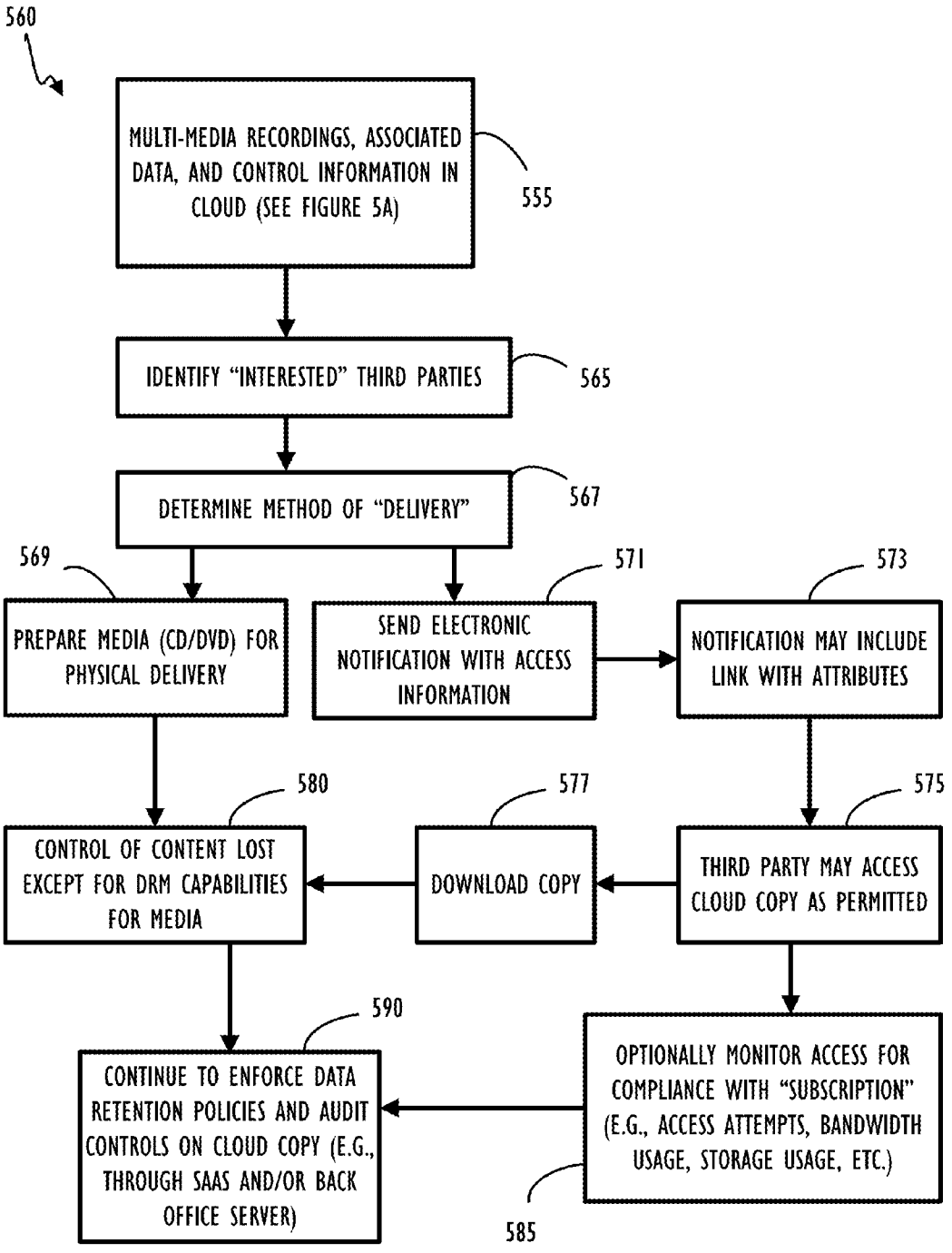

560
MULTI-MEDIA RECORDINGS, ASSOCIATED DATA, AND CONTROL INFORMATION IN CLOUD (SEE FIGURE 5A)
555
IDENTIFY "INTERESTED" THIRD PARTIES
565
DETERMINE METHOD OF "DELIVERY"
567
569
PREPARE MEDIA (CD/DVD) FOR PHYSICAL DELIVERY
571
SEND ELECTRONIC NOTIFICATION WITH ACCESS INFORMATION
573
NOTIFICATION MAY INCLUDE LINK WITH ATTRIBUTES
580
CONTROL OF CONTENT LOST EXCEPT FOR DRM CAPABILITIES FOR MEDIA
577
DOWNLOAD COPY
575
THIRD PARTY MAY ACCESS CLOUD COPY AS PERMITTED
590
CONTINUE TO ENFORCE DATA RETENTION POLICIES AND AUDIT CONTROLS ON CLOUD COPY (E.G., THROUGH SAAS AND/OR BACK OFFICE SERVER)
OPTIONALLY MONITOR ACCESS FOR COMPLIANCE WITH "SUBSCRIPTION" (E.G., ACCESS ATTEMPTS, BANDWIDTH USAGE, STORAGE USAGE, ETC.)
585

FIGURE 5B

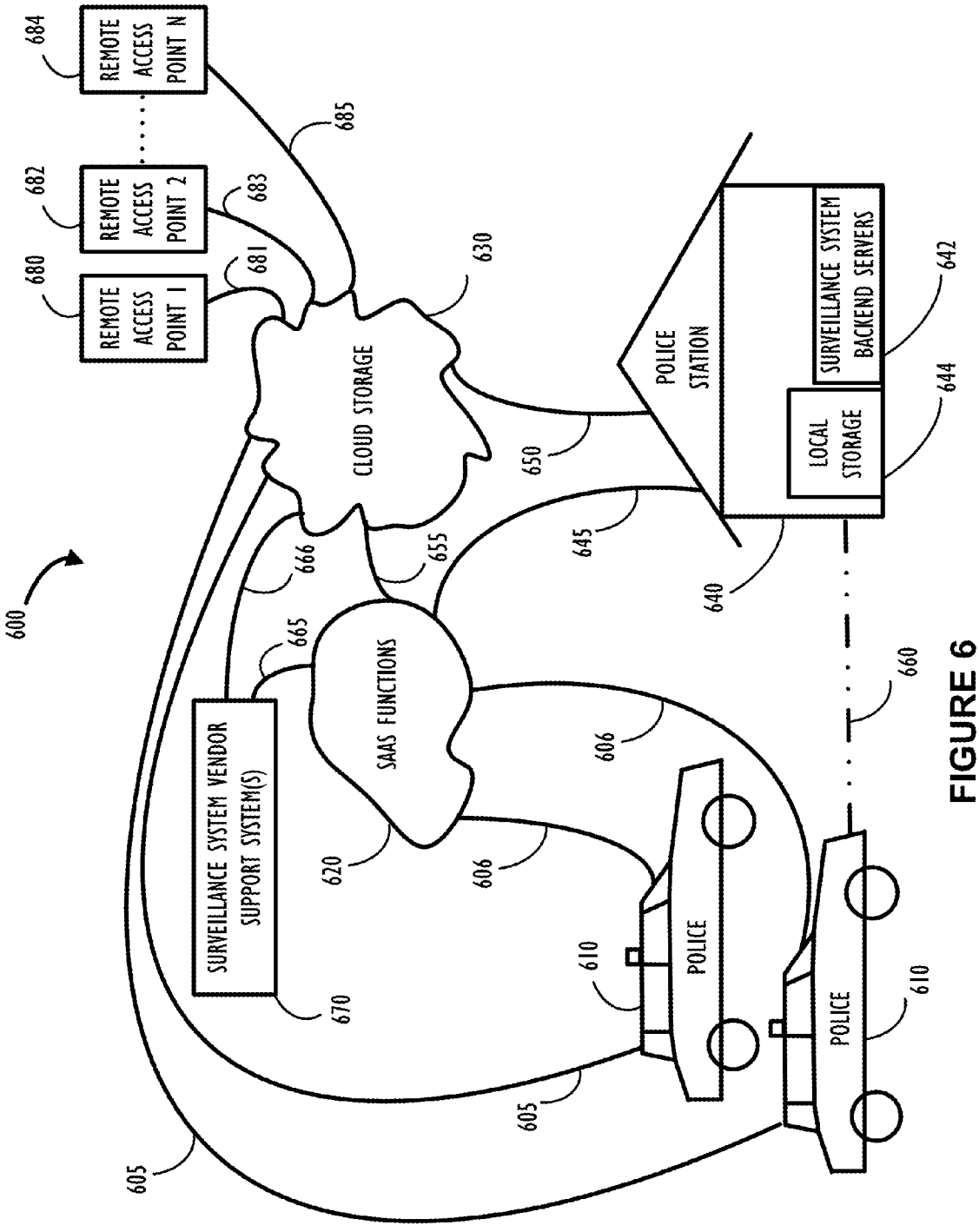

600
605
605
606
606
610
610
610
620
630
640
642
644
645
650
655
660
665
666
670
680
681
682
683
684
685
REMOTE ACCESS POINT 1
REMOTE ACCESS POINT 2
REMOTE ACCESS POINT N
CLOUD STORAGE
POLICE STATION
SURVEILLANCE SYSTEM BACKEND SERVERS
LOCAL STORAGE
SAAS FUNCTIONS
SURVEILLANCE SYSTEM VENDOR SUPPORT SYSTEM(S)
POLICE
POLICE

FIGURE 6

CLOUD INFORMATION STORAGE, ACCESS, AND SECURITY

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of, and priority to, U.S. Provisional Application No. 62/044,139, filed Aug. 29, 2014, and entitled, "Compact Multi-Function DVR with Multiple Integrated Wireless Data Communication Devices," which is incorporated herein by reference.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH

[0002] Not applicable.

FIELD OF THE INVENTION

[0003] This disclosure relates generally to systems and methods to assist in managing information including multi-media and/or associated data files in a cloud based storage area. More particularly, but not by way of limitation, this disclosure relates to systems and methods for managing storage, access, and security requirements of cloud based copies of potential evidentiary information collected by one or more surveillance systems.

BACKGROUND

[0004] Today's law enforcement agencies are increasing their use of digital data to collect surveillance information and other forms of data to be used as evidence in legal proceedings. Devices and methods for managing multi-media files collected as part of this surveillance and evidence collection are increasing both in number and complexity over time. Multi-media files may be large. As used in law enforcement and other industries that require secure access, multi-media files have traditionally been burned onto Digital Versatile Disks (DVDs) or other high capacity storage medium such that the physical media may be transported to another location in a secure manner.

[0005] For example, traditional law-enforcement video solutions typically offer a way to export videos onto optical media such as DVDs and distribute the recorded media to third parties. Third parties typically include other parties to a particular legal proceeding or investigation. Third parties may include the district attorney, defendants, other attorneys, other law enforcement agencies, and so on. For a large agency, creation of optical media may involve expensive equipment (e.g., disc burning and duplication machines) as well as material costs. Technical personnel may also be required to maintain and operate that equipment. Further, once a media is burned into a physical copy, security around access to that physical copy may be a labor intensive undertaking for law-enforcement employees.

[0006] Accordingly, systems and methods for cloud based information storage, access and security as disclosed herein, may provide alternatives to previously known methods of providing access to evidentiary information while conforming to special requirements associated with that type of data.

SUMMARY

[0007] According to a first aspect of the invention, a computer system configured to receive and manage multi-media recordings is disclosed. This embodiment of the computer system includes one or more processors; one or more network communication interfaces communicatively coupled to the one or more processors; and a storage area accessible to the one or more processors. The one or more processors are configured to execute instructions to cause the one or more processors to at least receive at least one multi-media file and one or more metadata files containing attributes of the at least one multi-media file using a network interface. The attributes including at least an event tag for use in categorizing the at least one multi-media file. The one or more processors are further configured to provide a set of evidentiary controls for the at least one multi-media file. Based on the categorization, a third party recipient of the information pertaining to the at least one multi-media file is determined and an indication pertaining to accessing the at least one multi-media file is sent.

[0008] According to a second aspect of the invention, a computer system configured to receive and manage multi-media recordings is disclosed. This embodiment of the computer system also includes one or more processors; one or more network communication interfaces communicatively coupled to the one or more processors; and a storage area accessible to the one or more processors. The one or more processors are configured to execute instructions to cause the one or more processors to receive from a network interface at least one multi-media file and one or more associated metadata files containing attributes including an event tag for the at least one multi-media file. The one or more processors are further configured to categorize the at least one multi-media file using the event tag and provide a set of evidentiary controls for the at least one multi-media file. Also, an automatic upload to a cloud based server of at least a portion of the one or more metadata files and the at least one multi-media file may be automatically initiated based on the categorization.

[0009] According to a third aspect of the invention, a computer system configured to capture and manage multi-media recordings is disclosed. In this embodiment, the computer system includes one or more processors; one or more audio capture devices communicatively coupled to the one or more processors; one or more video capture devices communicatively coupled to the one or more processors; one or more network communication interfaces communicatively coupled to the one or more processors; and a storage area accessible to the one or more processors. The one or more processors are configured to execute instructions to cause the one or more processors to receive information from the one or more audio capture devices and the one or more video capture devices, the information used to create one or more metadata files and at least one multi-media file associated with the one or more metadata files. An event tag may be determined for use in categorizing the created multi-media file. Automatic upload may be initiated to a cloud based server based on the event tag.

[0010] Other aspects of the embodiments described herein will become apparent from the following description and the accompanying drawings, illustrating the principles of the embodiments by way of example only.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] It being understood that the figures presented herein should not be deemed to limit or define the subject matter claimed herein, the applicants' disclosure may be understood by reference to the following description taken in conjunction

with the accompanying drawings, in which like reference numerals identify like elements.

[0012] FIGS. **1**A-B illustrate a rear view and a front view, respectively, of a device for capturing (e.g., recording) multi-media and metadata according to some disclosed embodiments.

[0013] FIGS. **2**A-C illustrates block diagrams of a processing system and two example removable storage devices that may be used for the disclosed integrated mobile surveillance system to capture and store multi-media files and associated metadata according to some disclosed embodiments.

[0014] FIG. **3** illustrates a block system diagram showing some additional internal components for the device of FIGS. **1**A-B, according to some disclosed embodiments.

[0015] FIG. **4** illustrates an intelligent docking, upload, and charging station for recording devices that may interface to cloud accessible storage according to some disclosed embodiments.

[0016] FIGS. **5**A-B illustrates a possible process flow to upload and manage information via a cloud based storage area as may be used between law enforcement personnel and other related third parties. The illustrated process flow may assist in audit tracking and security requirements of the uploaded information according to some disclosed embodiments.

[0017] FIG. **6** illustrates possible data flow and software as a service (SAAS) components for working with information made accessible from cloud based storage according to some disclosed embodiments.

NOTATION AND NOMENCLATURE

[0018] Certain terms are used throughout the following description and claims to refer to particular system components and configurations. As one skilled in the art will appreciate, the same component may be referred to by different names. This document does not intend to distinguish between components that differ in name but not function. In the following discussion and in the claims, the terms "including" and "comprising" are used in an open-ended fashion, and thus should be interpreted to mean "including, but not limited to . . . ." Also, the term "couple" or "couples" is intended to mean either an indirect or direct connection. Thus, if a first device couples to a second device, that connection may be through a direct connection, or through an indirect connection via other devices and connections.

[0019] As used throughout this disclosure the terms "computer device" and "computer system" will both be used to refer to an apparatus that may be used in conjunction with disclosed embodiments of cloud based information, storage, access, and security methods and systems. As used herein, a computer device may be thought of as having a subset of functionalities as compared to a computer system. That is, a computer device may refer to a special purpose processor-based device such as a digital video surveillance system primarily configured for executing a limited number of applications. A computer system may more generally refer to a general purpose computer such as a laptop, workstation, or server which may be configured by a user to run any number of off the shelf or specially designed software applications. Computer systems and computer devices will generally interact with disclosed methods and systems for cloud information, storage, access and security in the same or similar ways.

[0020] The terms "cloud storage" or "cloud based storage" are used interchangeably in this disclosure to describe that data is stored in an area generally accessible across a network (which may or may not be the Internet). A "cloud" may refer to a public cloud, private cloud, or combination of a public and private cloud (e.g., hybrid cloud). The term "public cloud" generally refers to a cloud storage area that is maintained by an unrelated third party but still has certain security measures in place to ensure that access is only allowed to authorized users. The term "private cloud" generally refers to a cloud storage area that is maintained by a related entity or that is maintained on separate physical computer resources from any unrelated users.

[0021] For simplicity the term "multi-media" will be used throughout this disclosure to refer to files collected (e.g., recorded) by an audio or audio/video recorder. Multi-media files may include only audio, only video, or audio and video together and the information may be compressed using an industry standard compression technology (e.g., Motion Picture Expert Group (MPEG) standards, Audio Video Interleave (AVI), etc.) or another proprietary compression or storage format. Multi-media files may have associated data files, including metadata files that may be configured in a structured text format such as eXtensible Markup Language (XML).

[0022] This disclosure also refers to storage devices and storage drives interchangeably. In general, a storage device/drive represents a medium accessible by a computer to store data and executable instructions. Also, throughout this disclosure reference will be made to "plugging in" a storage drive. It is noted that "plugging in" a storage drive is just one way to connect a storage drive to a computer device/system. This disclosure is not intended to be limited to drives that physically "plug in" and disclosed embodiments are also applicable to devices that are "connected" to a computer device or computer system. For example devices may be connected by using a cable or by connecting using a computer bus. Additionally, references to "removable" storage are analogous to plugging-in/unplugging a device, connecting/disconnecting cabled access to a device, and/or establishing/disconnecting networked access to a device or storage area on a network (either wired or wireless).

[0023] As used herein, the term "evidentiary requirements" refers to one or more requirements required for data collected that may later be used as evidence in a legal proceeding. These requirements are discussed throughout this disclosure and include: chain of custody of evidence, access controls, audit functions, retention policies, and the like. The term "evidentiary controls" refers to controlling at least some of the discussed evidentiary requirements.

DETAILED DESCRIPTION OF DISCLOSED EMBODIMENTS

[0024] While various embodiments are described herein, it should be appreciated that the present disclosure encompasses many inventive concepts that may be embodied in a wide variety of contexts. Thus, the following detailed description of exemplary embodiments, read in conjunction with the accompanying drawings, is merely illustrative and is not to be taken as limiting the scope of this disclosure. Rather, the scope of the invention is defined by the appended claims and equivalents thereof.

[0025] Illustrative embodiments of this disclosure are described below. In the interest of clarity, not all features of an actual implementation are described for every embodiment disclosed in this specification. In the development of any such

actual embodiment, numerous implementation-specific decisions must be made to achieve the design-specific goals, which will vary from one implementation to another. It will be appreciated that such a development effort, while possibly complex and time-consuming, would nevertheless be a routine undertaking for persons of ordinary skill in the art having the benefit of this disclosure.

[0026] Embodiments of the present disclosure provide for management and "virtual" sending of multi-media files and/or associated data files stored in cloud based storage. Virtual sending refers to sending of a link, such as a hyperlink, to assist in accessing the remotely stored information rather than sending actual files themselves. In some embodiments, the data shared relates to data that might be collected by one or more, mobile surveillance systems, portable video recording devices, and other types of data recorders. The mobile (and possibly stationary) surveillance system devices may be configured to capture video, audio, and data parameters pertaining to activity in the vicinity of the surveillance system, for example a police vehicle. Other type of vehicles and other situations requiring a surveillance unit are also within the scope of this disclosure. Other types of vehicles may include, but are not limited to, any transportation means equipped with a mobile surveillance system (e.g., civilian transport trucks). The disclosed embodiments are explained in the context of mobile surveillance systems that aid in law enforcement such as busses, ambulances, police motorcycles or bicycles, fire trucks, airplanes, boats, military vehicles, and so on. However, in some embodiments, data collected from other types of vehicles including non law enforcement vehicles may be collected and managed in cloud based storage as required by that different industry.

[0027] Mobile surveillance systems have been in use by police departments for the past few decades. Over that period of time, several advances have been introduced in the technology used to provide video/audio and data regarding specific police events. In the late 1990s through the early 2000s, digital technologies became prevalent in the industry, replacing existing analog technologies. With the use of digital technologies, law enforcement agencies obtained several advances over previous technologies and may further benefit from additional advances (e.g., as described in this disclosure). In general, digital technologies are more adaptable and offer more opportunities for improvement than corresponding analog technologies. This is largely because digital video/audio files may be processed in a multitude of ways by specifically configured computer devices. This disclosure elaborates on several novel techniques to enhance the capability, reliability, ease of use, security, integrity, and other aspects of mobile surveillance systems and the information they collect.

[0028] Today, there are numerous surveillance systems in use by law enforcement and the data they collect continues to increase in volume and complexity. Accordingly, enhanced management techniques for the amount of available data may be required. That is, vast amounts of data may need to be collected and controlled with conformance to "evidentiary requirements" as discussed herein. Additionally, there is a need to improve data access and distribution, integrity, reliability, and security throughout the lifecycle of that data. Legal requirements for data collected by a remote/mobile surveillance system include conformance to judiciary requirements such as "chain of custody/evidence," and "preservation of evidence." Chain of custody (CoC), in legal contexts, refers to the chronological documentation or paper trail audit, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. Preservation of evidence is a closely related concept that refers to maintaining and securing evidence from a particular crime scene before it ultimately appears in a courtroom. For example, the evidence may go to a forensic laboratory prior to arriving at the courtroom. Evidence admissibility in court is predicated upon an unbroken chain of custody. It is important to demonstrate that the evidence introduced at trial is the same evidence collected at the crime scene [e.g. that is, all access to the evidence (e.g., electronic files) was controlled and documented], and that the evidence was not altered in any way. Requirements for law enforcement are further described in "Criminal Justice Information Services (CJIS) Security Policy," version 5.3 published Aug. 4, 2014 referenced as "CJISD-ITS-DOC-08140-5.3" which is hereby incorporated by reference in its entirety.

[0029] As will be recognized, disclosed embodiments may allow for comprehensive back-office video management software to be provided using a software as a service (SAAS) architecture, giving each agency (even small remote agencies) the tools they need to capture, transfer, store and manage their digital video evidence from car to court. That is, the disclosed system and back-office management techniques meet the preservation of evidence requirements outlined above with respect to management of digital evidence for law enforcement. All activity with respect to digital evidence in the back-office system may be logged to ensure proper documentation of evidence handling. The disclosed system may include electronic transfer of evidence in a controlled manner and may provide comprehensive coordination of potential evidence captured from a plurality of surveillance systems. While the focus of this disclosure relates to cloud based maintenance and access to collected data, the disclosed system may also include integrated DVD burning software at different points in the evidence maintenance lifecycle as a means of evidence transfer to work in conjunction with cloud based maintenance and "virtual" transfer.

[0030] Referring now to FIGS. **1**A-B, disclosed embodiments of an integrated mobile surveillance system **100** are intended to incorporate a plurality of functions as being "built-in" to mobile surveillance system **100**. Additionally, aspects of integrated mobile surveillance system **100** have been designed with consideration for future expansion as new technologies and capabilities become available. Aspects of integrated system **100** include, but are not limited to, the following integrated functional units. Integrated system **100** may be configured to have one or more than one of each of these functional units, as appropriate. Integrated wireless microphone receivers **105** to allow capture of audio from a remote wireless microphone located within proximity of integrated system **100**. An external multi-conductor interface cable **110** to allow a wired connection to one or more internal interfaces of integrated system **100**. Universal serial bus (USB) port(s) **140** for general peripheral connectivity and expansion. An integrated global positioning system (GPS) module **120** with optional external antenna or connector **115** to be used in part for capturing location data, time sync, speed logging. The GPS information may also be used for time synchronization and to coordinate data, ultimately facilitating map based search and synchronization (e.g., locate recorded information from a time and/or location across a plurality of recording devices). Dual front facing cameras **125**

may include both a wide angle video camera and a tight field of view camera for optical zoom effect snap shots. A record indicator **130** provides an indication of a current operating mode for integrated system **100**. A wired Ethernet adapter (e.g., Gigabit, 10/100 BASE-T, etc.) **135** (or a wireless network adapter, not shown) for data upload, computer interface, remote display and configuration. Additionally, multiple wireless data communication devices (not shown) may be integrated for flexibility and expansion. For example, the system may include adapters conforming to wireless communication specifications and technologies such as, 802.11, Bluetooth, radio-frequency identification (RFID), and near field communication (NFC). Each of these interfaces may be used, at least in part, for data exchange, device authentication, and device control. A serial port (not shown) may be used to interface with radar/laser speed detection devices and other devices as needed. A G-Sensor/Accelerometer (not shown) may be used for impact detection and to automatically initiate record mode. The G-Sensor/Accelerometer may also provide data logging for impact statistics and road condition data. A DIO (Digital Input/Output) (not shown) that may be used for external triggers to activate record mode and/or provide metadata to the system. The DIO may also be used to control external relays or other devices as appropriate. The DIO may also be used to detect brake, light bar, car door, and gun lock so that the video recording may be automatically triggered. As shown in FIG. **1**B, a combination power button and brightness control **145** may be used to turn on the system and control the brightness of the monitor after the system is turned on. Programmable function button **150** provides a user definable external button for easy access to instigate any function provided by integrated system **100**. For example, rather than traversing through a set of menus on articulating touch screen **165**, a user may define function button **150** to perform an action with one touch (e.g., instant replay, event tagging of a particular type, etc.). An articulating touch screen **165** that may be used to view video in real-time, or in one or more play back modes. Touch screen **165** may also serve as an input mechanism, providing a user interface to integrated system **100**. An integrated speaker (not shown) may be used for in-car audio monitoring and in-car video/audio file playback. An integrated internal battery **155** for proper shutdown in the event of sudden power loss from the vehicle that might occur as a result of a crash, for example, is shown. Also depicted is a removable media **170** that in accordance with some embodiments may be an SSD Flash drive (e.g., secure digital (SD) or universal serial bus (USB) type), including any type of storage that may be inserted or attached to the system via a storage interface (e.g., SCSI, SATA, etc.). For security of access to data, removable SSD flash drive **170** may be secured via a mechanical removable media key lock **160**. In some embodiments, event based data is recorded and written to the removable drive to be transferred to a back office server and/or cloud repository for storage and management. Wireless microphone sync contacts **175** may be configured to synchronize a wireless microphone/camera, such as a body worn camera and microphone, for communication with integrated system **100**. In addition to actual sync contacts, that require physical contact, other synchronization methods for wireless microphone/cameras include utilizing NFC or RFID capability between the wireless device and integrated system **100**.

[0031] In addition to the components mentioned above, disclosed embodiments of integrated mobile surveillance system **100** may be configured to include functional components to provide operational characteristics that may include the following. A pre-event playback function which may be used to tag historical events. Recall, normal operation may be to record continuously to internal storage and to store tagged information (e.g., marked for export) to removable storage. However, in order to cover the case in which an incident occurred without a timely event trigger, the operator may instruct the system to navigate back to an earlier time captured in the internal storage and play back that video/audio information. The selected historical video, at any available point in time, may be marked, tagged for extraction, and stored to removable storage, as if the event had been tagged at that historical time. Another functional component may provide an instant replay function configured to playback the last predetermined amount of time with one button press. Note that both the instant replay and pre-event playback (along with general system operation) allow for simultaneous playback while the system is concurrently recording information. Pre-defined event tags and a pre-defined event tagging functions may also be provided. For example, tags may include DWI, felony, speeding, stop sign, chase, etc. The tagging action may be used to catalog portions of recorded data. For example, after an event is cleared, such as stop recording, an option to select a predefined event may be displayed. Upon selection the system may allow an associated portion of collected information to be marked in a text file for current and future identification and storage. Further, when the tagged information is transferred to the data management software, the tagged information may be searched by event type and maintained on the server or in the cloud with the proper retention period as appropriate—based on the defined event type. A streaming function may also be provided to stream live view and recorded video, audio, and/or data over available wireless and wired networks. The integrated system **100** may also integrate "hotspot" capabilities which allow the system to serve as an agency accessible, mobile wireless local area network (WLAN).

[0032] Referring now to FIGS. **2**A-C, possible internals and peripheral components of an example device **200**, which may be used to practice the disclosed functional capabilities of an integrated surveillance system such as system **100**, are shown. Example device **200** comprises a programmable control device **210** which may be optionally connected to input device **260** (e.g., keyboard, mouse, touch screen, etc.), display **270** or Program Storage Device (PSD) **280**. Also, included with programmable control device **210** is a network interface **240** for communication via a network with other computers and infrastructure devices (not shown). Note network interface **240** may be included within programmable control device **210** or be external to programmable control device **210**. In either case, programmable control device **210** may be communicatively coupled to network interface **240**. Also, note PSD **280** represents any form of non-volatile storage including, but not limited to, all forms of optical and magnetic storage elements including solid-state storage.

[0033] Program control device **210** may be included in a device **200** and be programmed to perform techniques including cloud based storage of data and/or associated multi-media files, in accordance with this disclosure. Program control device **210** comprises a processor unit (PU) **220**, input-output (I/O) interface **250** and memory **230**. Processing unit (PU) **220** may include any programmable controller device including, for example, the Intel Core®, Pentium® and Celeron®

processor families from Intel and the Cortex ARM processor families from ARM® (INTEL® CORE®, PENTIUM® and CELERON® are registered trademarks of the Intel Corporation. CORTEX® is a registered trademark of the ARM Limited Corporation. ARM® is a registered trademark of the ARM Limited Company). Memory **230** may include one or more memory modules and comprise random access memory (RAM), read only memory (ROM), programmable read only memory (PROM), programmable read-write memory, and solid state memory. One of ordinary skill in the art will also recognize that PU **220** may also include some internal memory including, for example, cache memory.

[0034] Various changes in the materials, components, circuit elements, as well as in the details of the illustrated systems, devices and below described operational methods are possible without departing from the scope of the claims herein. For instance, acts in accordance with disclosed functional capabilities may be performed by a programmable control device executing instructions organized into one or more modules (comprised of computer program code or instructions). A programmable control device may be a single computer processor (e.g., PU **220**), a plurality of computer processors coupled by a communications link or one or more special purpose processors (e.g., a digital signal processor or DSP). Such a programmable control device may be one element in a larger data processing system such as a general purpose computer system. Storage media, as embodied in storage devices such as PSD **280** and memory internal to program control device **210** are suitable for tangibly embodying computer program instructions. Storage media may include, but not be limited to: magnetic disks (fixed, floppy, and removable) and tape; optical media such as CD-ROMs and Digital Versatile Disks (DVDs); and semiconductor memory devices such as Electrically Programmable Read-Only Memory (EPROM), Electrically Erasable Programmable Read-Only Memory (EEPROM), Programmable Gate Arrays and flash devices. These types of storage media are also sometimes referred to as computer readable medium or program storage devices.

[0035] FIG. **2**B illustrates a secure digital (SD) card that may be configured as the removable storage device described above. An SD card is a nonvolatile memory card format for use in portable devices, such as mobile phones, digital cameras, handheld consoles, and tablet computers, etc. An SD card may be inserted into a receptacle on the device conforming to the SD specification or may alternately be configured with an interface to allow plugging into a standard USB port (or other port). An example of the adapter for USB compatibility is illustrated in FIG. **2**C. Modern computer operating systems are typically configured to automatically permit access to an SD card when it is plugged into an active computer system (sometimes referred to as plug-n-play). In computing, a plug and play device or computer bus is one with a specification that provides for or facilitates the discovery of a hardware component in a system without the need for physical device configuration or user intervention in resolving resource conflicts. Because of additional security requirements regarding data access with respect to the law enforcement field, disclosed systems may incorporate a specifically modified interface to the removable storage drive utilized in device **100** (i.e., removable media **170**). Modifications permitting specialized access to removable media, such as a secure storage drive, are described in co-pending U.S. patent application Ser. No. 14/588,139, entitled "Hidden Plug-in Storage Drive for Data Integrity," by Hung C. Chang, which is incorporated by reference herein. Modifications permitting specialized functionality from removable media are described in co-pending U.S. patent application Ser. No. 14/593,722, entitled "Self-contained Storage Device for Self-contained Application Execution," by Allan Chen et al., which is incorporated by reference herein. Modifications permitting enhanced storage and upload models are described in co-pending U.S. patent application Ser. No. 14/686,192, entitled "Shared Server Methods and Systems for Information, Storage, Access, and Security," by Allan Chen et al., which is incorporated by reference herein.

[0036] Referring now to FIG. **3**, block diagram **300** illustrates one embodiment of an integrated audio-video-data surveillance system. Note that each of the components shown in block diagram **300** may be communicatively coupled to other components via communication channels (e.g., bus) not shown in the block diagram. The flow arrows of block diagram **300** are very general in nature. In use, video and audio may be captured by camera **305** and microphone **306** respectively. Captured data may be provided initially to video/audio encoder **310** to encode and optionally compress the raw video data and the encoded data may be stored in a memory area (not shown) for access by CPU **315**. Encoded data may also be selectively stored to either internal failsafe hard drive **320** or removable mobile hard drive **325** individually or to both simultaneously. Data may also be transferred, for example at the direction of a user, from internal failsafe hard drive **320** to removable mobile hard drive **325**. Data capture devices such as general purpose input output (GPIO) **330** and GPS **331** may be used to capture metadata to associate with captured surveillance information (e.g., multi-media files). All pertinent captured metadata may be associated with captured video/audio recordings using structured text files such as, for example, eXtensible Markup Language (XML) files. In addition to captured metrics provided by real-time capture inputs, XML files may be utilized to store many different types of metadata associated with captured video and data. This collection of metadata may be used to provide enhanced security and auditing functions associated with the surveillance information (e.g., multi-media recordings). That is, the metadata may describe, when, where, who, and why information was accessed, among other things, in addition to indentifying security parameters for access to the surveillance information. The metadata may include, but not be limited to, timestamps of capture, [internal clock (not shown) of system **100** may be synchronized using GPS data] event tags, GPS coordinates, GPS and RADAR/LIDAR measurement from a target vehicle, breathalyzer analysis information, analytical information, and so on. Wireless interface **335** (or a wired interface (not shown) when available) may be used to upload information from one or more surveillance systems to back office servers located, for example, at a police station or to cloud based resources. Back office servers and cloud based resources will be discussed in more detail below with reference to FIGS. **5**A-B and **6**.

[0037] Referring now to FIG. **4**, advanced docking station **400** may provide additional benefits for users that maintain a plurality of portable body worn cameras **450** and/or a plurality of surveillance systems. Docking station **400** may also perform different aspects of the cloud upload process described below in FIGS. **5**A-B. Some or all portable body worn cameras **450** may incorporate one or more programmable function buttons **405**. As shown in FIG. **4**, docking

station **400** may have multiple ports/cradles **415**. Docking station **400** may assist in data upload, device checkout, device upgrade (e.g., firmware/software update), recharging of battery packs **420** and other maintenance type functions that may be performed, for example, at a police station. For clarity, not all repeated elements in FIG. **4** have an associated reference number. Embodiments of the disclosed docking station may support maintenance functions for multiple portable devices such as body worn cameras **450** concurrently. The disclosed docking station **400** may be multifunctional for uploading and/or downloading of video/audio and associated metadata. Configuration data such as unit ID, user ID, operational modes, updates, and so on, may be maintained and versions of such configuration information may be presented on display screen **410** (which may also be a touch screen interface to docking station **400**).

[0038] Docking station **400** may have integrated interfaces to different types of surveillance systems. Interfaces such as, USB, wired Ethernet or wireless network, as well as interface ports for battery charging may be included. Docking station **400** may also contain: a CPU and be configured as a computer device (see FIG. **2**) with optional integrated touch screen display **410**, output connectors (not shown) for an optional external display/mouse or device expansion. Docking station **400** may have an option for a wireless display (not shown) to be used for status indication as well as for user interface capabilities. Docking station **400** may include wireless communications such as Bluetooth and/or 802.4AC/AD. Docking station **400** may also be configured to work as an Access Point for a wireless network or may be configured to act as a bridge to allow portable client devices to access functionality of docking station **400** and possibly connect to other system components including local or cloud based servers. Docking station **400** may also include functional software or firmware modules to support automatic upload to cloud based storage based on different criteria associated with multi-media and/or data files. Upload to cloud based storage is discussed in more detail below with reference to FIGS. **5**A-B and **6**.

[0039] Docking station **400** may also have an internal storage device to facilitate fast off-load storage which may be used to facilitate a download/forward process for audio/video and metadata captured on a surveillance system device (e.g. the body worn camera **450**). For example, the user may place the body worn camera **450** into a docking station cradle **415** and docking station **400** offloads the data to the local onboard storage drive (not shown) which may immediately (or based on a timer) upload that information, or a portion thereof, to a server (e.g., back office server or cloud storage). Uploads may be prioritized based on many different attributes such as time, size, event type priority, and so on. Docking station **400** may also have an integrated locking mechanism for one or more of the uploading/charging ports/cradles **415**. The docking station **400** may be configured to control the locking mechanism to hold or release the wearable device in order to prevent the user from taking it out during uploading/downloading, or to make sure that only the recently "checked out" device is removed, for example.

[0040] The touch screen display **410** of FIG. **4** illustrates one possible graphical user interface (GUI) layout as an example only. Actual layouts may contain more information and features and may be configurable based on requirements of different end users. In FIG. **4**, the GUI shows examples of upload status and battery charging progress. Other screens may be available on the GUI display **410** to provide other status information such as unit ID, user ID, and/or to assist with initiating upload to cloud based storage.

[0041] Having the above understanding of how multi-media files and associated metadata may be collected, we now turn to a discussion of a cloud based storage model for securing and auditing access to recorded information. The cloud based storage model may be beneficial for both small and large law-enforcement agencies as well as other industries.

[0042] Referring now to FIGS. **5**A-B, process flow **500** and its continuation process flow **560** illustrate a possible method for uploading information to cloud based storage for access or distribution to interested third parties. The process flows **500**, **560** may also assist law enforcement personnel with compliance to chain of custody of evidence requirements for legal evidence and other required maintenance functions as explained further below. In this example overall process flow, the recording device may for example be mobile surveillance system **100** or body worn camera **450**, the docking station may be docking station **400** described above, and the back office servers may be the back office servers **642** of FIG. **6** described below. For clarity of reading, these specific examples and their reference numbers will not be repeated throughout the discussion. Also note that docking station **400** is an example embodiment of computer device including a programmable control device (See FIG. **2**) described above while back office servers **642** may be more accurately thought of as computer systems (a superset of computer devices as used herein).

[0043] Beginning at block **505**, video recorded and its associated metadata are identified. This may happen during a patrol shift, or may happen at the end of a patrol shift. For example, as the officer performs his shift duties (e.g., goes on patrol, etc.), a recording device may record and store evidence and surveillance data onto the storage device of the recording device. During the shift, all data recorded on the storage device may be associated with the officer for audit tracking purposes and a metadata file may be used to "tag" or "mark" any recorded data with any number of pertinent attributes such as, officer's ID, event type, date/time, GPS location, etc. This "tagging" may happen automatically or manually as discussed above and shown at block **510**. Next, at block **515** the recording device may connect to a network using one of many different connection types. Different types of connections may be available during a patrol shift (e.g., broadband, satellite link, and so on) or at the end of a patrol shift (e.g., WiFi, Bluetooth, broadband, satellite link, Ethernet, and so on). For simplicity, only a few specific examples are described here, but others would be apparent to those of ordinary skill in the art, given the benefit of this disclosure. At block **520**, based on a) the connection type and b) what other system/device the recording device has established a connection to, different process flow options are shown in FIG. **5**A as a non-exhaustive set of examples. Block **525** represents that the recording device has connected to a back office server. Block **530** represents that the recording device or possibly only its removable storage media has connected to a docking station. Also, as illustrated, it is possible to have a direct connection type from the recording device directly to SAAS and/or cloud storage as illustrated by block **540**. As illustrated in FIG. **5**A, the communication flows between the back office server and SAAS and/or cloud storage (i.e., block **525** and block **540**) may be bidirectional. The communication flow between the back office server and the data offload and staging area (i.e., block **525** and block **535**) may be bidirectional.

The communication flow between docking station and SAAS and/or cloud storage may be bidirectional (i.e., block **530** and block **540**). Each of these bi-directional links may be used to facilitate coordinated decision making regarding what information to upload/download/delete based on a) status of completion of transfer or b) retention criteria information (among other possibilities). Thus, coordinated decision making may take place across the different processing systems utilized to implement the overall methods of this disclosure.

[0044] After a connection is established (as shown at block **525**) between the recording device and one or more back office servers, the functionality of the one or more back office servers may interact with the recording device and either perform data offload and staging functions (block **535**) and/or communicate directly with SAAS functionality and/or cloud storage (block **540**). Of course, the back office servers may perform different offload functions based on the attributes of the multi-media files (e.g., metadata tags). For example, the back office servers may transmit some multi-media files with their associated metadata directly to the cloud storage while offloading others to a local offload storage area. Some multi-media files and their associated metadata files may be both staged locally and sent to the cloud concurrently. Many different options are available. Options discussed here are only to be considered non-limiting examples. Similarly, block **530** indicates a connection has been established with a docking station such as docking station **400**. As explained above, some embodiments of a docking station may include functionality to automatically offload and stage data via the docking station itself and upload to cloud storage (block **540**). Additionally, like the back office servers, a docking station may, in some embodiments, communicate directly with SAAS and/or cloud storage (block **540**). Although not explicitly shown in FIG. **5**A, data offload and staging area may be internal to either or both of a docking station or back office servers and they may each be configured to access the other's internal area either directly or indirectly (e.g., via proxy connection). In any case, multi-media files and their associated data files are processed to determine which multi-media files and data to upload as shown at block **545**. The determination may be unilaterally made by any one of the above mentioned functional units (e.g., recording device, back office server, docking station, and SAAS functionality) or may be made in a coordinated fashion by one or more of the above mentioned functional units working together. As shown at block **550**, after a determination is made, the multi-media files and associate metadata may be uploaded. Additional multi-media files and associated metadata may also be uploaded based on manual selection. Finally, block **555** indicates that recordings, associated data (e.g., metadata), and possibly additional control information is available in cloud storage.

[0045] Continuing on with FIG. **5**B, process flow **560** begins at block **555** when the multi-media recordings and associated information is available in cloud storage. At block **565**, interested third parties may be identified based on criteria associated with one or more of the uploaded multi-media recordings. After identification a method of "delivery" to the identified third party may be determined at block **567**. In this example, "delivery" may be either physical delivery or virtual delivery (e.g., via a network link). Block **569** represents a physical delivery method where a copy of data uploaded to the cloud storage and accessible to the SAAS functionality may be put onto a media, such as Compact Disk (CD) or Digital Versatile Disk (DVD), for physical transfer to the interested third party. As indicated in block **580**, once a physical copy has been extracted from a cloud storage area, the SAAS and other control over the multi-media recordings is "lost." That is, the cloud functionality will no longer have control because the multi-media recordings have been extracted from it. Techniques to prevent and/or control access to the content of the physical media may be implemented through encryption or other types of Digital Rights Management (DRM) capabilities. An alternative to physical delivery and the "loss" of control would be to maintain control of the multi-media files in the cloud and send electronic notification and access information as illustrated in block **571**. Flow would then continue to block **573** where a notification may be prepared containing a link (e.g., hyperlink, URL, URI, etc.) to the appropriate multi-media recording(s) for the identified third party. The link may further be embedded with information to convey to the interested third party information about the multi-media recording and/or its access restrictions. For example, the link may indicate that password security or possibly biometric security may be required to access the content pointed to by the link. The link may further inform the recipient of the type of access they have (e.g., review only, download, delete, etc.) and/or provide an indication of expiration date by which to access the content of the link. At block **575**, the third party may access the cloud based copy of the multi-media while it is still under the control of the cloud based functionality (e.g., SAAS and cloud storage). Block **577** indicates that some users may be permitted to download a copy of the information. As indicated by the flow to **580** for this case, once downloaded, some control capability may be lost as explained above. Block **585** indicates that third parties may be optionally monitored for compliance with subscription criteria enforced by the SAAS or cloud based functionality. For example, a third party may be monitored for access attempts, bandwidth usage, storage usage, or other criteria that may be set out based on a level of subscription they are paying for with regards to the service. Finally, block **590** indicates that while data is maintained on the cloud storage, the SAAS or cloud functionality may continue to enforce and monitor data retention policies, audit controls, and so on.

[0046] Having an understanding of the above discussed data flows **500** and **560**, it will be understood that one example embodiment may include a remote application and database server that may be hosted by a software as a service (SAAS) cloud application to reduce (or eliminate) the need to hire additional computer technicians. Some disclosed embodiments may be implemented in a hybrid cloud and provide local (on site) data storage for portions of data that require high bandwidth across a network (e.g., Internet, police network) while maintaining metadata in the cloud. This configuration may help ensure security and integrity of digital evidentiary data by maintaining a single global copy of metadata in the cloud (for storage) while still allowing fast local access speeds for review of potentially large video/audio files. Also, optionally, data on a shared server may be downloaded to the local data storage site as backup data and then re-uploaded to a remote (or cloud based) site if there is a systems failure or "intrusion" attack at the remote (or cloud based site).

[0047] To eliminate the need for (or to augment) a conventional DVD burner based system, the user may auto upload all data and metadata to the cloud. Optionally, a user may provide (or user event tags may be used as) identification criteria for certain types of videos (and their metadata) to be sent to the cloud automatically as soon as the videos are uploaded to

a server (or staged on docking station **400**) with certain "event type" metadata. For example, an administrator may define: all Driving under the Influence (DUI) videos are sent to cloud based storage and 2 DVD copies are burned. When an officer tags a video as a DUI event type, as soon as the video is uploaded to the cloud, the video may also be sent to a DVD burner for 2 copies automatically. Alternatively, rather than burning DVD copies, an email may be automatically generated and sent or instructions may be provided to an employee to create and send an email. The email may include a time limited access link to personnel or third parties (e.g., prosecuting attorney) that may have an interest in the DUI event. Based on the tag type assigned, a wide number of triggers and follow-on responses may be generated automatically. Furthermore, actions relating to compliance with record retention policies may be automatically generated so that as specific retention periods pass, records are automatically deleted. Thus, the user may readily and easily take advantage of cloud-based storage for an almost limitless cataloguing and archiving device.

[0048] Referring now to FIG. **6**, data flow in a content management system that may utilized the disclosed SAAS functionality and cloud storage is illustrated in block diagram **600**. The SAAS component (including SAAS functions **620**) may be a system which typically includes a web-based portal that is the entry point to the software services for all users requiring data access. As with other data access points, access may be controlled by authentication means such as, but not limited to, passwords, fingerprints, encryption, and so on. Authorized users may access specific content utilizing a "link" as described above in the discussion of FIG. **5**B. In most cases a user will interact with a cloud based copy of the multi-media files they are allowed to access via their supplied link. However, the cloud based system may include enough information to allow secure access back to local storage and backend servers (e.g., **644** and **642**) so that a user at police station **640** may efficiently view locally stored multi-media files. That is, interact with a locally available copy of the cloud based copy pointed to by the link while maintaining audit trail information in the cloud. Alternatively, a user located remotely from police station **640** may obtain access (e.g., secure access via virtual private network (VPN)) to network and storage infrastructure at police station **640** and perform desired actions on multi-media files. That is, if required, a remote user may be redirected from the cloud to an alternative identical copy of a multi-media file while again maintaining audit trail information in the cloud. Of course, bandwidth constraints of the obtained remote access (e.g., VPN) may have an effect on what actions a remote user decides to perform.

[0049] Local hardware/software storage **644** at police station **640** may be any storage device, such as local hard drives, removable drives, network drives, and so on. As shown in FIG. **6**, the SAAS functions **620** may incorporate cloud storage (**630**) which is not typically as limited in storage capacity as local hardware/software storage. However, remote access to large files may have associated communication bandwidth concerns. Such a SAAS content management system may limit data handling (and thus the potential for breaking the evidentiary chain of custody) because copies are not directly controlled by users.

[0050] As disclosed, a cloud-based video export and access system may reduce the hardware and ongoing maintenance costs of optical media based systems by providing users a secure, controlled, reliable and cost-effective method for sending video and data to third parties. Video and data may be uploaded to the cloud for storage, one or more third party recipients may be assigned access rights, and a defined expiration date for third party access may also be provided. Additionally, use of the cloud may permit real-time data upload and storage which provides nearly limitless data storage capacity for mobile surveillance system **100** (FIGS. **1**A and **1**B). Hybrid storage models may be implemented to define pre-requisites as to what actual multi-media files are stored in the cloud. For example, only multi-media files requiring access by third parties are uploaded to the cloud. Another example may be that only multi-media files that have been tagged with a particular event tag (e.g., based on event type) are uploaded to the cloud. In either or both of these examples, other multi-media files that may be less important or have not yet been fully analyzed may be maintained on local storage for future consideration. Note that even though multi-media files may be maintained on local storage, it may be desirable to upload associated metadata to the cloud based system to provide more comprehensive indexing and searching functionality across all recorded data.

[0051] Exported data may be stored in cloud-based storage that is remotely accessible through a secured means (for example, but not limited to, a password, finger print reader, etc). As explained above in the discussion of FIGS. **5**A-B, the system may be configured to send one or more recipients an access link through automated communication methods such as email, text, and Multimedia Messaging Service (MMS), etc. The link sent to each recipient may include an expiration date for accessing the associated data. The system may also allow a recipient of the link to review the data stored in the cloud using a remote access point (e.g., **680**, **682**, **684**) communicatively coupled through a communication channel (e.g., **681**, **683**, **685**). The communication channel may be a VPN or simply some other communication facilitated via the Internet (e.g., encrypted HTTPS). Once a third party (remote user) obtains access to selected files on cloud storage they may also be able to download a local copy of the data for future use, and delete the data after review or download. Downloading of data may of course have negative implications as described above (see FIG. **5**B) regarding "loss" of control of content. The link sent to each recipient may also limit access rights of recipients (e.g. read only, data editing, deletion, etc.) and may actually prevent downloading of data.

[0052] In order to comply with laws, court orders or record-retention policies relating to data access, the system may be configured to remove the accessible data after a predetermined expiration date. A cloud-based system thus allows users to retain the original data while limiting third party access to such data. For example, remote access point **1** (**680**) may allow a first group of users to access content via communication channel **681**. Similarly, remote access point **2** (**682**) may allow additional groups of people to access content via communication channel **683**. Any number of remote user groups and links may be provided for as represented by remote access point N (**684**) and communication channel **685**. Once an access link has expired, no third party may access the expired data. The disclosed SAAS system may also provide bookkeeping functions to track content access, bandwidth usage, and subscription expiration, etc. This bookkeeping function may be capable of statistical analysis, billing, and may generate reports and invoices as needed.

[0053] FIG. **6** also graphically illustrates an example data exchange flow in block diagram **600**, thorough which video, audio, and related data may be shared. Numerous users, computer-based functionalities, storage options, and associated lines of communication may be involved in data uploading and downloading. For example, one or several police vehicles **610** may transmit video and audio data and associated metadata via wireless communication means **605** to a cloud storage system **630**. This wireless communication may occur, for example, while police vehicles **610** are on patrol (e.g., in transit) via a wireless communication path (e.g., satellite, cellular data, or the like). Concurrently with receipt in the cloud (or as needed), this data or a subset of this data may be made accessible to software applications, for example SAAS functions **620**, via communication link **606**. Police vehicle(s) **610** may also manually transfer data and metadata to local storage **644** upon arrival at police station **640** using data transmission channel **660**. Data transmission channel **660** may be a wired connection or a wireless connection. In an alternative, a classical "sneakernet" may be used by connecting a portable recording device to another device (e.g., docking station **400**). After connection, data may be uploaded to local storage **644**, which is located at the police station, and then optionally (based on a number of different criteria, one criterion including event tags) to the cloud **630**.

[0054] In the example of block diagram **600**, a surveillance system vendor **670** oversees and maintains SAAS functions **620** utilizing communication channel **665**. The vendor may also optionally maintain the security and integrity of any cloud based storage system **630** utilizing communication channel **666**. Vendor **670** may also provide all necessary technical support through its software **620** and communication channel **645** to assist police station **640** in implementing best practices in the preservation of data evidence. Police station **640**, depending on available resources, may have "in-house" routers (not shown) and surveillance system backend server(s) **642** which provide redundant data storage systems. Police station **640**, in order to avoid expensive data storage solutions, may optionally utilize cloud storage **630** via communication channel **650**. Cloud storage system **630** may also communicate directly with SAAS functions through communications channel **655**. Having multiple channels of secured communications may provide rapid and efficient data exchange. Use of various storage means, (locally or cloud-based) allows an inexpensive and flexible alternative to resource-limited users.

[0055] In light of the principles and example embodiments described and illustrated herein, it will be recognized that the example embodiments may be modified in arrangement and detail without departing from such principles. Also, the foregoing discussion has focused on particular embodiments, but other configurations are also contemplated. In particular, even though expressions such as "in one embodiment," "in another embodiment," or the like are used herein, these phrases are meant to generally reference embodiment possibilities, and are not intended to limit the invention to particular embodiment configurations. As used herein, these terms may reference the same or different embodiments that are combinable into other embodiments. As a rule, any embodiment referenced herein is freely combinable with any one or more of the other embodiments referenced herein, and any number of features of different embodiments are combinable with one another, unless indicated otherwise.

[0056] Similarly, although example processes have been described with regard to particular operations performed in a particular sequence, numerous modifications might be applied to those processes to derive numerous alternative embodiments of the present invention. For example, alternative embodiments may include processes that use fewer than all of the disclosed operations, processes that use additional operations, and processes in which the individual operations disclosed herein are combined, subdivided, rearranged, or otherwise altered.

[0057] This disclosure may include descriptions of various benefits and advantages that may be provided by various embodiments. One, some, all, or different benefits or advantages may be provided by different embodiments. In view of the wide variety of useful permutations that may be readily derived from the example embodiments described herein, this detailed description is intended to be illustrative only, and should not be taken as limiting the scope of the invention. What is claimed as the invention, therefore, are all implementations that come within the scope of the following claims, and all equivalents to such implementations.

1. A computer system configured to receive and manage multi-media recordings, the computer system comprising:

one or more processors;

one or more network communication interfaces communicatively coupled to the one or more processors; and

a storage area accessible to the one or more processors,

wherein the one or more processors are configured to execute instructions to cause the one or more processors to:

receive, via the one or more network communication interfaces, at least one multi-media file and one or more metadata files containing attributes of the at least one multi-media file, the attributes including at least an event tag;

categorize the at least one multi-media file using the event tag;

provide a set of evidentiary controls for the at least one multi-media file; and

determine where to store the at least one multi-media file, the determination based on one or more of the attributes of the at least one multi-media file.

2. The computer system of claim **21**, wherein the indication including information pertaining to accessing the at least one multi-media file comprises a link for accessing the at least one multi-media file in a secure manner, the link providing an indication of security restrictions associated with the at least one multi-media file.

3. The computer system of claim **21**, wherein the indication including information pertaining to accessing the at least one multi-media file comprises a link for accessing the at least one multi-media file in a secure manner, the link providing an indication of duration of availability of the at least one multi-media file via the link.

4. The computer system of claim **1**, wherein the one or more processors are further configured to execute instructions to cause the one or more processors to:

automatically create a copy of the at least one multi-media file on a physical storage medium for transport to the third party recipient.

5. The computer system of claim **1**, wherein the one or more processors are further configured to execute instructions to cause the one or more processors to:

provide data retention policies regarding access to the at least one multi-media file while taking into consideration the set of evidentiary controls.

6. The computer system of claim **1**, wherein the one or more processors are further configured to execute instructions to cause the one or more processors to:

monitor and/or control access to the at least one multi-media file while taking into consideration the set of evidentiary controls.

7-9. (canceled)

10. The computer system of claim **21**, where the indication of the at least one multi-media file transmitted to the third party recipient includes an indication for a redirect via a secure network to local storage for the at least one multi-media file.

11. The computer system

of claim **1**, wherein the one or more processors are further configured to execute instructions to cause the one or more processors to:

transmit the at least one multi-media file to a particular storage location, the particular storage location determined based on the one or more of the attributes of the at least one multi-media file.

12. The computer system of claim **11**, wherein the particular storage location is a cloud storage location, and the one or more processors are further configured to execute instructions to cause the one or more processors to interface with a software as a service (SAAS) cloud based infrastructure regarding the transmission of the at least one multi-media file to the cloud storage location.

13. The computer system of claim **12**, wherein the particular storage location is a cloud storage location, and the one or more processors are further configured to execute instructions to cause the one or more processors to interface with the SAAS cloud based infrastructure regarding evidentiary controls, data retention policies, and/or audit controls for the at least one multi-media file.

14. (canceled)

15. The computer system of claim **11**,

wherein the one or more processors are further configured to execute instructions to cause the one or more processors to interface with both a software as a service (SAAS) cloud based infrastructure and a docking station to initiate upload of particular metadata files and at least one particular multi-media file from the docking station to a cloud based server, the upload occurring after transmission of the particular metadata files and the at least one particular multi-media file to the docking station and the upload occurring independently of the computer system after initiation thereof,

wherein the particular metadata files may be the same as or different from the one or more metadata files containing attributes of the at least one multi-media file, and the at least one particular multi-media file may be the same as or different from the at least one multi-media file.

16. The computer system of claim **1**, further comprising:

one or more audio capture devices communicatively coupled to the one or more processors; and

one or more video capture devices communicatively coupled to the one or more processors,

wherein the one or more processors are further configured to execute instructions to cause the one or more processors to:

receive information from the one or more audio capture devices and the one or more video capture devices, the information used to create one or more metadata files and at least one multi-media file associated with the one or more metadata files.

17. The computer system of claim **16**, wherein the computer system is configured as a mobile surveillance system.

18. The computer system of claim **17**,

wherein at least one of the one or more network communication interfaces comprises a wireless communication interface, and

wherein transmission of the at least one multi-media file to a particular storage location, the particular storage location determined based on the one or more of the attributes of the at least one multi-media file, is initiated via the wireless communication interface while the mobile surveillance system is in transit.

19. The computer system of claim **18**, wherein the at least one multi-media file is transmitted to the particular storage location at the same time as the one or more processors are receiving information from the one or more audio capture devices and the one or more video capture devices,

20. (canceled)

21. The computer system of claim **1**, wherein the one or more processors are further configured to execute instructions to cause the one or more processors to:

determine a third party recipient of information pertaining to the at least one multi-media file based on the at least one multi-media file categorization; and

initiate transmission of an indication of the at least one multi-media file to the third party recipient, the indication including information pertaining to accessing the at least one multi-media file.

22. The computer system of claim **1**, wherein the determination of where to store the at least one multi-media file, based on the one or more of the attributes of the at least one multi-media file, is made after the at least one multi-media file has been initially recorded.

23. The computer system of claim **1**, wherein the determination of where to store the at least one multi-media file, based on the one or more of the attributes of the at least one multi-media file, is made prior to transmission of the at least one multi-media file to a third party.

24. A computer system configured to receive and manage multi-media recordings, the computer system comprising:

one or more processors;

one or more network communication interfaces communicatively coupled to the one or more processors; and

a storage area accessible to the one or more processors,

wherein the one or more processors are configured to execute instructions to cause the one or more processors to:

receive, via the one or more network communication interfaces, at least one multi-media file and one or more metadata files containing attributes of the at least one multi-media file, the attributes including at least an event tag;

categorize the at least one multi-media file using the event tag;

provide a set of evidentiary controls for the at least one multi-media file; and

store in local storage the at least one multi-media file and store in cloud storage the one or more metadata files containing attributes of the at least one multi-media file.

25. A computer system configured to receive and manage multi-media recordings, the computer system comprising:

one or more processors;

one or more network communication interfaces communicatively coupled to the one or more processors; and

a storage area accessible to the one or more processors,

wherein the one or more processors are configured to execute instructions to cause the one or more processors to:

receive, via the one or more network communication interfaces, at least one multi-media file and one or more metadata files containing attributes of the at least one multi-media file, the attributes including at least an event tag;

categorize the at least one multi-media file using the event tag;

provide a set of evidentiary controls for the at least one multi-media file; and

transmit the at least one multi-media file to storage according to an ordering, the ordering based on a priority assigned to the at least one multi-media file,

wherein the at least one multi-media file comprises a plurality of multi-media files, each of the plurality of multi-media files being assigned a different priority, the different priorities based on attributes of respective ones of the plurality of multi-media files.

* * * * *