

EXHIBIT 1

You've Got Mail:
The promise of cyber communication in prisons and need for regulation

Patents and Patent Applications

PRISON
POLICY INITIATIVE



US009117171B2

(12) **United States Patent**
Torgersrud et al.

(10) **Patent No.:** **US 9,117,171 B2**
(45) **Date of Patent:** **Aug. 25, 2015**

(54) **DETERMINING A THREAT LEVEL FOR ONE OR MORE INDIVIDUALS**

(71) Applicant: **Telmate, LLC**, San Francisco, CA (US)

(72) Inventors: **Richard Torgersrud**, San Francisco, CA (US); **Christopher Ditto**, San Jose, CA (US)

(73) Assignee: **INTELMATE LLC**, San Francisco, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 247 days.

(21) Appl. No.: **13/831,431**

(22) Filed: **Mar. 14, 2013**

(65) **Prior Publication Data**

US 2014/0279767 A1 Sep. 18, 2014

(51) **Int. Cl.**
G06F 1/00 (2006.01)
G06N 5/00 (2006.01)
G06N 5/02 (2006.01)

(52) **U.S. Cl.**
CPC **G06N 5/02** (2013.01)

(58) **Field of Classification Search**
CPC G06N 5/02; G06N 7/005; G06N 3/02; G06N 5/025

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2005/0171816 A1* 8/2005 Meinert et al. 705/3
2010/0299292 A1* 11/2010 Collazo 706/14
2013/0298244 A1* 11/2013 Kumar et al. 726/25

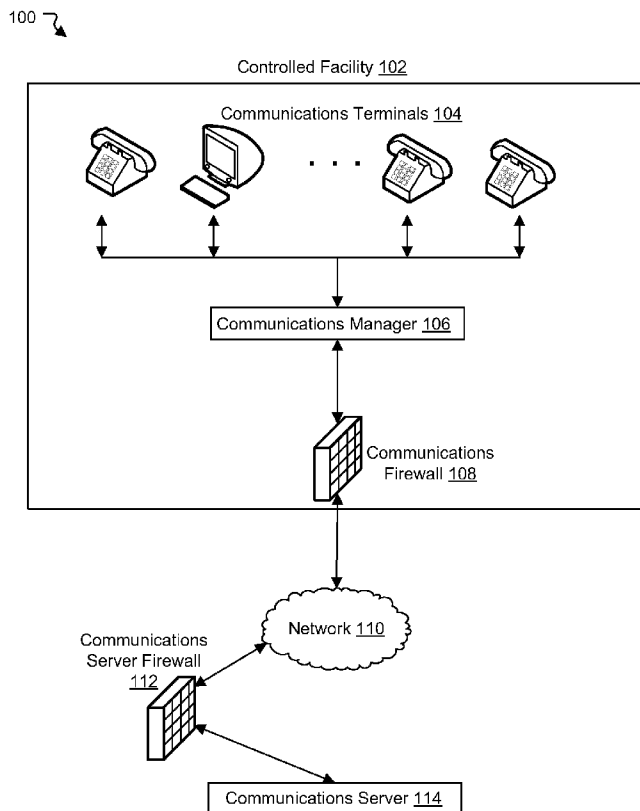
* cited by examiner

Primary Examiner — Jeffrey A Gaffin
Assistant Examiner — Kalpana Bharadwaj
(74) *Attorney, Agent, or Firm* — McDermott Will & Emery LLP

(57) **ABSTRACT**

A system and computer-implemented method for determining a threat level for one or more individuals includes accessing a data structure to obtain aggregated data stored therein, wherein the aggregated data comprises at least one of communication history data or transaction history data for one or more individuals. One or more predetermined metrics are applied to the obtained aggregated data, to determine threat level information for the one or more individuals. The determined threat level information is provided for display.

20 Claims, 5 Drawing Sheets



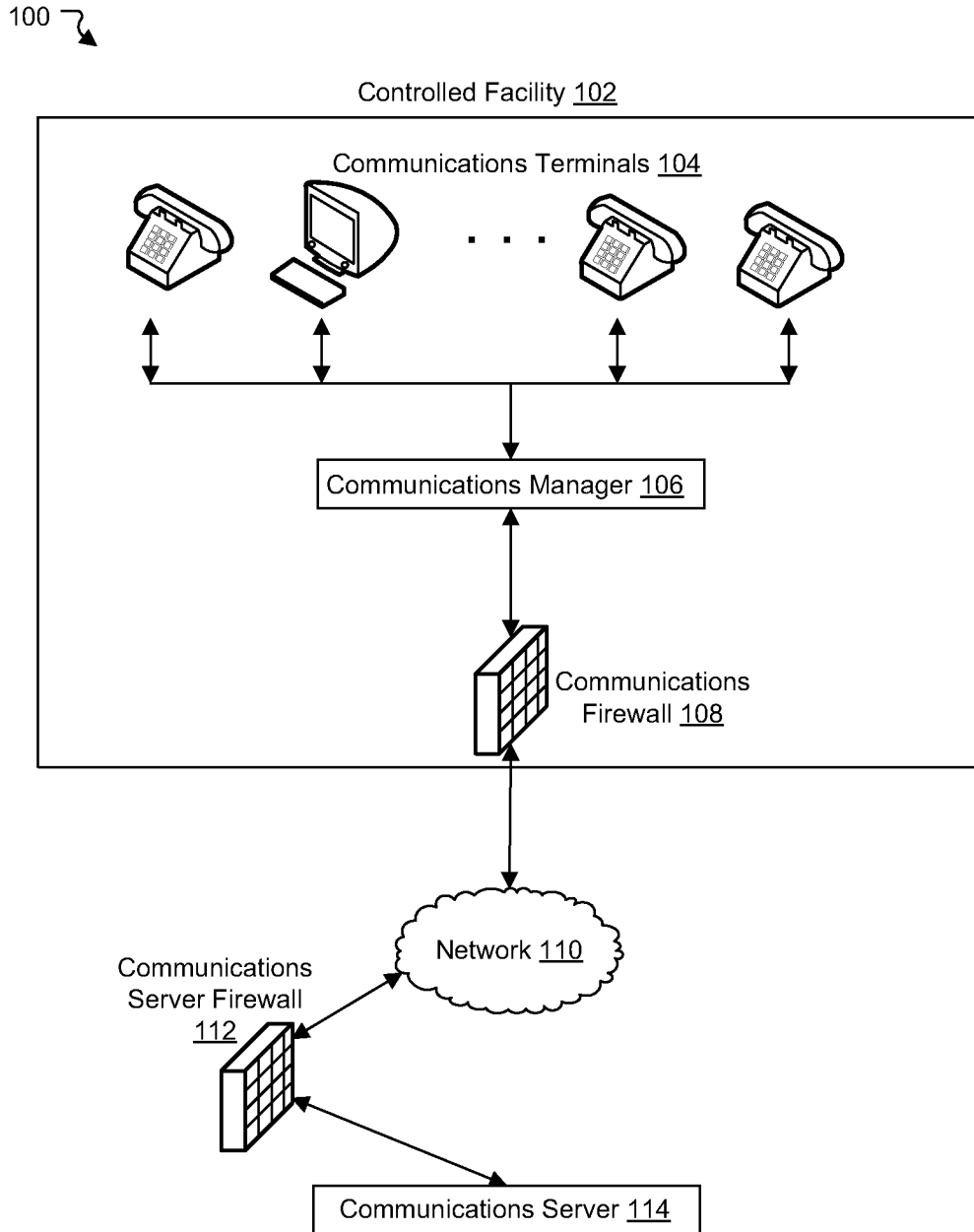


FIG. 1

200 ↘

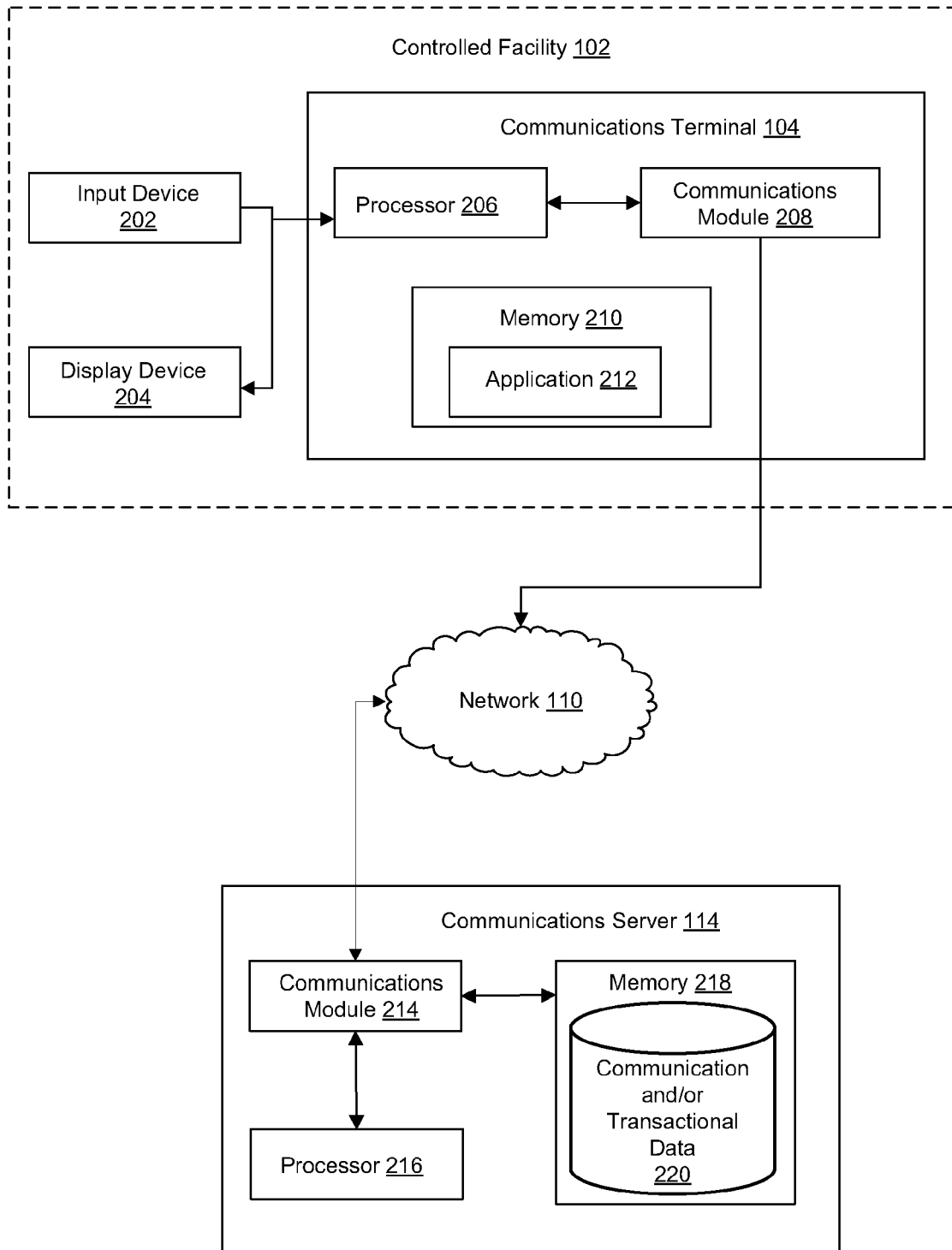
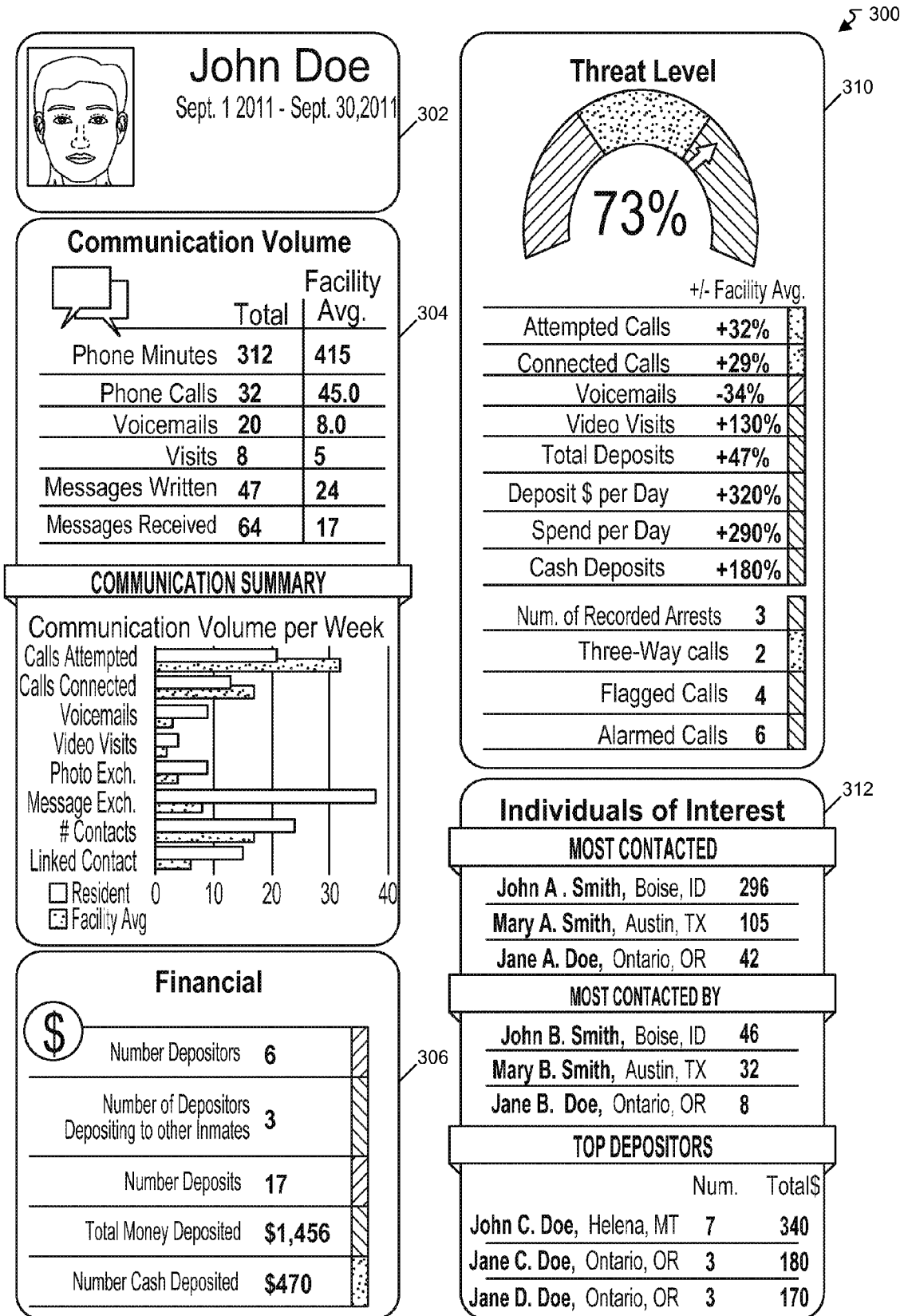


FIG. 2

FIG. 3



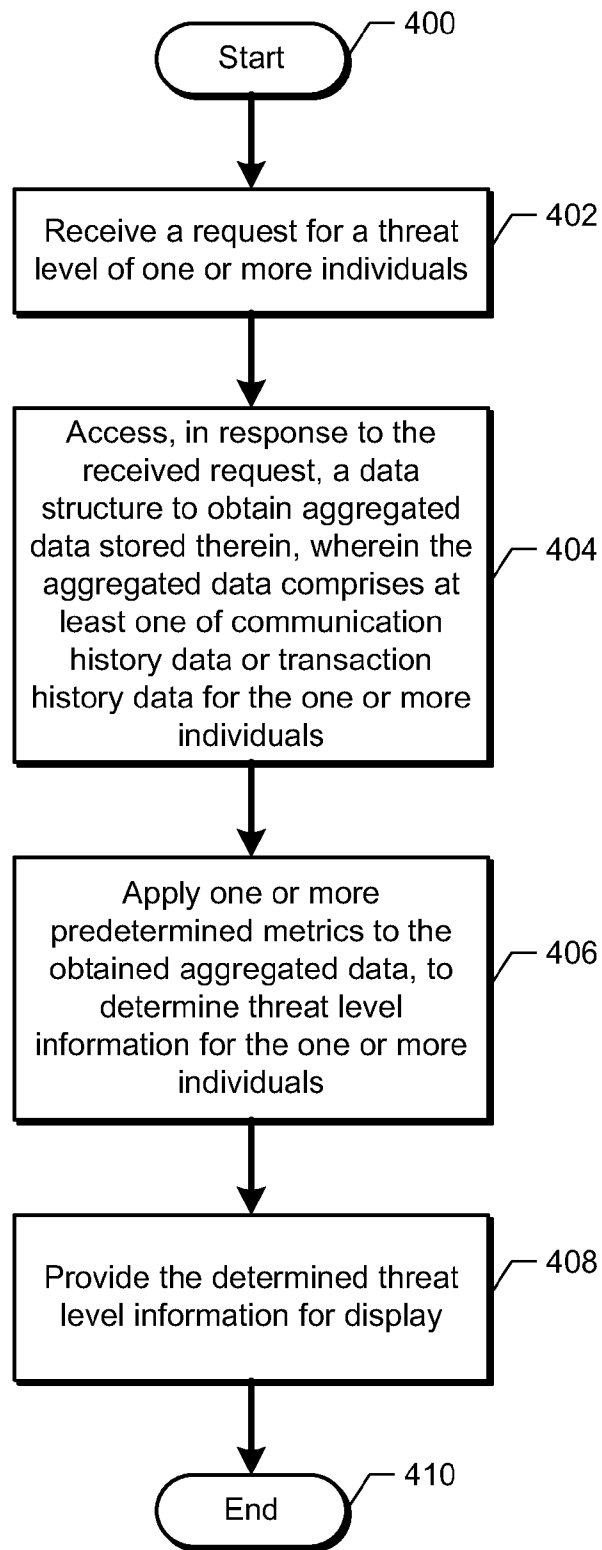


FIG. 4

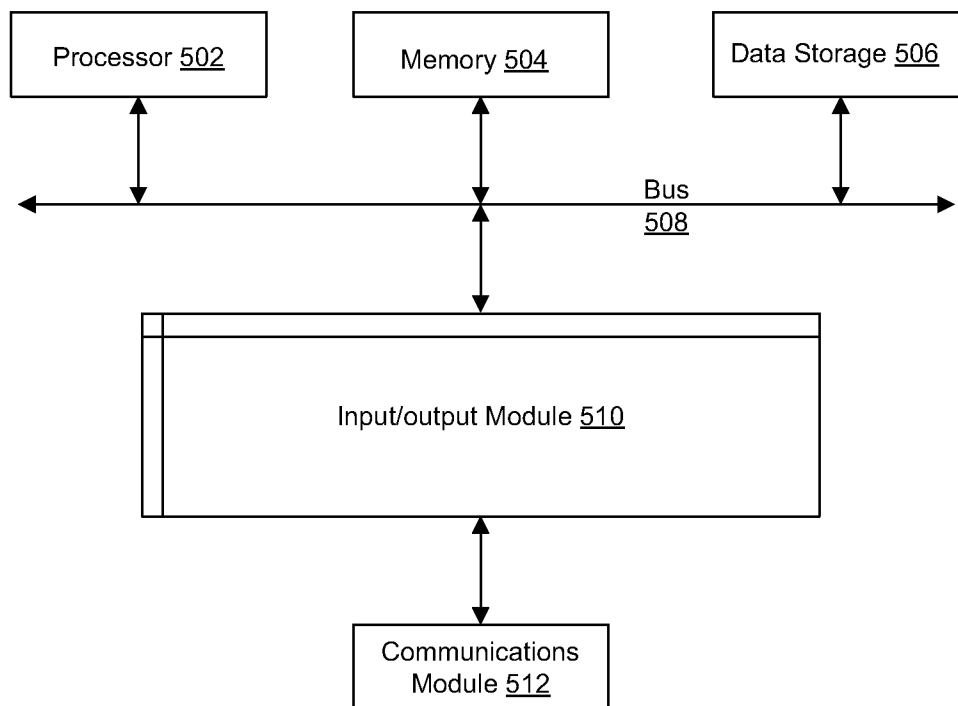


FIG. 5

1

DETERMINING A THREAT LEVEL FOR ONE OR MORE INDIVIDUALS

FIELD

The present disclosure generally relates to computer systems, and more particularly to the use of a computer system to determine a threat level for one or more individuals.

DESCRIPTION OF THE RELATED ART

Certain types of people can be placed in situations that require them to determine a detainee's threat to the public, threat to correctional staff, threat to other detainees or to themselves, and likelihood to commit crimes after release. Such types of people include, but are not limited to, law enforcement officials, judges who determine bail and sentencing, prosecuting attorneys who decide whether to prosecute or the details of a plea agreement and correctional officers who determine where to house detainees, and parole board members.

These people rely on a small pool of available data when determining a detainee's threat, often relying on reports of violent behaviors recorded by correctional staff while the detainee is in custody, and the nature of the crime or crimes the detainee is accused or convicted of.

SUMMARY

According to one embodiment of the present disclosure, a computer-implemented method for determining a threat level for one or more individuals is provided. The method comprises accessing a data structure to obtain aggregated data stored therein, wherein the aggregated data comprises at least one of communication history data or transaction history data for one or more individuals. The method further comprises applying one or more predetermined metrics to the obtained aggregated data, to determine threat level information for the one or more individuals, and providing the determined threat level information for display.

According to another embodiment of the present disclosure, a system for determining a threat level for one or more individuals is provided. The system comprises one or more processors, and a machine-readable medium comprising instructions stored therein, which when executed by the processors, cause the processors to perform operations comprising accessing a data structure to obtain aggregated data stored therein, wherein the aggregated data comprises at least one of communication history data or transaction history data for one or more individuals, applying one or more predetermined metrics to the obtained aggregated data, to determine threat level information for the one or more individuals, and providing the determined threat level information for display.

According to a further embodiment of the present disclosure, machine-readable medium is provided. The machine-readable medium comprises instructions stored therein, which when executed by a system, cause the system to perform operations comprising accessing a data structure to obtain aggregated data stored therein, wherein the aggregated data comprises at least one of communication history data or transaction history data for one or more individuals. The operations further comprise applying one or more predetermined metrics to the obtained aggregated data, to determine threat level information for the one or more individuals, and providing the determined threat level information for display.

It is understood that other configurations of the subject technology will become readily apparent to those skilled in

2

the art from the following detailed description, wherein various configurations of the subject technology are shown and described by way of illustration. As will be realized, the subject technology is capable of other and different configurations and its several details are capable of modification in various other respects, all without departing from the scope of the subject technology. Accordingly, the drawings and detailed description are to be regarded as illustrative in nature and not as restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are included to provide further understanding and are incorporated in and constitute a part of this specification, illustrate disclosed embodiments and together with the description serve to explain the principles of the disclosed embodiments. In the drawings:

FIG. 1 illustrates an example architecture for determining a threat level for one or more individuals.

FIG. 2 is a block diagram illustrating the example communications terminal and communications server from the architecture of FIG. 1 according to certain aspects of the disclosure.

FIG. 3 illustrates an example of a user interface displaying threat level information for an individual.

FIG. 4 illustrates an example process in which a threat level for one or more individuals is determined.

FIG. 5 is a block diagram illustrating an example computer system with which the example communications terminal and communications server of FIG. 2 can be implemented.

DETAILED DESCRIPTION

In the following detailed description, numerous specific details are set forth to provide a full understanding of the present disclosure. It will be apparent, however, to one ordinarily skilled in the art that the embodiments of the present disclosure may be practiced without some of these specific details. In other instances, well-known structures and techniques have not been shown in detail so as not to obscure the disclosure.

As noted above, certain types of people (e.g., law enforcement officials, judges who determine bail and sentencing, prosecuting attorneys, and parole board members) are placed in situations that require them to determine a detainee's threat to the public, threat to correctional staff, threat to other detainees, and likelihood to commit crimes after release. These individuals rely on a small pool of available data when determining a detainee's threat, often relying on reports of violent behaviors recorded by correctional staff while the detainee is in custody, and the nature of the crime or crimes the detainee is accused or convicted of.

However, other data with statistical relevance is overlooked because it is difficult to access and difficult to interpret, and often officials simply may not realize that inferences regarding behavior and threats can be made from data that, on the surface, may appear unrelated.

The subject technology analyzes the communication and transactional history of an individual (e.g., a detainee), providing additional metrics for determining the individual's threat level. Using this information, officials can be alerted to patterns or trends that correlate with actual threatening behavior of individuals who exhibited similar communication patterns.

More particularly, the subject technology provides for determining a threat level for one or more individuals. A data structure is accessed to obtain aggregated data stored therein,

wherein the aggregated data comprises at least one of communication history data or transaction history data for one or more individuals. One or more predetermined metrics are applied to the obtained aggregated data, to determine threat level information for the one or more individuals. The determined threat level information is provided for display.

As used herein, the “threat level” is an individual’s likelihood of threatening activity. This activity can include, but is not limited to, harming others, harming themselves (e.g., risk of suicide or self-harm), or recidivism. In example aspects, threat level can also indicate a likelihood of depression for an individual.

While many examples are provided herein in the context of a correction facility, the principles of the present disclosure contemplate other types of controlled facilities as well. For example, businesses and governmental entities (e.g., administrative or military) are all considered within the scope of the present disclosure.

Furthermore, although many examples provided herein describe an individual’s communication or transaction history information being stored in memory, permission may be granted for each individual to have such information stored. In the context of a detention environment, permission may be granted by the detainee agreeing to be present in the detention environment, or by another entity with appropriate legal authorization to grant permission to track the such information in the detention environment. Each detainee can be provided notice that such information will be stored. The stored individual information may be encrypted to protect individual security.

FIG. 1 illustrates an example architecture for determining a threat level for one or more individuals. The architecture 100 illustrates a controlled facility 102 (e.g., a detention environment) that includes communications terminals 104 connected to a network 110 through a communications firewall 108 using a communications manager 106. The architecture 100 further includes a communications server 114 as described herein connected to the network 110 through a communications server firewall 112. The firewalls 108 and 112 can be software-based or hardware-based.

Each of the communications terminals 104 is connected to a communications manager 106. In certain aspects, for purposes of load balancing, the communications terminals 104 can be connected to many communications managers. The communications terminals 104 can be audio communication terminals, video communication terminals, tactile communications terminals (e.g., for the visual and/or hearing impaired), or other terminals configured for communication between two individuals. In certain aspects, the communication terminals can be mobile, such as mobile smartphones or mobile kiosks.

Alternatively, or in addition, the communications terminals can be kiosks for depositing funds (hereinafter “deposit kiosks”). For example, deposit kiosks can be located in an inmate intake area of a detention center (e.g., controlled facility 102), for a newly-booked detainee/inmate to post bail, or for a family member or friend to post bail or otherwise deposit funds for a detainee.

The communications manager 106 to which the communications terminals 104 are connected can be, for example, a networking device such as a router, gateway, or switch. The communications manager 106 can be configured for various protocols of communication including, for example, Internet Protocol (IP), voice over IP (VoIP), audio and video Internet telephony network protocols, or telephone switching.

The communications manager 106 is connected to the network 110, such as the Internet, a metropolitan area network

(MAN), a wide area network (WAN), a broadband network (BBN), and the like. Further, the network 110 can include, but is not limited to, any one or more of the following network topologies, including a bus network, a star network, a ring network, a mesh network, a star-bus network, tree or hierarchical network, and the like. In certain aspects where the communications server 114 is located at the controlled facility 102, the network 110 can include, for example, any one or more of a personal area network (PAN), a local area network (LAN), or a campus area network (CAN). The connection between the communications manager 106 and the network 110 can be protected using a communications firewall 108, which can be particularly relevant to protecting the security of the controlled facility 102 by limiting access to devices in the controlled facility 102 to authorized individuals or processes.

The communications server 114 is connected to the network 110 through the communications server firewall 112. In example aspects, the communications server 114 is responsible for storing communication data and/or transaction from the communications terminals 104 for individuals in the controlled facility 102, and for creating aggregated communication history data and/or transaction history data. The communications server 114 can be any device having an appropriate processor, memory, and communications capability for hosting the terminal-based resident location information.

In certain aspects, the communications server 114 can receive a request for a threat level of one or more individuals. The threat level can be requested automatically (e.g., periodic requests) or manually for an individual (e.g., detainee). In response to the received request, communications server 114 accesses aggregated data (e.g., from a data structure) comprising at least one of communication history data or transaction history data for the one or more individuals. Communications server 114 applies one or more predetermined metrics (e.g., algorithms) to the obtained aggregated data, to determine threat level information for the one or more individuals. Communications server 114 provides the determined threat level information for display. Thus, with reference to correctional facility 102, communications server 114 can analyze detainee communication statistical data to estimate the threat that the detainee poses to other detainees, facility staff, and the public.

As described in greater detail below with reference to FIG. 2, application of the predetermined metrics may correspond to analyzing one or more of the following over a given time period: call volume data, voicemail data, deposit data, visitation data, exchange of messages, photos and video and arrest data. Based on this data, and other available communication data, the subject technology can create a threat estimate, for example, in the same way that the financial industry creates a credit score. By assigning weight to information derived from the above list, the subject technology can provide an estimate of the threat that an individual poses. In example aspects, this threat level can be balanced with traditional information (e.g., detainee behavior when arrested and while in custody, body language, and human interpretation of criminal charges) in order to estimate a threat level.

FIG. 2 is a block diagram 200 illustrating an example communications terminal 104 and communications server 114 in the architecture 100 of FIG. 1 according to certain aspects of the disclosure. The communications terminal 104 and communications server 114 are connected over the network 110 via respective communications modules 208 and 214. The communications modules 208 and 214 are configured to interface with the network 110 to send and receive information, such as data, requests, responses, and com-

mands to other devices on the network **110**. The communications modules **208** and **214** can be, for example, modems or Ethernet cards.

The communications terminal **104**, which can be, but is not limited to, a telephone, videophone, camera, or deposit kiosk, includes a processor **206** (or connected downstream to a processor, e.g., at communications server **114**), the communications module **208**, and a memory **210** that includes an application **212**. Although the communications terminal **104** is illustrated as including the processor **206** for example only, it is understood that in certain aspects where, for example, the communications terminal **104** is a telephone, the processor **206** is not included in the communications terminal. In example aspects, the application is configured to report communications and/or transactions for the communications terminal **104**. As discussed below, such reporting can log the time/duration of the communication, and the identity of the participating individuals (e.g., the detainee and the other participating party). The communications terminal **104** also includes (or is coupled to) an input device **202** and an output device **204**, such as a display. The input device **202** can include, for example, a keyboard, a touchpad, a microphone, a camera, touchscreen, or mouse.

The processor **206** of the communications terminal **104** is configured to execute instructions, such as instructions physically coded into the processor **206**, instructions received from software (e.g., application **212**) in memory **210**, or a combination of both, to provide individual communication and/or transaction reports, for aggregation by communications server **114**.

Communications server **114** receives the communication and/or transaction reports (e.g., using communications module **214**), and can store received multiple communication and/or transaction reports on a per-detainee basis. In the example of FIG. **2**, the aggregated data is stored in memory **218**, and more particularly, in communication and/or transactional database **220**.

Furthermore, communications server **114**, using processor **216**, can receive a request for a threat level of one or more individuals. The threat level can be requested automatically (e.g., periodic requests) or manually for an individual (e.g., detainee). In response to the received request, communications server **114** accesses the aggregated data (e.g., from communication and/or transactional database **220**) comprising at least one of communication history data or transaction history data for the one or more individuals. Communications server **114** applies one or more predetermined metrics (e.g., algorithms) to the obtained aggregated data, to determine threat level information for the one or more individuals. Communications server **114** provides the determined threat level information for display.

Although the disclosed block diagram **200** illustrates the communication and/or transactional database **220** as being stored in the memory **218** of the communications server **114**, the communication and/or transactional database **220** can be stored in the memory **210** of the communications terminal **104**, or the communications server **114** can be located in the controlled facility **102**. For example, the communication and/or transactional database **220** can be provided by the communications server **114** to one or many communications terminals **104**, for example, as a form of data replication.

Thus, the subject technology can be implemented as a process that may be scheduled to run regularly on some or all individuals, or it may be triggered to run for an individual, or group of individuals. The process may be run for a specific time range (e.g., one week or one month period), for individuals current period of detention, or for all available deten-

tion periods for a specific individual (for example, multiple jail stints that could be in multiple facilities).

As noted above, communications server may apply one or more predetermined metrics for user data obtained from communication and/or transactional database **220**. For each individual over a given time period, the software may analyze one or more fields, including but not limited to, calls, voicemails, visits, other communications, deposits, detainee spend information, detainee system details or other information.

For calls, the following information may be aggregated within communication and/or transactional database **220** and analyzed via processor **216** using predetermined metrics: a total number of attempted calls; a total number of connected calls; an average length of connected calls; a total minutes of connected calls; a number of three-way calls (which may be prohibited in correctional facilities); a percent of calls found to be three-way calls; a number of flagged calls (e.g., calls are manually flagged to indicate interest on the part of an investigator); a percent of calls that are flagged; a number of alarmed calls (e.g., calls are automatically flagged as alarms when conditions set by an investigator occur; such as person A calling person B); a percent of alarmed calls; and a total number of unique persons communicated with over the phone.

With reference to voicemails, the following information may be aggregated within communication and/or transactional database **220** and analyzed via processor **216** using predetermined metrics: a total number of voicemails received; an average length of voicemails received; and total minutes for received voicemails.

For visits, the following information may be aggregated within communication and/or transactional database **220** and analyzed via processor **216** using predetermined metrics: a total number of onsite phone visits conducted; an average length of onsite phone visits conducted; total minutes of onsite phone visits conducted; a total number of onsite video visits conducted; an average length of onsite video visits conducted; total minutes of onsite video visits conducted; total onsite video visits canceled or no show; a total number of Internet video visits conducted; an average length of Internet video visits conducted; total minutes of Internet video visits conducted; total Internet video visits canceled or no show; and total number of unique persons visited with.

For other communications, the following information may be aggregated within communication and/or transactional database **220** and analyzed via processor **216** using predetermined metrics: a total number of photos sent; a total number of photos received; a total number of videos sent; a total number of videos received; a total number of text based messages sent; a total number of text based messages received; and a total number of unique persons communicated with via text, video or photos.

With reference to deposits, the following information may be aggregated within communication and/or transactional database **220** and analyzed via processor **216** using predetermined metrics: total number of kiosk deposits, an average amount of kiosk deposits; a total dollar amount of kiosk deposits; a percent of all deposits made with cash; a percent of overall cash deposits made with large denomination bills; a total number of cash deposits with large denomination bills; a total dollar amount of cash deposits with large denomination bills; an average size of cash deposits with large denomination bills; a total number of over-the-phone deposits; an average amount of over-the-phone deposits; a total dollar amount of over-the-phone deposits; a total number of unique persons depositing funds.

Regarding detainee spend information, the following information may be aggregated within communication and/or transactional database **220** and analyzed via processor **216** using predetermined metrics: total spent on communication; and total spent on entertainment. In addition, for detainee system details, the following information may be aggregated within communication and/or transactional database **220** and analyzed via processor **216** using predetermined metrics: a number of known arrests; a cumulative time spent detained; a number of correctional facilities that the individual is known to have been housed in; and an alleged or convicted crime (e.g., whether it is categorized as violent).

In example aspects, other information that may be aggregated within communication and/or transactional database **220** and analyzed via processor **216** using predetermined metrics include: an average number of individuals connected to persons called by the individual (e.g., if each person called by a individual has connected with numerous other individuals, then this number would be high and possibly suspicious); a number of persons in contact with the individuals who are also in contact with known violent individuals (e.g., do the friends have other friends known to be violent); a total number of known violent incidents in the individuals past.

In addition to the above fields of data and type of information that can be aggregated, it is also possible for communications server **114** to analyze the content of one or more individual communications using predetermined metrics. For example, text versions of communications (e.g., emails or other text-based messages, audio or image data converted to text) can be analyzed for keywords that indicate, or that do not indicate, a likelihood of threatening activity by one or more individuals.

With further reference to the predetermined metrics, in order to create a useable threat index, data can be aggregated from various sources, the data can be calculated into numbers that can be analyzed, weights can be applied to the numbers, and a summary of the results that includes a threat index can be generated. In example aspects, the algorithm that is used to determine the threat index may change over time as variables are compared to those of individuals that are known to be violent (e.g., based on actual behavior).

This algorithm may be determined manually, or aspects of it may be determined by automated statistical analysis to determine the strength of individual variables in contributing to violent behavior. For example, if a weak correlation is made between number of voicemails and violent behavior and a strong correlation is made between a high number of large denomination cash deposits (e.g., \$50 and \$100 bills) and violence, then the algorithm will be adjusted to give more weight to the later variable in computing the threat index.

Also, because the statistical relevance of data may vary based on identifiable factors regarding the individual. The algorithm may vary between individuals based on factors such as, but not limited to: age; gender; geography; charged or convicted crime; and length of time detained. For example, communication patterns of 18-year-old females who have been in jail for less than two weeks may be different from those of 50-year-old males who have been in prison for over 20 years. As a result, algorithms have the potential to vary between individuals.

In example aspects, the subject technology requires access to communications data and a display mechanism, such as a Web browser or printer, to display the information. Display of the threat level information will be described in greater detail below with reference to FIG. 3.

It should be noted that a statistically significant amount of time or data may be required for the algorithm to perform

well. For example, the algorithm may work for a individual who is in custody for a short period of time, but who generates enough data (e.g., call attempts, deposits, visits, etc.) to analyze. In another example, the algorithm may work for a person who is in custody for a reasonable period of time, perhaps over a week, and makes little or no attempt to communicate and receives few or no deposits (e.g., lack of contact over time can be statistically relevant). However, in example aspects, for someone who is in custody for a few days or less and makes little or no attempt to communicate and receives few or no deposits, the algorithm may not be as effective.

Thus, the subject technology analyzes available data, populates variables with aggregate data, assigns weight to variables (e.g., with extra significance to variables that are more statistically relevant to determining likelihood of threatening behavior), and calculates a score or other visual representation.

Today, estimates of a detainee's likelihood to commit violent behavior are based on human interpretation of past violent incidences, criminal charges or convictions, and less tangible elements like a detainee's attitude towards correctional officers. This base information is a very narrow slice of available data.

The subject technology supplements already available information with detailed analysis of data that is either unavailable or difficult to acquire or understand. The subject technology is also able to give weight to statistically significant variables that may not make intuitive sense to a person. When humans make decisions, they can give far more weight to factors that they fully comprehend. For example, a muscular detainee with gang tattoos is more likely to attract the attention of detention staff than a skinny detainee who is constantly trying to make phone calls but rarely succeeding in connecting with someone. With the subject technology, if it is determined statistically that detainees that make three to five unsuccessful phone call attempts for every phone call that is answered by a human are more likely to be a threat to others, that can be factored into the threat index without anyone first needing to know why.

One major advantage is that the subject technology is capable of providing law enforcement officials with a list of detainees that have a higher probability of causing problems in the future. Even if detainees identified by a high threat index are only 10% more likely than a randomly selected group of detainees to engage in threatening behavior, the identification of those detainees is still useful to law enforcement officials.

A facility that spreads limited resources (such as the attention of guards) evenly is more likely to have problems than a facility that is able to apply more attention to individuals who have a higher likelihood of posing a threat. A comparison may be drawn to police departments that use crime statistics and census statistics to determine areas that warrant higher numbers of officer patrols.

FIG. 3 illustrates an example of a user interface displaying threat level information for an individual. In the example of FIG. 3, user interface **300** includes a name portion **302**, a communication history portion **304**, a transaction history portion **306**, a threat level analysis portion **310** and a individuals of interest portion **312**.

User interface **300** corresponds to a visual representation of threat level analysis, and is created and displayed for the requesting party. The display of the user interface **300** can be in the form of an email, an onscreen display, a printed page, or a file (e.g., PDF) that is available for download.

As shown with reference to threat level analysis portion **310**, the threat index is displayed in the form of a visual image

indicating a level of threat. In the example of FIG. 3, threat level analysis portion 310 displays the threat level in the form of a dial. In alternative aspects, the visual image may be in the form of a thermometer, traffic light, or color (e.g., on a scale). Alternatively, or in addition, the threat index score may be represented by a number, a percentage (e.g., a percentage of likelihood that the individual will act violently), or a category, such as “Likely Violent,” or “Possibly Violent” or “Unlikely Violent.”

In the example of FIG. 3, user interface 300 displays the threat index data for a single detainee. However, in alternative example aspects, user interface 300 can display the threat index data for numerous detainees at once (e.g., in a logical order, such as listing the highest threat first in the list).

User interface 300 can display communication volume (e.g., phone minutes, phone calls, etc.) and a communication summary (e.g., calls attempted, calls connected) within communication history portion 304. In addition, financial history portion 306 can display a history of transactions for an individual, for example, a number of depositors, a number of depositors depositing to other detainees, a number of deposits, etc.

User interface 300 may show additional information in an individuals of interest portion 312. Individuals of interest portion 312 may display which individuals were contacted by the detainee the most, which individuals attempted to contact the detainee the most, and which individuals deposited the most funds, and made the most frequent deposits for the detainee.

By virtue of the foregoing, a facility staff member can use the information provided by user interface 300 to identify potentially threatening individuals in their correctional facility who might not otherwise have come to their attention. An individual who has not exhibited violent or unusual behavioral patterns and who was arrested for a non-violent crime, for example, probably would not come to the attention of corrections staff.

However, using the subject technology, corrections staff could run a threat index report, or receive a threat index alert, or view individuals with a high threat index value from within an administration system for a correctional facility. If a individual is found with a high threat index, but without exhibiting other threatening behavior, corrections staff could interview the individual, move the individual, or simply give the individual more attention. Thus, law enforcement officials can be given information that they may not normally have to defend against, prevent, or otherwise address before a threatening incident takes place.

In example aspects, the threat index by itself may not lead to direct action, such as separating a individual from others. The subject technology can alert officials to an individual or group of individuals based on patterns or trends that correlate with actual threatening behavior of individuals who exhibited similar communication patterns.

Likewise, the subject technology can be used to provide facility staff with additional information to indicate that a detainee is less likely to be a threat. A individual who calls his/her family regularly and who receives regular deposits of money from a small number of people may be considered a lower threat than a individual who does not connect regularly with outsiders or who receives money from a large number of people.

FIG. 4 illustrates an example process in which a threat level for one or more individuals is determined. Following start block 400, a request for a threat level of one or more individuals is received at step 402. The threat level can indicate, for each of the one or more individuals, a level of likelihood

that the individual will exhibit violent or recidivistic behavior (e.g., to others or to themselves). The request can be an automatically-generated request, such as an automatic request for a threat level of all detainees scheduled for transport on a given day. Alternatively, or in addition, the request can be manually-generated by a user requester. The one or more individuals can be detainees within a correctional facility.

At step 404, in response to the received request, a data structure is accessed to obtain aggregated data stored therein. The aggregated data includes at least one of communication history data or transaction history data for the one or more individuals.

Each of the communication history data and the transaction history data can include statistical data. The statistical data for the communication history data can correspond to at least one of telephone calls, voicemails, onsite phone visits, onsite video visits, photo messages, video messages, text messages. The statistical data for the transaction history data can correspond to deposits, or spending for communication or entertainment.

At step 406, one or more predetermined metrics are applied to the obtained aggregated data, to determine threat level information for the one or more individuals. The one or more predetermined metrics can apply respective weights to the statistical data for the communication history data or the transaction history data, to determine the threat level information for the one or more individuals.

At step 408, the determined threat level information is provided for display. In example aspects, subsequent to determining the threat level information, indication of actual threat data performed by one of the one or more individuals can be received. In response to the received indication, the one or more predetermined metrics can be updated based on the aggregated data for the one individual, for future determination of threat level information.

In example aspects, it is not necessary to receive a request at step 402, and the process can proceed directly to step 404 from start block 400. By skipping step 402, it is possible for the process to calculate threat levels for multiple inmates (e.g., all inmates), for example, to report the inmates with the highest threat levels.

In a case where the one or more individuals are detainees, the threat level can further be determined based on a number of known arrests or a cumulative time spent detained for the individual. The process then ends at end block 410.

FIG. 5 is a block diagram illustrating an example computer system with which the example communications terminal and communications server of FIG. 2 can be implemented. In certain aspects, the computer system 500 may be implemented using hardware or a combination of software and hardware, either in a dedicated server, or integrated into another entity, or distributed across multiple entities.

Computer system 500 (e.g., communications terminal 104 and communications server 114) includes a bus 508 or other communication mechanism for communicating information, and a processor 502 (e.g., processor 206, 222, and 242) coupled with bus 508 for processing information. By way of example, the computer system 500 may be implemented with one or more processors 502. Processor 502 may be a general-purpose microprocessor, a microcontroller, a Digital Signal Processor (DSP), an Application Specific Integrated Circuit (ASIC), a Field Programmable Gate Array (FPGA), a Programmable Logic Device (PLD), a controller, a state machine, gated logic, discrete hardware components, or any other suitable entity that can perform calculations or other manipulations of information.

Computer system **500** can include, in addition to hardware, code that creates an execution environment for the computer program in question, e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, or a combination of one or more of them stored in an included memory **504** (e.g., memory **210**, **226**, and **246**), such as a Random Access Memory (RAM), a flash memory, a Read Only Memory (ROM), a Programmable Read-Only Memory (PROM), an Erasable PROM (EPROM), registers, a hard disk, a removable disk, a CD-ROM, a DVD, or any other suitable storage device, coupled to bus **508** for storing information and instructions to be executed by processor **502**. The processor **502** and the memory **504** can be supplemented by, or incorporated in, special purpose logic circuitry.

The instructions may be stored in the memory **504** and implemented in one or more computer program products, i.e., one or more modules of computer program instructions encoded on a computer readable medium for execution by, or to control the operation of, the computer system **500**, and according to any method well known to those of skill in the art, including, but not limited to, computer languages such as data-oriented languages (e.g., SQL, dBase), system languages (e.g., C, Objective-C, C++, Assembly), architectural languages (e.g., Java, .NET), and application languages (e.g., PHP, Ruby, Perl, Python). Instructions may also be implemented in computer languages such as array languages, aspect-oriented languages, assembly languages, authoring languages, command line interface languages, compiled languages, concurrent languages, curly-bracket languages, data-flow languages, data-structured languages, declarative languages, esoteric languages, extension languages, fourth-generation languages, functional languages, interactive mode languages, interpreted languages, iterative languages, list-based languages, little languages, logic-based languages, machine languages, macro languages, metaprogramming languages, multiparadigm languages, numerical analysis, non-English-based languages, object-oriented class-based languages, object-oriented prototype-based languages, off-side rule languages, procedural languages, reflective languages, rule-based languages, scripting languages, stack-based languages, synchronous languages, syntax handling languages, visual languages, wirth languages, embeddable languages, and xml-based languages. Memory **504** may also be used for storing temporary variable or other intermediate information during execution of instructions to be executed by processor **502**.

A computer program as discussed herein does not necessarily correspond to a file in a file system. A program can be stored in a portion of a file that holds other programs or data (e.g., one or more scripts stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (e.g., files that store one or more modules, subprograms, or portions of code). A computer program can be deployed to be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network. The processes and logic flows described in this specification can be performed by one or more programmable processors executing one or more computer programs to perform functions by operating on input data and generating output.

Computer system **500** further includes a data storage device **506** such as a magnetic disk or optical disk, coupled to bus **508** for storing information and instructions. Computer system **500** may be coupled via input/output module **510** to various devices. The input/output module **510** can be any

input/output module. Example input/output modules **510** include data ports such as USB ports. The input/output module **510** is configured to connect to a communications module **512**. Example communications modules **512** (e.g., communications modules **208** and **214**) include networking interface cards, such as Ethernet cards and modems. In certain aspects, the input/output module **510** is configured to connect to a plurality of devices, such as an input device (e.g., input device **202**) and/or an output device **516** (e.g., display device **204**). Example input devices **514** include a keyboard and a pointing device, e.g., a mouse or a trackball, by which a user can provide input to the computer system **500**. Other kinds of input devices **514** can be used to provide for interaction with a user as well, such as a tactile input device, visual input device, audio input device, or brain-computer interface device. For example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, tactile, or brain wave input. Example output devices include display devices, such as a LED (light emitting diode), CRT (cathode ray tube), or LCD (liquid crystal display) screen, for displaying information to the user.

According to one aspect of the present disclosure, the communications terminal **104** and communications server **114** can be implemented using a computer system **500** in response to processor **502** executing one or more sequences of one or more instructions contained in memory **504**. Such instructions may be read into memory **504** from another machine-readable medium, such as data storage device **506**. Execution of the sequences of instructions contained in main memory **504** causes processor **502** to perform the process steps described herein. One or more processors in a multi-processing arrangement may also be employed to execute the sequences of instructions contained in memory **504**. In alternative aspects, hard-wired circuitry may be used in place of or in combination with software instructions to implement various aspects of the present disclosure. Thus, aspects of the present disclosure are not limited to any specific combination of hardware circuitry and software.

Various aspects of the subject matter described in this specification can be implemented in a computing system that includes a back end component, e.g., as a data server, or that includes a middleware component, e.g., an application server, or that includes a front end component, e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the subject matter described in this specification, or any combination of one or more such back end, middleware, or front end components. The components of the system can be interconnected by any form or medium of digital data communication, e.g., a communication network. The communication network (e.g., network **110**) can include, for example, any one or more of a PAN, LAN, CAN, MAN, WAN, BBN, the Internet, and the like. Further, the communication network can include, but is not limited to, for example, any one or more of the following network topologies, including a bus network, a star network, a ring network, a mesh network, a star-bus network, tree or hierarchical network, or the like. The communications modules can be, for example, modems or Ethernet cards.

Computer system **500** can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other. Computer system **500** can be, for example, and without limitation, a desktop com-

puter, laptop computer, or tablet computer. Computer system 500 can also be embedded in another device, for example, and without limitation, a mobile telephone, a personal digital assistant (PDA), a mobile audio player, a Global Positioning System (GPS) receiver, a video game console, and/or a television set top box.

The term “machine-readable storage medium” or “computer readable medium” as used herein refers to any medium or media that participates in providing instructions or data to processor 502 for execution. Such a medium may take many forms, including, but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media include, for example, optical disks, magnetic disks, or flash memory, such as data storage device 506. Volatile media include dynamic memory, such as memory 504. Transmission media include coaxial cables, copper wire, and fiber optics, including the wires that comprise bus 508. Common forms of machine-readable media include, for example, floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, DVD, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, an EPROM, a FLASH EPROM, any other memory chip or cartridge, or any other medium from which a computer can read. The machine-readable storage medium can be a machine-readable storage device, a machine-readable storage substrate, a memory device, a composition of matter effecting a machine-readable propagated signal, or a combination of one or more of them.

As used herein, the phrase “at least one of” preceding a series of items, with the terms “and” or “or” to separate any of the items, modifies the list as a whole, rather than each member of the list (i.e., each item). The phrase “at least one of” does not require selection of at least one item; rather, the phrase allows a meaning that includes at least one of any one of the items, and/or at least one of any combination of the items, and/or at least one of each of the items. By way of example, the phrases “at least one of A, B, and C” or “at least one of A, B, or C” each refer to only A, only B, or only C; any combination of A, B, and C; and/or at least one of each of A, B, and C.

Furthermore, to the extent that the term “include,” “have,” or the like is used in the description, including the claims, such term is intended to be inclusive in a manner similar to the term “comprise” as “comprise” is interpreted when employed as a transitional word in a claim.

A reference to an element in the singular is not intended to mean “one and only one” unless specifically stated, but rather “one or more.” The term “some” refers to one or more. All structural and functional equivalents to the elements of the various configurations described throughout this disclosure that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and intended to be encompassed by the subject technology. Moreover, nothing disclosed herein is intended to be dedicated to the public regardless of whether such disclosure is explicitly recited in the above description.

While this specification contains many specifics, these should not be construed as limitations on the scope of what may be claimed, but rather as descriptions of particular implementations of the subject matter. Certain features that are described in this specification in the context of separate embodiments can also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment can also be implemented in multiple embodiments separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even

initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a subcombination or variation of a subcombination.

Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system components in the aspects described above should not be understood as requiring such separation in all aspects, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

The subject matter of this specification has been described in terms of particular aspects, but other aspects can be implemented and are within the scope of the following claims. For example, the actions recited in the claims can be performed in a different order and still achieve desirable results. As one example, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. In certain implementations, multitasking and parallel processing may be advantageous. Other variations are within the scope of the following claims.

These and other implementations are within the scope of the following claims.

What is claimed is:

1. A computer-implemented method for determining a threat level for one or more individuals, the method comprising:

accessing a data structure to obtain aggregated data stored therein, wherein the aggregated data comprises at least one of communication history data or transaction history data for one or more individuals;

applying one or more predetermined metrics to the obtained aggregated data, to determine threat level information for the one or more individuals, wherein at least one of the one or more predetermined metrics is weighted so that the threat level information is indicative, for each of the one or more individuals, of a level of likelihood that the individual will exhibit violent or recidivistic behavior; and

providing the determined threat level information for display.

2. The method of claim 1, wherein each of the communication history data and the transaction history data comprise statistical data.

3. The method of claim 2, wherein the statistical data for the communication history data corresponds to at least one of telephone calls, voicemails, onsite phone visits, onsite video visits, photo messages, video messages, text messages.

4. The method of claim 2, wherein the statistical data for the transaction history data corresponds to deposits, or spending for communication or entertainment.

5. The method of claim 2, wherein the one or more predetermined metrics apply respective weights to the statistical data for the communication history data or the transaction history data, to determine the threat level information for the one or more individuals.

6. The method of claim 1, further comprising: receiving, subsequent to determining the threat level information, indication of actual threat data performed by one of the one or more individuals; and

15

updating, in response to the received indication, the one or more predetermined metrics based on the aggregated data for the one individual, for future determination of threat level information.

7. The method of claim 1, wherein the accessing is performed in response to a received request for the threat level of the one or more individuals.

8. The method of claim 7, wherein the request is one of an automatically generated request or a request manually generated by a user.

9. The method of claim 1, wherein the one or more individuals are detainees within a correctional facility.

10. The method of claim 9, wherein for each of the one or more individuals, the threat level is further determined based on a number of known arrests or a cumulative time spent detained for the individual.

11. A system for determining a threat level for one or more individuals, the system comprising:

one or more processors; and

a machine-readable medium comprising instructions stored therein, which when executed by the processors, cause the processors to perform operations comprising: accessing a data structure to obtain aggregated data stored therein, wherein the aggregated data comprises at least one of communication history data or transaction history data for one or more individuals;

applying one or more predetermined metrics to the obtained aggregated data, to determine threat level information for the one or more individuals, wherein at least one of the one or more predetermined metrics is weighted so that the threat level information is indicative, for each of the one or more individuals, of a level of likelihood that the individual will exhibit violent or recidivistic behavior; and

providing the determined threat level information for display.

12. The system of claim 11, wherein each of the communication history data and the transaction history data comprise statistical data.

13. The system of claim 12, wherein the statistical data for the communication history data corresponds to at least one of telephone calls, voicemails, onsite phone visits, onsite video visits, photo messages, video messages, text messages.

16

14. The system of claim 12, wherein the statistical data for the transaction history data corresponds to deposits, or spending for communication or entertainment.

15. The system of claim 12, wherein the one or more predetermined metrics apply respective weights to the statistical data for the communication history data or the transaction history data, to determine the threat level information for the one or more individuals.

16. The system of claim 11, the operations further comprising:

receiving indication of at least one threatening action performed by one of the one or more individuals; and updating, in response to the received indication, the one or more predetermined metrics based on the aggregated data for the one individual, for subsequent determination of threat levels.

17. The system of claim 11, wherein the accessing is performed in response to a received request for the threat level of the one or more individuals.

18. A non-transitory, machine-readable medium comprising instructions stored therein, which when executed by a system, cause the system to perform operations comprising: accessing a data structure to obtain aggregated data stored therein, wherein the aggregated data comprises at least one of communication history data or transaction history data for one or more individuals;

applying one or more predetermined metrics to the obtained aggregated data, to determine threat level information for the one or more individuals, wherein at least one of the one or more predetermined metrics is weighted so that the threat level information is indicative, for each of the one or more individuals, of a level of likelihood that the individual will exhibit violent or recidivistic behavior; and

providing the determined threat level information for display.

19. The non-transitory, machine-readable medium of claim 18, wherein each of the communication history data and the transaction history data comprise statistical data.

20. The non-transitory, machine-readable medium of claim 19, wherein the statistical data for the communication history data corresponds to at least one of telephone calls, voicemails, onsite phone visits, onsite video visits, photo messages, video messages, text messages.

* * * * *



US007742582B2

(12) **United States Patent**
Harper

(10) **Patent No.:** **US 7,742,582 B2**
(45) **Date of Patent:** **Jun. 22, 2010**

(54) **OFFENDER MESSAGE DELIVERY SYSTEM**

(75) Inventor: **Terry D. Harper**, La Quinta, CA (US)

(73) Assignee: **Core Systems (ND) Limited**, Belfast (IE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1052 days.

(21) Appl. No.: **11/357,869**

(22) Filed: **Feb. 16, 2006**

(65) **Prior Publication Data**

US 2006/0184544 A1 Aug. 17, 2006

Related U.S. Application Data

(60) Provisional application No. 60/654,546, filed on Feb. 17, 2005.

(51) **Int. Cl.**

H04M 11/00 (2006.01)

H04M 1/64 (2006.01)

G06Q 20/00 (2006.01)

G06F 17/00 (2006.01)

G06F 15/16 (2006.01)

(52) **U.S. Cl.** **379/100.08**; 379/88.19;
705/64; 705/408; 705/406; 709/206

(58) **Field of Classification Search** 379/88.19,
379/100.08, 199; 705/64, 408, 406; 709/206
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,665,380 B1 * 12/2003 Cree et al. 379/88.25

6,668,045 B1 12/2003 Mow
7,502,451 B2 * 3/2009 Gyllenskog et al. 379/100.08
2006/0245559 A1 * 11/2006 Hodge et al. 379/88.19

OTHER PUBLICATIONS

Regional Advisory Council Meeting "National Law Enforcement and Corrections Technology Center," Rocky Mountain Region, Denver, CO, Jul. 20 & 21, 2006, 5 pages.

Advanced Technologies Group (ATG) "Offender Management Suite," www.a-t-g.com, Dec. 6, 2006, 2 pages.

Inmatesmail "InmatesMail with Inmate Locators," www.inmatesmail.com, published prior to 2005, 2 pages.

Patti Micciche, "Colorado Department of Corrections Launches Inmate Locator On-line System," Dec. 5, 2005, 1 page.

(Continued)

Primary Examiner—Curtis Kuntz

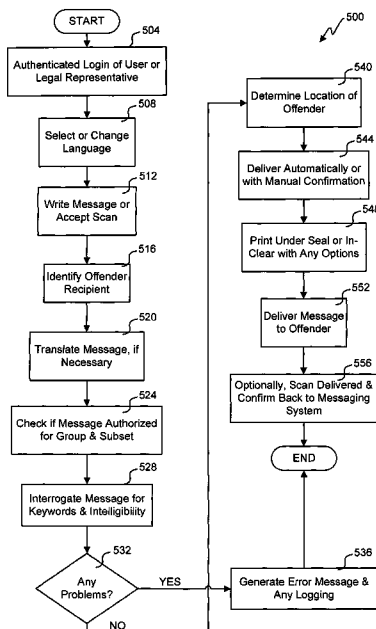
Assistant Examiner—Mohammad K Islam

(74) *Attorney, Agent, or Firm*—Townsend and Townsend and Crew LLP

(57) **ABSTRACT**

A correctional facility communication system for sending an external message to an offender of a correctional facility is disclosed. The correctional facility communication system includes a messaging system and a correctional facility system coupled together with a wide area network. The messaging system is at a first location and the correctional facility system is at a second location, different from the first location. The messaging system authenticates a sender of the external message, receives the external message in electronic form at the first location, checks the external message against criteria specified by the correctional facility, determine a second location of the offender and a corresponding printer, and sends the external message to the second location for automatic printing with the corresponding printer.

27 Claims, 6 Drawing Sheets



OTHER PUBLICATIONS

Dave Mintie, "Washington DOC Monitors Offenders with Biometrics," www/biometricwatch.com, Mar. 12, 2005, 4 pages.

Judy Nichols, "Prisoner monitor gets a test," www/azcentral.com, Dec. 25, 2005, 2 pages.

Author Unknown, "2005 NASCIO Nomination Digital Government: Government to Citizen Arkansas Department of Correction Inmate Banking," 4 pages.

John S. Pistole, "Congressional Testimony, Terrorist Recruitment in Prisons and The Recent Arrests Related to Guantanamo Bay Detainees," Oct. 14, 2003, 2 pages.

2006 JPay, Inc., "jpay, The Easy Way to Send Money to an Inmate," www/jpay.com, 1 page.

CBS News, "Gangs Thrive in Maximum Security," www/cbsnews.com, May 15, 2005, 6 pages.

Allen Trovillion, "Maintaining Family Contact," www/fplao.org/MaintainingFamilyContoct.html, Nov. 1998, 69 pages.

CBS News, "New PC Fingerprint Passwords," www/cbsnews.com, Sep. 9, 2004, 2 pages.

Reason Public Policy Institute, "Competitive Corrections Research Project," The Reasons Foundation, www/rppi.org, 2004, 5 pages.

JUSTNET, "Contraband Detection in Inmate Mail," www/nlectc.org, 2 pages.

2006 About, Inc., "Families of Prisoners," www/crime.about.com, 2 pages.

Advanced Technologies Group, Inc., "Offender Management Suite," www/a-t-g.com, 2 pages.

ARKANSAS.GOV, "A Service of the Information Network of Arkansas," 1997-2006 Information Network of Arkansas, www.arkansas.gov, 1 page.

* cited by examiner

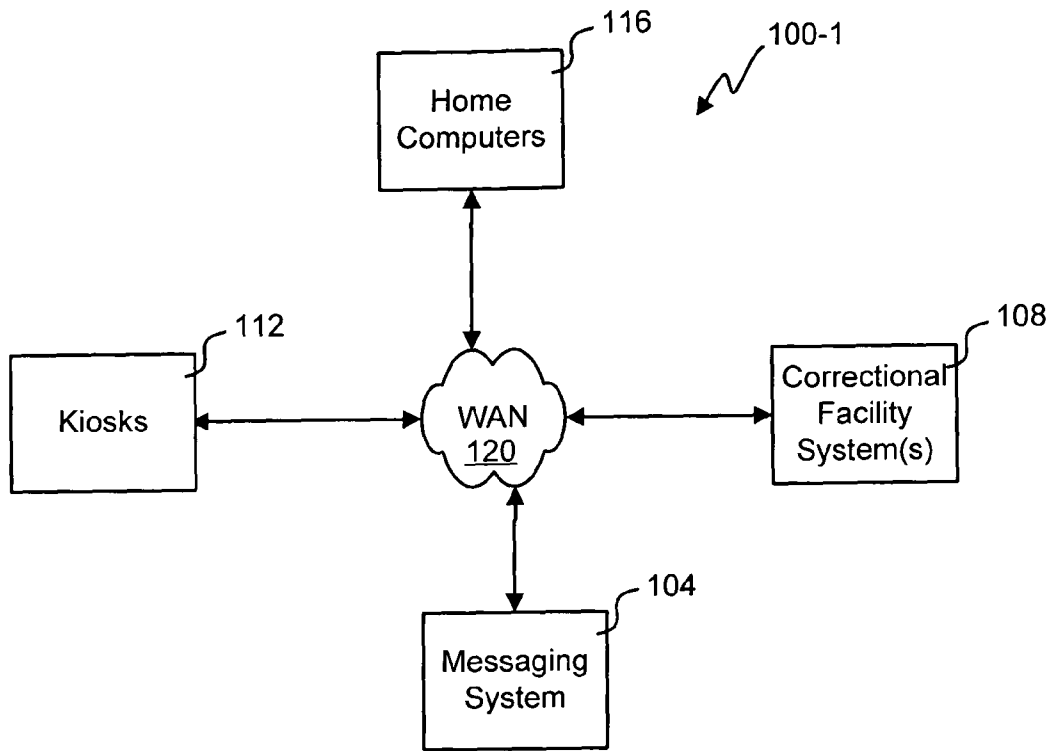


Fig. 1A

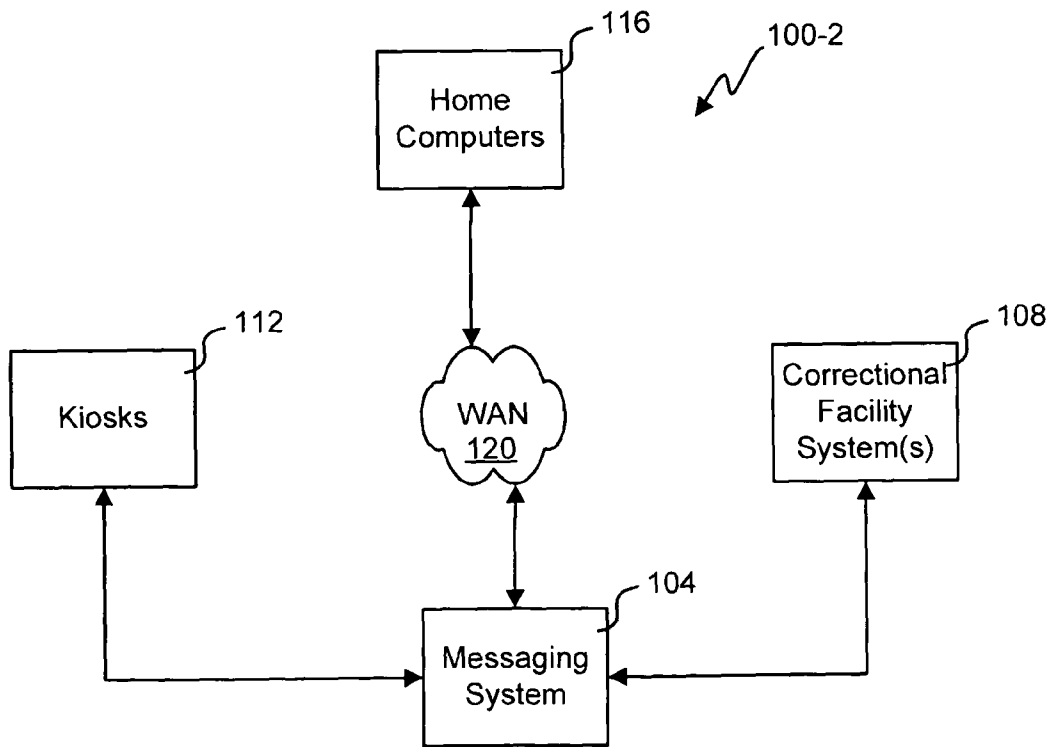


Fig. 1B

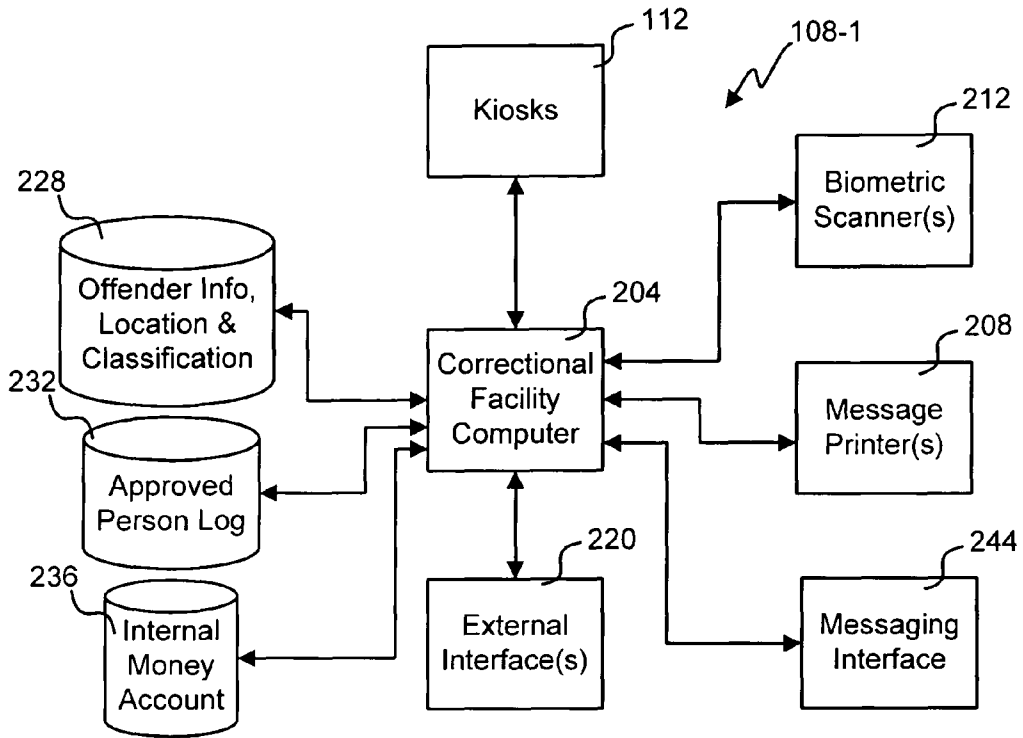


Fig. 2A

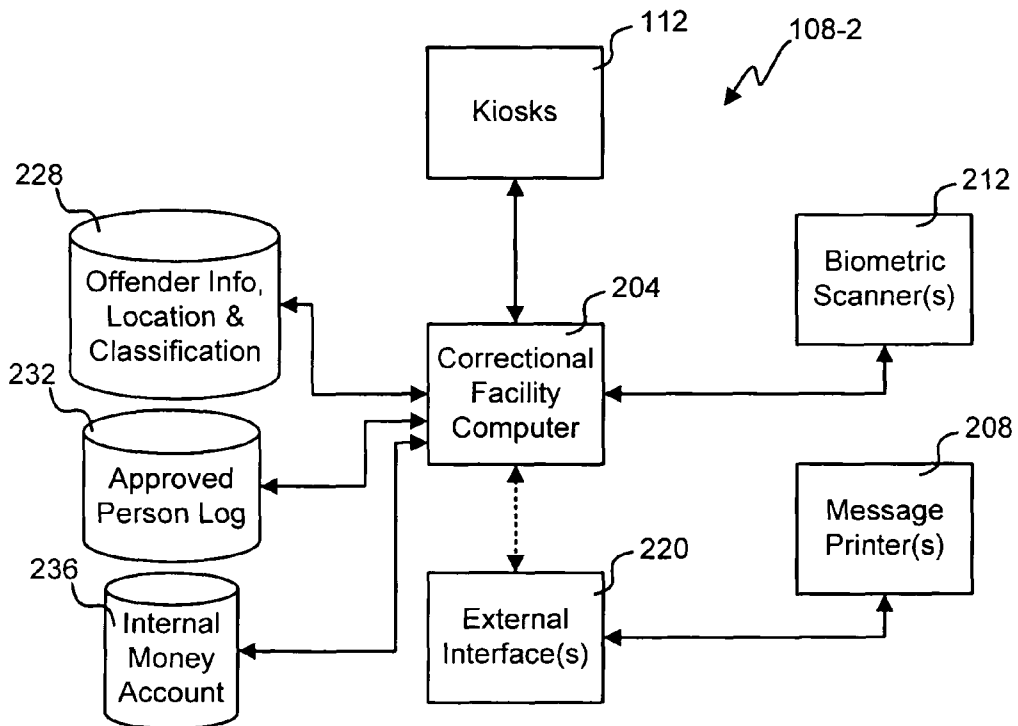


Fig. 2B

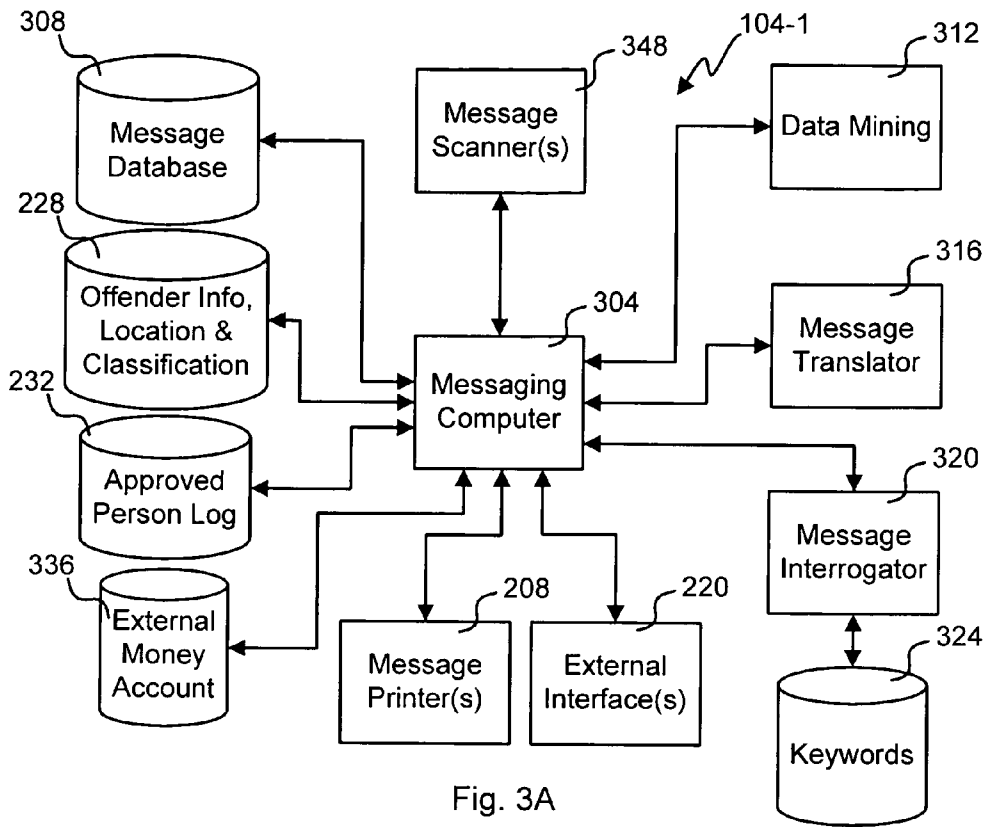


Fig. 3A

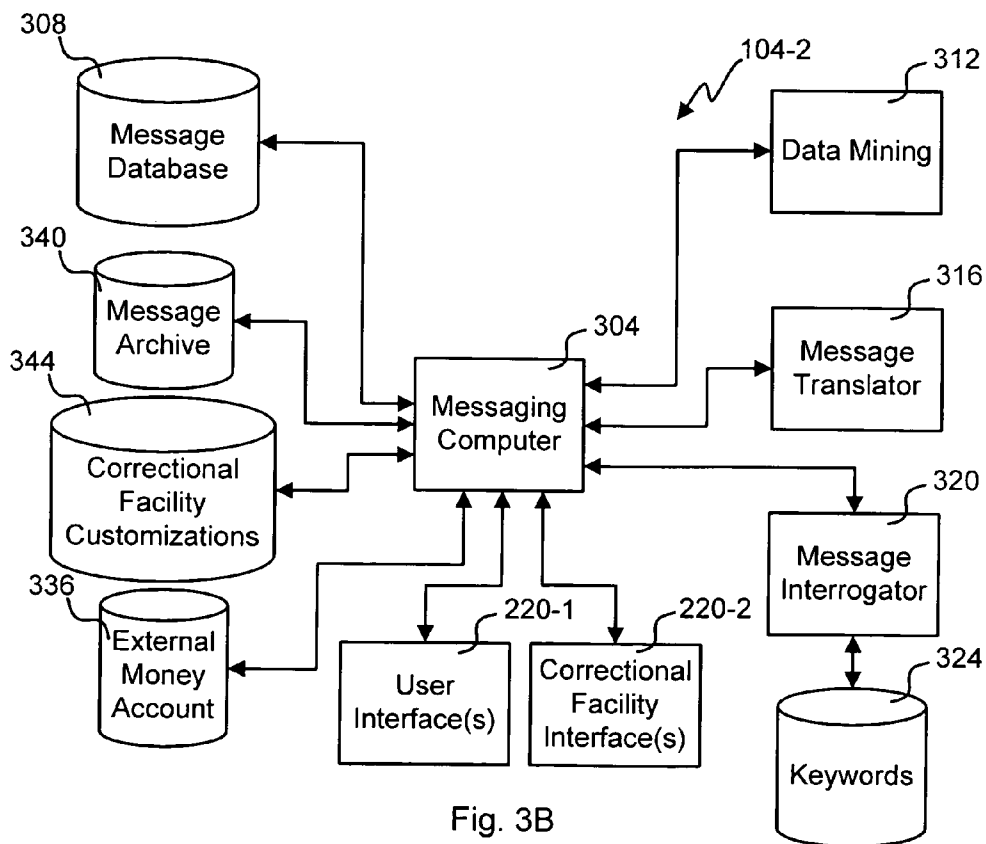


Fig. 3B

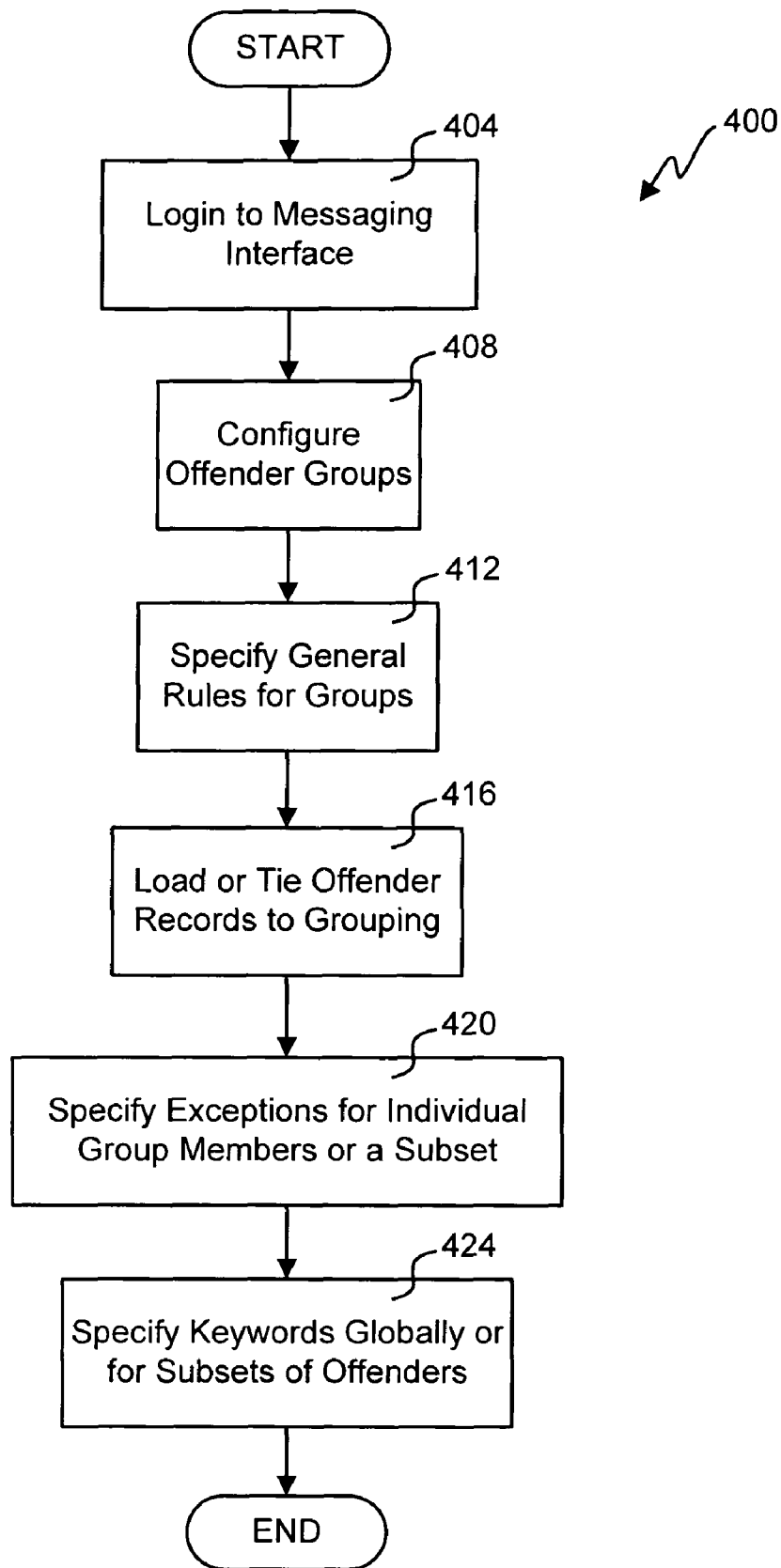


Fig. 4

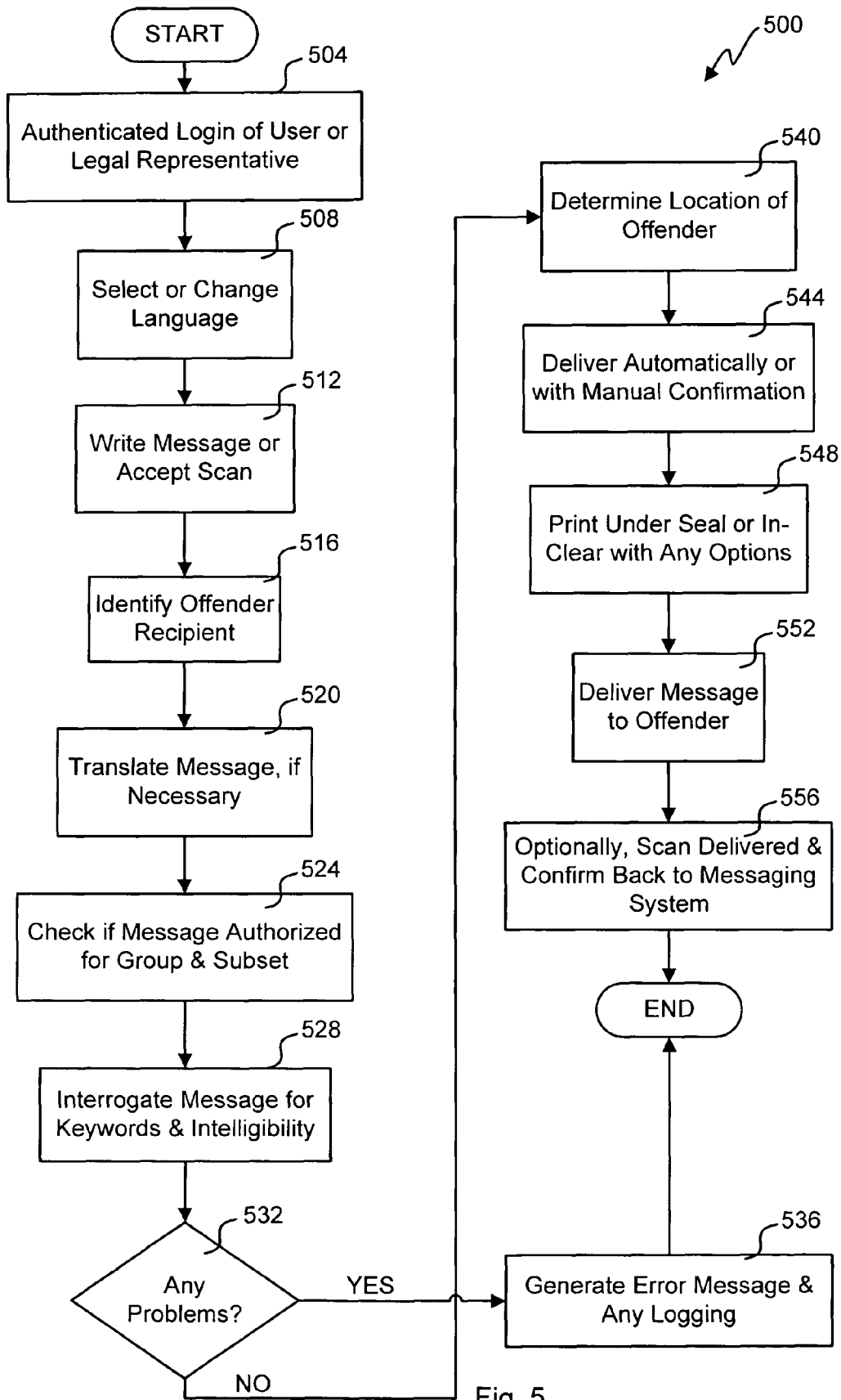


Fig. 5

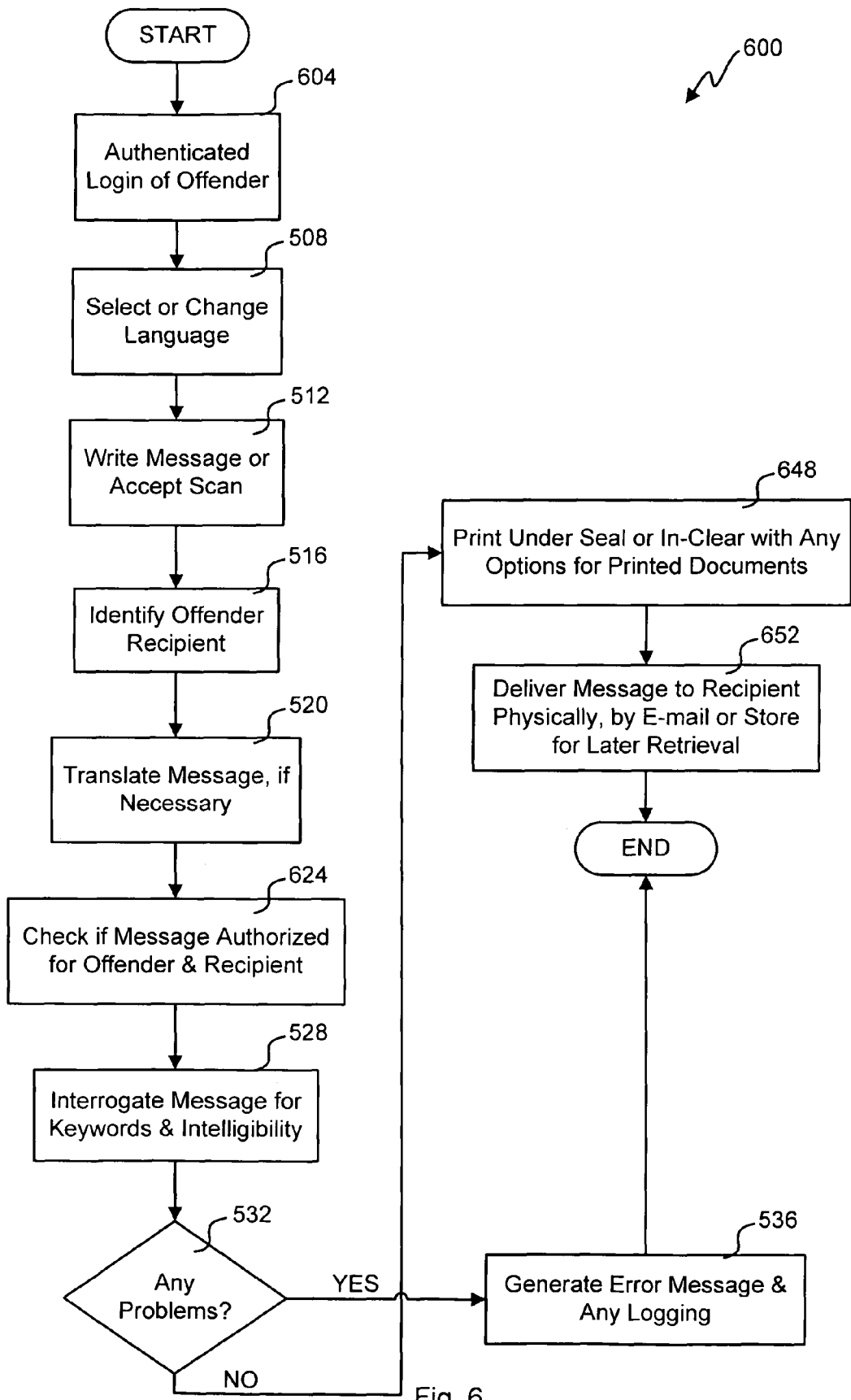


Fig. 6

OFFENDER MESSAGE DELIVERY SYSTEM

This application claims the benefit of and is a non-provisional of U.S. Provisional Application Ser. No. 60/654,546 filed on Feb. 17, 2005, which is assigned to the assigner hereof and hereby expressly incorporated by reference in its entirety for all purposes.

BACKGROUND

This disclosure relates in general to message delivery and, but not by way of limitation, to delivery of messages for incarceration facilities.

Offenders in correctional facilities can send and receive postal service mail. This mail can take weeks to get through screening that may be performed at a correctional facility. In some cases, the mail can be in a foreign language, which can further delay screening. Screening may include searching for contraband and reading the content.

Correctional facilities are under constant pressure to reduce costs and perform more efficiently. Delivery and control of mail is labor intensive. Legal papers are controlled to restrict review. Often, the legal papers have their envelope opened in front of a prisoner to assure that the legal papers are received without review.

The anthrax terrorist attacks on the postal system in the United States demonstrated how venerable the mail delivery is to this type of terrorist threat. Correctional facilities are vulnerable to this sort of threat and do not lack persons who wish to inflict damage on these institutions. Mail rooms have become the front line for these sorts of attacks.

Offenders are known to use the mail system to pass improper messages. Despite screening, the mail system often misses coded messages and contraband. Manual review of letters is labor intensive and subject to error. For example, the letter may be in a foreign language not understood by the reviewer.

BRIEF DESCRIPTION OF THE DRAWINGS

The present disclosure is described in conjunction with the appended figures:

FIGS. 1A and 1B depict block diagrams of embodiments of a communication system;

FIGS. 2A and 2B depict block diagrams of embodiments of a correctional facility system;

FIGS. 3A and 3B depict block diagrams of embodiments of a messaging system;

FIG. 4 illustrates a flow diagram of an embodiment of a process for customizing the communication system for a particular correctional facility system;

FIG. 5 illustrates a flow diagram of an embodiment of a process for sending a message to an offender; and

FIG. 6 illustrates a flow diagram of an embodiment of a process for sending a message from an offender.

In the appended figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label by a dash and a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

DETAILED DESCRIPTION

The ensuing description provides preferred exemplary embodiment(s) only, and is not intended to limit the scope, applicability or configuration of the disclosure. Rather, the ensuing description of the preferred exemplary embodiment(s) will provide those skilled in the art with an enabling description for implementing a preferred exemplary embodiment. It being understood that various changes may be made in the function and arrangement of elements without departing from the spirit and scope as set forth in the appended claims.

Specific details are given in the following description to provide a thorough understanding of the embodiments. However, it will be understood by one of ordinary skill in the art that the embodiments may be practiced without these specific details. For example, circuits may be shown in block diagrams in order not to obscure the embodiments in unnecessary detail. In other instances, well-known circuits, processes, algorithms, structures, and techniques may be shown without unnecessary detail in order to avoid obscuring the embodiments.

Also, it is noted that the embodiments may be described as a process which is depicted as a flowchart, a flow diagram, a data flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed, but could have additional steps or blocks not included in the figure. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

Moreover, as disclosed herein, the term "storage medium" may represent one or more devices for storing data, including read only memory (ROM), random access memory (RAM), magnetic RAM, core memory, magnetic disk storage mediums, optical storage mediums, flash memory devices and/or other machine readable mediums for storing information. The term "machine-readable medium" includes, but is not limited to portable or fixed storage devices, optical storage devices, wireless channels and various other mediums capable of storing, containing or carrying instruction(s) and/or data.

Furthermore, embodiments may be implemented by hardware, software, firmware, middleware, microcode, hardware description languages, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine readable medium such as storage medium. A processor(s) may perform the necessary tasks. A code segment or machine-executable instructions may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a class, or any combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, etc. may be passed, forwarded, or transmitted via any suitable means including memory sharing, message passing, token passing, network transmission, etc.

Referring first to FIG. 1A, a block diagram of an embodiment of a communication system **100-1** is shown. The communication system **100** allows sending and receiving messages between an offender within the correctional facility

system **108** and a member of the public interacting with the messaging system **104**. A home computer **116** or kiosk **112** can be used by the member of the public to interact with the messaging system **104**. There could be a single correctional facility system **108** or multiple correctional facility systems **108** that are accessible from the messaging system **104**. The correctional facility systems **108** could be groups of correctional facilities arranged by city, county, state, country, private company, or other commonality. The term correctional facility is meant to include any institution housing offenders, offenders and/or prisoners, for example, a jail, a federal or state detention center or a military prison.

The messaging system **104** has an application or web interface that is accessible from a wide area network (WAN) **120**. Any home computer **116**, kiosk **112**, personal digital assistant (PDA), mobile phone, web pad, laptop or other computing device can interact with the messaging system **104** in various embodiments. The kiosks **112** could be located at a correctional facility system **108**, library, post office, judicial building, business, law firm, or other location.

Various embodiments have different ways to enter messages. In one embodiment, a voice recognition system accessible from a phone line, for example, can be used to enter a message for the messaging system **104**. The home computer or kiosk **112**, **116** includes a keyboard, mouse and/or voice interface to allow entering messages. Some embodiments of the home computer or kiosk **116**, **112** could include a scanner to enter typed or handwritten messages. Photographs could be sent by loading them from some sort of machine readable medium or scanning them.

In this embodiment, the messaging system **104** is coupled to the correctional facility system by way of the WAN **120**. The WAN could include the Internet, private connections and/or virtual private networks to facilitate this communication. This embodiment encrypts the communication between the messaging system **104** and the correctional facility system **108** over a public network such as the Internet. Although various embodiments show certain blocks being implemented in the messaging system **104** or correctional facility system **108**, those skilled in the art appreciate that those blocks could be shuffled around the communication system **100**.

With reference to FIG. 1B, a block diagram of another embodiment of a communication system **100-2** is shown. In this embodiment, only the home computers **116** use the WAN **120** to communicate with the messaging system **104**. The kiosks **112**, messaging system **104** and correctional facility system(s) **108** use direct connections. For example, the kiosk might have an encrypted link or circuit switched connection to the messaging system **104**. Any topology of circuit or packet switched or public or private networks could be used to facilitate data transfer in the communication system **100**.

Referring next to FIG. 2A, a block diagram of an embodiment of the correctional facility system **108-1** is shown. A correctional facility computer **204** generally controls the correctional facility system **108**. The correctional facility computer could be a number of computers distributed throughout the correctional facility system **108** that communicate with a network. Kiosk **112** may be made available to offenders in some embodiments to allow sending and/or reading messages. Some embodiments do not allow reading messages at the kiosks **112**, which are printed by a message printer **208** for hand delivery to the offender.

An approved person log **232** is maintained at the correctional facility system **108**. Approved persons could include relatives, those approved for visitation, legal representatives, law enforcement, etc. Approved persons that can visit the

offender could have a biometric stored in the approved person log **232**. A biometric scanner **212** at a correctional facility could be used to gather the biometric. Other embodiments could use public biometric information such as drivers license fingerprints or photos. Biometric scanners at the kiosks **112** and home computers **116** can be verified against those stored in the approved person log **232** to authenticate identity for visitation or messaging purposes. In some cases, an approved person may have a background check to allow authorized contact with the offender.

An external interface **220** is used to communicate with the correctional facility system **108**. This external interface **220** could be for a single correctional facility or a system of correctional facilities. Communication with the external interface **220** is protected from hacking by using cryptography or physical security in various embodiments. In this embodiment, the external interface **220** uses a virtual private network to connect through the Internet to the messaging system **104**. Another embodiment uses a circuit switched network in the external interface **220** to provide physical security.

Message printers **208** are distributed through the correctional facility system **108** to allow efficient delivery of messages to offenders. The message printers can print messages with bar code, watermark, RFID, or other tracking embedded to allow tracking messages. Additionally, location and recipient information for the offender could be printed to ease delivery. The tracking information, location and recipient information could be printed on the back of sheets or in margins. For legal correspondence, the message printers could print messages and automatically insert them into an envelope to insure privacy of that communication. At delivery, the legal document can be opened in the presence of the offender if that is the correctional facility policy.

In some embodiments, the message printer **208** or special photo printers can print a photograph included with the message or sent separately. Various sized photos may be allowed for different price points. Software at the messaging system **104** could be used to screen photos for appropriateness.

An messaging interface **244** to an operator could allow confirming the offender is located near the printer and to screen any flagged messages. Messages are automatically screened at the messaging system **104** as described below, but could be manually screened when flagged or when warranted for an offender or group of offenders using the messaging interface **244**. Messages screened out during this process would not be printed for delivery to the offender. The messaging interface **244** is also used to configure the messaging system according to the policies for the correctional facility, group of offenders and/or a particular offender. Rules and policies can be entered from pre-configured templates or created from scratch.

In cases where the wrong printer **208** for an offender is initially chosen, the messaging interface could be used to re-route the message. In one embodiment, all messages are sent to an operator for manual routing to the appropriate printer **208**. Some embodiments determine routing to the printer **208** at the messaging system **104** or the correctional facility system **108** in any number of automatic and/or manual ways.

An internal money account **236** may be used to fund the message delivery costs for each prisoner in one embodiment. The internal money account **236** could be the same account used to fund other purchases by the offender. In other embodiments, an external money account is maintained by the messaging system **104**. The internal money account **236** could be used to fund the external money account or it could be funded

in other ways (e.g., credit/debit card, wire transfer, cash deposit at correctional facility, electronic check, mailed check).

An offender information, location and classification database (“offender database”) **228** is used to track various information related to the offender. The current location of the offender (i.e., correctional facility, cell block, cell identifier, floor, bed, etc.) is recorded in the offender database **228**. The classification of the offender is also stored such that groupings of offenders with similar classifications can be determined. Any investigatory flagging can also be stored such that messages are viewed with greater scrutiny. Persons capable of communicating with the offender are also stored such that messages can be limited to those persons who have been also approved. Biometrics used in authenticating the offender when using the kiosk **112** is also stored in the offender database **228**.

With reference to FIG. 2B, a block diagram of another embodiment of the correctional facility system **108-2** is shown. This embodiment of the correctional facility system **108-2** does not have a messaging interface **244**, which could allow configuration at the messaging system. The operator at the printer could manually review the printed messages and/or photos. Any flagged messages and/or photos could be held at the messaging system for review there before putting them through to the message printer **208**.

This embodiment doesn’t have a persistent connection between the external interface **220** and the remainder of the correctional facility system **108-2**. Messages are received by the external interface **220** for output by the message printer **208** without information from the remainder of the correctional facility system **108-2**. Intermittently, the external interface **220** may be used to allow configuring or reconciling data with the messaging system **104**. For example, a disk may be used to transport information that is sent by the external interface **220** to the messaging system **104**. The transported information could be used by the messaging system to properly screen, test and route messages, for example.

Referring next to FIG. 3A, a block diagram of an embodiment of a messaging system **104-1** is shown. Some blocks are similar to those of prior figures. Specifically, the external interface **220** allows communication with correctional facility systems **108** and users, the message printer **208** allows printing of messages and pictures sent from offenders, the offender database **228** gathering of offender information from various correctional facilities, and the approved person log **232** that lists who can use the messaging system **104** for specified offenders. The messaging system **104** generally serves as the interface to the message function under the control of the messaging computer(s) **304**. Additionally, screening, translation, data mining, setup, and other functions are performed or controlled by the messaging computer **304**, which may include a number of computers and/or systems. Messages from an offender could be printed at the messaging system **104** for mail or courier delivery to an approved person or any mail recipient.

Messages for sending or reading are stored in the message database **308**. According to policies for the group the offender belongs to or to unique flagging, messages may be archived for some amount of time. Once the offender is released or a period of time expires, the messages could be purged. In certain cases, the periodic purging could be stayed if there is an associated investigation or some other interest. In some embodiments, the message database may be duplicative of a number of databases at the correctional facilities that could also store messages.

A message scanner **348** allows digitizing messages or photos received in physical form. Some correctional facility systems **108** could require that all mail be routed through the messaging system **104** to avoid transporting contaminants and contraband into the correctional facilities using the mail system. Legal documents could be scanned at the law offices and uploaded to the messaging system **104** electronically for private delivery. These documents could be stored in the message database under an electronic seal or with encryption to protect the attorney-client privilege.

As mentioned above, an external money account **336** could log account balances. The account balance could be used to pay for the services of the messaging system **104** and/or to transfer funds to the internal money account **236**. The offender and/or approved person could fund the external money account **336**. Users of the messaging system **104** could be charged on a per message basis or according to a subscription. For example, for \$10 a month a particular offender could receive up to 100 sheets of messages from any number of approved persons. The revenue collected to the service could be shared on a per sheet, per message, and/or profit share basis with the cooperating correctional facilities. For example, if it were \$1 a sheet to print and deliver a picture, the messaging system could receive 80% with the remainder to the correctional facility who printed the photo.

All the messages in the message database **308** could be potentially investigated. A data mining block **312** would allow making these queries and finding patterns among messages in a manner done by data mining software. For example, when a new code word were uncovered, the data mining block **312** could query to see all the other messages from related individuals included that code word in an unusual way. Law enforcement officials could have access to the data mining tool **312** to perform these investigations. Users of the messaging system **104** could waive their right to privacy in the terms of use such that a warrant may not even be required.

The messaging system **104** could be capable of use in several different languages. When a particular offender or approved person chooses a non-English language, all messages are flagged for translation. Even if English menuing is chosen, the users are asked to specify the language of the message. Automatically, the message is translated by the message translator **316** to aid in automatic and manual review of the message. The message may be stored in both languages in the message database **308**. Some embodiments, use the message translator **316** to allow communication between parties who only speak different languages. One party can specify the delivery language to the other party.

A message interrogator **320** performs several functions to screen and/or flag messages. A keyword database **324** could search for suspect terms that are globally specified or could only search messages from certain parties or groups for certain words. For example, any mention of “murder” could be flagged, but a code word “redlight” could only be flagged by the gang members known to use that term could be flagged. The message interrogator **320** also searches for unintelligible or odd communications. An unintelligible message could signal code is being used or that the translation was not performed correctly. Odd communications could be use of obscure terms in strange ways. For example, repeated use of a term such as “redlight” could point to a potential code word.

Any flagging or screening is noted in the message database and forwarded to the correctional facility system **108** for possible additional screening. Different screening policies could exist for different offenders or groups of offenders. For example, screening for gang code words in a minimum secu-

city half way house might not be performed unless an individual is suspected as belonging to a gang. The messaging computer **304** passes messages through the external interface **220** in communicating with the appropriate correctional facility system **108**.

With reference to FIG. 3B, a block diagram of another embodiment of a messaging system **104-2** is shown. This embodiment does not include a message scanner **348** or message printer **208** to allow mail conversion for electronic messaging. This embodiment includes separate user interfaces **220-1** and correctional facility interfaces **220-2**. The correctional facility interface **220-2** may be isolated from other parts of the messaging system **104** using physical security and/or firewalling. The messaging computer **304** be a secure processor or use other techniques to prevent hacking through the user interface **220-1** to get at confidential information or disable the messaging system **104**.

The data structure of this messaging system **104-2** is different from other embodiments. The offender database **228** and approved person log **232** are not maintained in the messaging system **104**. This information could be queried on demand from the relevant correctional facility system **108** rather than storing it locally. This embodiment includes a separate message archive **340** to keep those messages that are likely to be used for data mining in the future. The message archive **340** could be a back-up system that uses removable media, such as tapes or optical disks. If needed, these archived messages can be maintained for years.

This embodiment also includes a correctional facility customizations database **344**. Each correctional facility system **108** can customize message policies for groups of offenders, individual offenders and/or subsets of groups of offenders. Further, translation and interrogation algorithms can be customized according to preferences by the various correctional facility systems **108**. Revenue agreement terms can be placed in the customizations database **344** to allow automatic division of revenue.

Referring next to FIG. 4, a flow diagram of an embodiment of a process **400** for customizing the communication system **100** for a particular correctional facility system **108** is illustrated. These customizations could be entered using the messaging interface **144** and stored in the correctional facility customizations database **344**. The depicted portion of the process begins in block **404** where the operator logs into the messaging interface **244**. A biometric could be used here for increased security. Some embodiments allow remote login, but others require the physical security of performing the customizations at the messaging system **104**. Offender groups are configured in block **408**. All offenders are categorized one or more of these groupings in the offender database **228**. The groups could be by cell block, crime, category of crime, gang affiliation, approved person affiliation, etc.

In block **416**, offender records are tied to the various groups in the offender database **228**. Exceptions to various groupings can be specified individually or in a subset in block **420**. For example, all undercover agents that are posing as gang members could be excluded from the policies specified for that group. Keywords can be specified globally or by group in block **424**. Other configurations, could be performed although not shown in the figure.

With reference to FIG. 5, a flow diagram of an embodiment of a process **500** for sending a message to an offender is shown. The depicted portion of the process begins in block **504** where the user or legal representative is authenticated. This could include matching biometrics and checking the approved person log **232**. First time users and legal representative might have to set up an account, get an authentic bio-

metric scan and/or have a background check performed before use of the messaging system **104** is allowed. Where authorization passes, processing continues to block **508** where the language of the web site and/or message is specified.

The message is written, uploaded or scanned into the messaging system **104** in block **512**. This message could be a photo or include a photo in addition to text. Where a legal representative wants the message to remain confidential, this can be specified. In block **516**, the offender recipient is identified. A check is made to confirm that the approved person is authorized to exchange messages with the particular offender. If necessary, the message is translated in block **520**. Both the translated and un-translated message are stored in the message database **308**.

Policies for groups, individuals and subsets are checked in block **524** to determine if authorized. For example, a particular correctional facility might be in lock down at the time the message is entered such that it would be stored for possible later delivery. Some embodiments could limit the number or length of the messages. Authorization may also include checking for sufficient credit or money in the money account (s) **236**, **336**. In block **528**, the message is interrogated for intelligibility and keywords. Other checks could be performed in this block to find patterns that should be flagged.

In block **532**, a determination is made if there were any problems in the preceding blocks. Where there are problems, an appropriate error message is generated before possibly logging the error and/or message in block **536**. The process could be initiated again or resumed once the problem is remedied. Where there is no problem processing goes from block **532** to block **540** to determine the location of the offender. This location is stored in the offender database **228** that might be local to the messaging system **104** or in the correctional facility system **108**.

In block **544**, the message is sent from the messaging system **104** to the proper correctional facility system **108**. This may be automatically done where the offender location is discernable. Other embodiments may send all messages to a particular location for manual direction to the appropriate part of the correctional facility system. Yet other embodiments may deliver most automatically, but some are still routed manually when the location of the offender cannot be discerned. Flagged, blocked and/or questionable messages can also be reviewed manually in this block to further investigate if delivery is appropriate.

The message and/or photos are printed in block **548**. For legal documents properly indicated, the printing can be done under seal to prevent viewing by correctional facility personnel under normal circumstances. Bar coding, water marking, expiration dates, delivery instructions, etc. can be included according to correctional facility customizations **344**. In block **552**, the message and/or pictures are delivered to the offender recipient. In this embodiment, a handheld scanner can scan a bar code associate with the printer and a bar code on the document to confirm delivery of the message. This delivery confirmation could be passed back to the messaging system **104** to provide an audit trail.

Referring next to FIG. 6, a flow diagram of an embodiment of a process **600** for sending a message from an offender is shown. This process is similar to that performed when sending a message to the offender. The below description accentuates the differences from the prior described process. In block **604**, the authentication is performed on the offender using biometrics, but could also include reading a correctional facility identity card. Blocks **508**, **512**, **516**, and **520** are performed as before. In block **624**, a determination is made of

whether the offender and recipient are authorized. The recipient is registered with the messaging system and authorized. In this embodiment, the recipient can register an e-mail address or physical address without giving that information to the offender. The messaging system **104** can redirect the message to the appropriate address without disclosing that information to the offender.

Next, blocks **528**, **532**, and **536** are performed as before. Where there are no problems in block **532**, processing continues to block **648** where messages for mailing are printed, which can be done under seal if the offender specifies that the message is legally protected. The message could still be stored in the message database **308** should a search warrant be issued to review the messages tagged as legal documents. In block **652**, the message is delivered electronically or physically. A particular recipient can view the messages by logging into the message system **104** and/or by specifying an e-mail address to receive any messages.

A number of variations and modifications of the disclosed embodiments can also be used. For example, the above embodiments describe delivering documents to offenders, but the messages could be similarly sent to or from correctional facility administration. Some embodiments discuss having the messages go between approved persons and approved visitors. Other embodiments could allow anyone to message offenders in much the same way that mail is allowed today. The ability for offenders to send messages to anyone may be curtailed or not in various embodiments. For example, messages that are sent by offenders for printing and mailing could be unrestricted, but e-mail messages could only be to approved persons.

The techniques described herein may be implemented by various means. For example, these techniques may be implemented in hardware, software, or a combination thereof. For a hardware implementation, the processing units may be implemented within one or more application specific integrated circuits (ASICs), digital signal processors (DSPs), digital signal processing devices (DSPDs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs), processors, controllers, micro-controllers, microprocessors, other electronic units designed to perform the functions described herein, or a combination thereof.

For a software implementation, the techniques, processes and functions described herein may be implemented with modules (e.g., procedures, functions, and so on) that perform the functions described herein. The software codes may be stored in memory units and executed by processors. The memory unit may be implemented within the processor or external to the processor, in which case it can be communicatively coupled to the processor via various means as is known in the art.

While the principles of the disclosure have been described above in connection with specific apparatuses and methods, it is to be clearly understood that this description is made only by way of example and not as limitation on the scope of the disclosure.

What is claimed is:

1. A correctional facility communication system for sending an external message to an offender of a correctional facility, the correctional facility communication system comprising:

a messaging system at a first location configured to:
 authenticate a sender of the external message,
 receive the external message at the first location,
 wherein the external message is in electronic form,
 check the external message against criteria specified by the correctional facility,

provide a unique identifier for the external message, wherein the unique identifier triggers analysis according to a criteria specified by the correctional facility, and

send the external message to a second location for automatic printing on a corresponding printer that prints the external message with the unique identifier being visible;

a correctional facility system at the second location, wherein the correctional facility system:

receives the external message,
 analyzes the unique identifier according to the criteria to determine the external message is confidential, and automatically prints the external message under seal and with an identifier, corresponding to the unique identifier, visible for distribution to the offender; and

a wide area network coupling the messaging system to the correctional facility system.

2. The correctional facility communication system for sending the external message to the offender of the correctional facility as recited in claim **1**, wherein the criteria is testing for coherent prose.

3. The correctional facility communication system for sending the external message to the offender of the correctional facility as recited in claim **1**, wherein the sender is subjected to a background check as part of the authentication process.

4. A method for sending an external message to an offender of a correctional facility, the method comprising steps of:

authenticating a sender of the external message;
 receiving the external message at a first location, wherein the external message is in electronic form;
 checking the external message against criteria specified by the correctional facility;

providing a unique identifier for the external message, wherein the unique identifier triggers analysis according to a criteria specified by the correctional facility,
 sending the external message to a second location for automatic printing on a corresponding printer that prints the external message with the unique identifier being visible;

receiving the external message at the second location;
 analyzing the unique identifier according to the criteria to determine the external message is confidential; and
 automatically printing the external message under seal and with an identifier, corresponding to the unique identifier, visible for distribution to the offender.

5. The method for sending the external message to the offender of the correctional facility as recited in claim **4**, further comprising a step of physically delivering the external message to the offender.

6. The method for sending the external message to the offender of the correctional facility as recited in claim **4**, further comprising a step of revenue sharing a charge for sending the external message between the correctional facility and the sender.

7. The method for sending the external message to the offender of the correctional facility as recited in claim **4**, further comprising a step of scanning the external message.

8. The method for sending the external message to the offender of the correctional facility as recited in claim **4**, wherein the second location tracks with bed movement of the offender.

9. The method for sending the external message to the offender of the correctional facility as recited in claim **4**, wherein the authenticating step further comprising steps of:
 accepting a scanned biometric from the sender;

11

comparing the scanned biometric with a previously-gathered biometric; and authenticating the sender where the scanned biometric is similar to the previously-gathered biometric.

10. A machine-readable medium having machine-executable instructions for sending an external message to an offender of a correctional facility of claim 4.

11. A machine adapted for sending an external message to an offender of a correctional facility of claim 4.

12. A communication system for sending an external message to an offender of a correctional facility, the communication system comprising:

a processor configured to:

authenticate a sender of the external message, receive the external message at a first location, wherein the external message is in electronic form, check the external message against criteria customized by the correctional facility,

provide a unique identifier for the external message, wherein the unique identifier triggers analysis according to a criteria specified by the correctional facility to cause printing the external message under seal, and send the external message to a second location for automatic printing on a corresponding printer that prints the external message with an identifier, corresponding to the unique identifier, being visible; and

a memory coupled with said processor.

13. The communication system for sending the external message to the offender of the correctional facility as recited in claim 12, wherein:

the processor is at the first location, and the correctional facility is at the second location.

14. The communication system for sending the external message to the offender of the correctional facility as recited in claim 13, further comprising a wide area network coupling the correctional facility to the processor.

15. The communication system for sending the external message to the offender of the correctional facility as recited in claim 12, wherein biometrics are used to authenticate the sender.

16. The communication system for sending the external message to the offender of the correctional facility as recited in claim 12, wherein the second location is determined by the criteria specified by the correctional facility.

17. The correctional facility communication system for sending the external message to the offender of the correctional facility as recited in claim 1, wherein the first location is different from the second location.

18. The correctional facility communication system for sending the external message to the offender of the correc-

12

tional facility as recited in claim 1, wherein the correctional facility communication system includes an offender database comprising at least one of:

offender location, and offender classification.

19. The correctional facility communication system for sending the external message to the offender of the correctional facility as recited in claim 18, wherein the correctional facility criteria includes groups of offenders, wherein the groups are determined by classification.

20. The correctional facility communication system for sending the external message to the offender of the correctional facility as recited in claim 18, wherein the location may be any one of correctional facility, cell block, cell identifier, floor, or bed.

21. The correctional facility communication system for sending the external message to the offender of the correctional facility as recited in claim 1, wherein the criteria is entered from pre-configured templates.

22. The correctional facility communication system for sending the external message to the offender of the correctional facility as recited in claim 21, wherein the templates may include one or more of the correctional facility criteria.

23. The correctional facility communication system for sending the external message to the offender of the correctional facility as recited in claim 1, wherein the criteria determine offender and sender permissions.

24. The correctional facility communication system for sending the external message to the offender of the correctional facility as recited in claim 1, wherein the identifier is a tracking code that includes any one or more of a barcode, a radio frequency identification, or a watermark.

25. The method for sending an external message to an offender of a correctional facility as recited in claim 4, wherein the step of checking the external message against criteria further comprises:

determining an offender location, and determining an offender classification.

26. The method for sending an external message to an offender of a correctional facility as recited in claim 25, wherein the correctional facility criteria includes groups of offenders, wherein the groups of offenders are determined by the offender classification.

27. The method for sending an external message to an offender of a correctional facility as recited in claim 25, wherein the offender location may be any one of correctional facility, cell block, cell identifier, floor, or bed.

* * * * *



US009231954B2

(12) **United States Patent**
Torgersrud et al.

(10) **Patent No.:** **US 9,231,954 B2**
(45) **Date of Patent:** **Jan. 5, 2016**

- (54) **COMMUNICATIONS SYSTEM FOR RESIDENTS OF SECURE FACILITY**
- (71) Applicant: **Telmate LLC**, San Francisco, CA (US)
- (72) Inventors: **Richard Torgersrud**, San Francisco, CA (US); **James Dominick Alessio**, Berkeley, CA (US); **John Satori Yamasaki**, San Francisco, CA (US); **Nick Garcia**, Oakland, CA (US); **Devon Brooke Lindsey**, San Francisco, CA (US)
- (73) Assignee: **Telmate, LLC**
- (*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 47 days.

8,699,998 B2 *	4/2014	Sprigg	H04L 51/12
				455/410
8,965,416 B2 *	2/2015	Moshir	G06Q 50/34
				455/405
2002/0067272 A1 *	6/2002	Lemelson et al.	340/573.4
2002/0120573 A1 *	8/2002	McCormick	G06Q 50/22
				705/50
2004/0146048 A1 *	7/2004	Cotte	370/352
2008/0161027 A1	7/2008	Benco et al.		
2008/0222127 A1 *	9/2008	Bergin	707/5
2009/0189736 A1 *	7/2009	Hayashi	G06F 21/32
				340/5.81
2009/0222329 A1 *	9/2009	Ramer et al.	705/10
2009/0265552 A1 *	10/2009	Moshir et al.	713/168
2010/0040007 A1	2/2010	Itagaki et al.		
2010/0180031 A1 *	7/2010	Cacheria, III	G06Q 10/1057
				709/225
2011/0153380 A1 *	6/2011	Velusamy	705/7.19
2012/0253868 A1	10/2012	Ach et al.		
2012/0289206 A1	11/2012	Shim		
2012/0309437 A1	12/2012	Salonen		
2013/0002433 A1 *	1/2013	Wilmeth et al.	340/573.4
2014/0162598 A1 *	6/2014	Villa-Real	H04M 1/66
				455/411

(21) Appl. No.: **13/842,015**

(22) Filed: **Mar. 15, 2013**

(65) **Prior Publication Data**
US 2014/0282896 A1 Sep. 18, 2014

(51) **Int. Cl.**
H01L 29/06 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC **H04L 63/101** (2013.01); **H04L 63/02** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS

5,537,102 A *	7/1996	Pinnow	340/5.8
6,853,739 B2 *	2/2005	Kyle	382/115
7,865,386 B2	1/2011	Sarkar		
8,629,755 B2 *	1/2014	Hashim-Waris	...	G06Q 30/0235
				340/10.1

OTHER PUBLICATIONS

Sankaran, Siva R.; Bui, Tung. A Web-Based Correctional Telemedicine System with Distributed Expertise. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=926798>.*

(Continued)

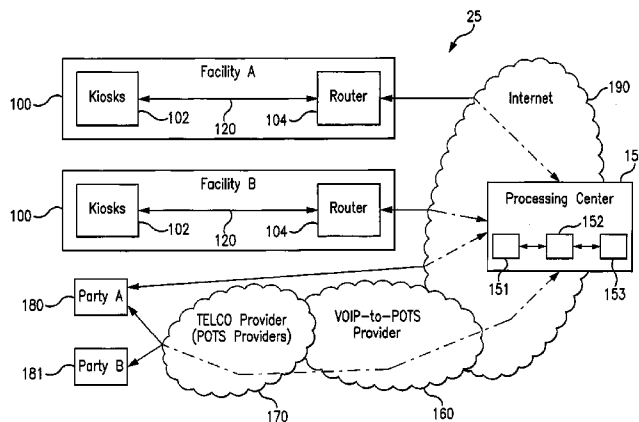
Primary Examiner — Jeremiah Avery

(74) *Attorney, Agent, or Firm* — Venable LLP; Jeffri A. Kaminski; Leslie A. Lal-Lee

(57) **ABSTRACT**

A system and a method are provided for two-way communications, automated request handling, and push notifications, via SMS, MMS, IM, email, and other electronic messaging systems, between (1) residents confined to a secure facility, such as a jail or a prison, and (2) persons located outside the secure facility who have friendly or family relationships with the confined residents.

13 Claims, 4 Drawing Sheets



(56)

References Cited

OTHER PUBLICATIONS

Armstrong, Natalie; Losavio, Michael; Keeling, Deborah. Digital System, Evidence & Forensic Issues in Correctional Environments. 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5491963>.*

Perusco, Laura; Michael, Katina. Control, Trust, Privacy, and Security: Evaluating Location-Based Services. Technology and Society Magazine, IEEE. vol. 26, issue 1. Pub. Date: 2007. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4135773>.*

“Matching a SMS Reply to the Original SMS Sent”, SMS & MMS Technical Form, Jun. 2, 2006, pp. 1-8.

“Two-Way Messaging and Matching a Response to an Outbound Message”, Stack Overflow, pp. 1-3.

* cited by examiner

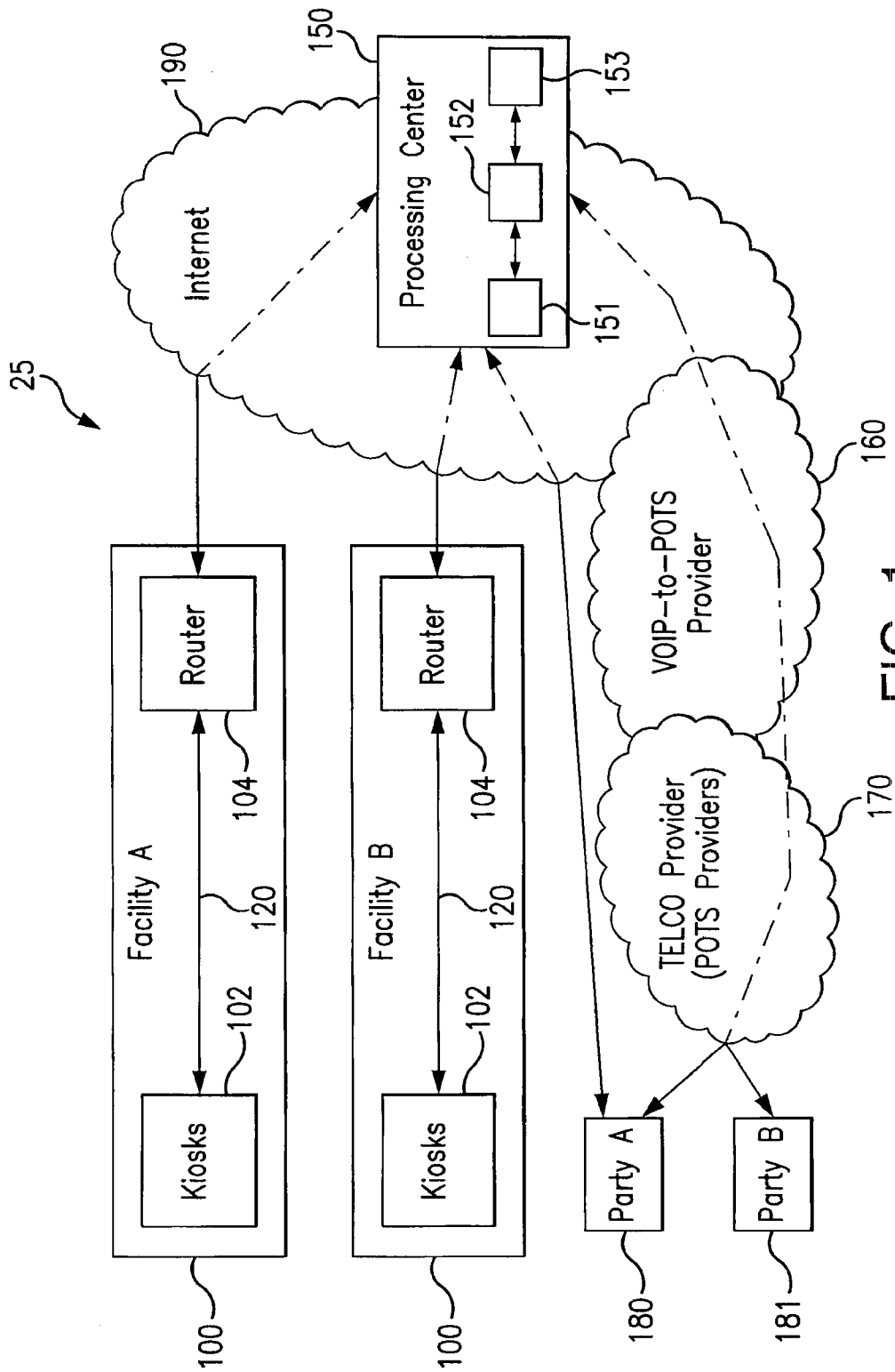


FIG. 1

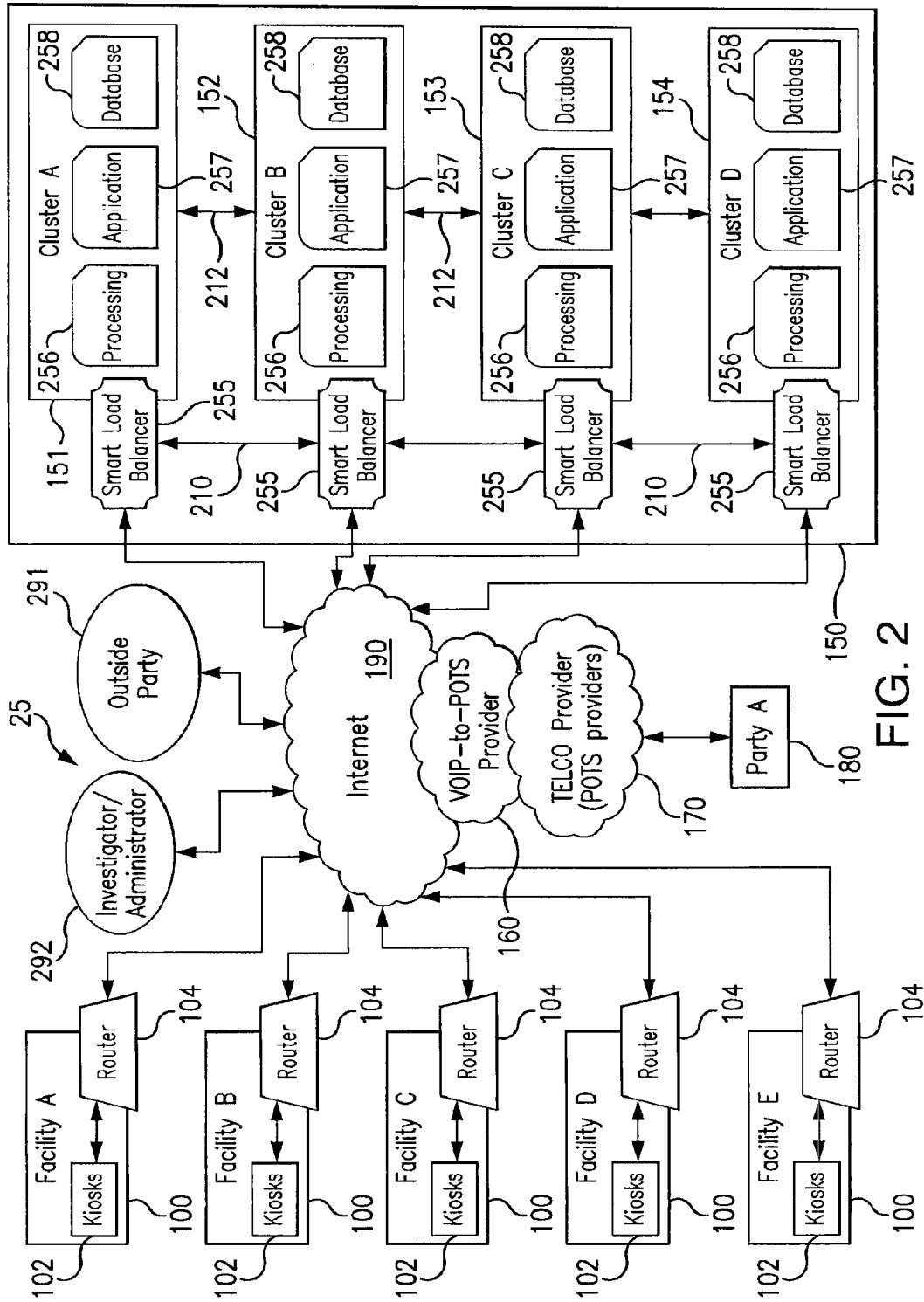


FIG. 2

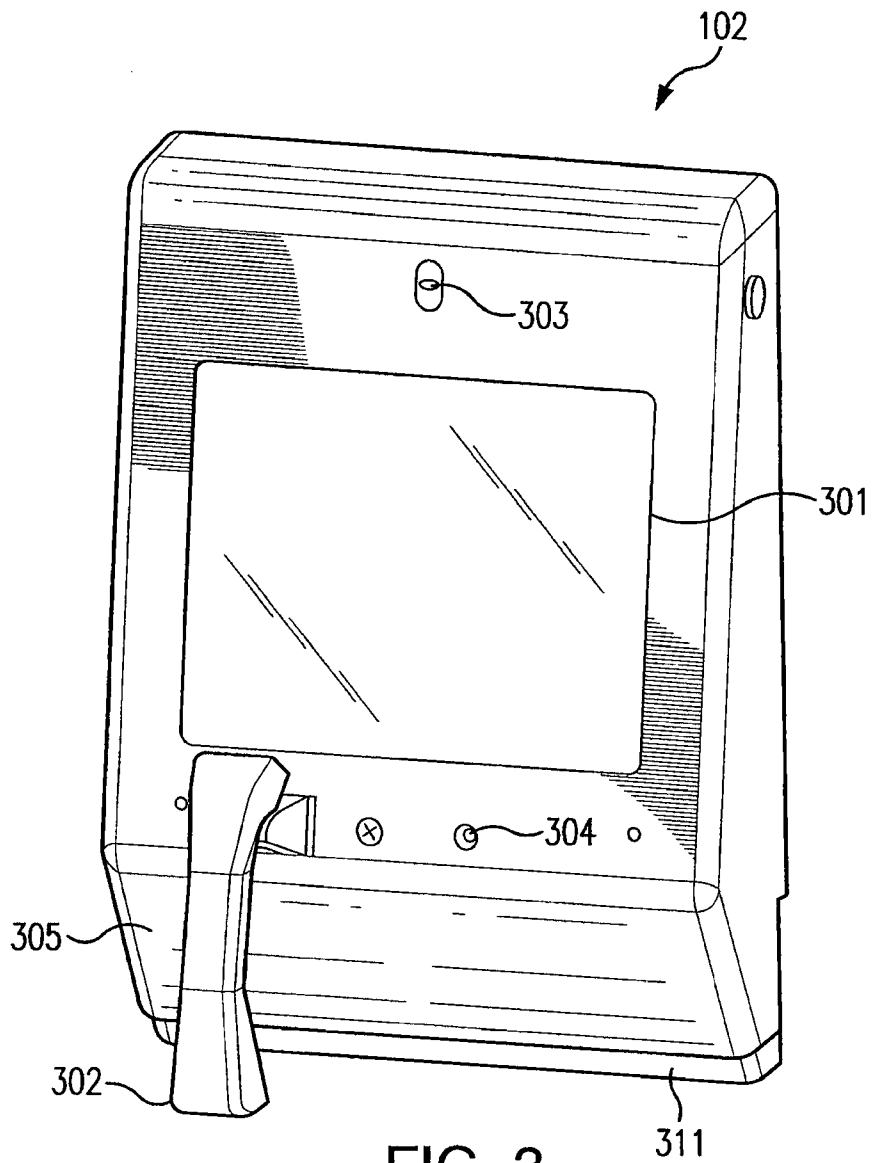


FIG. 3

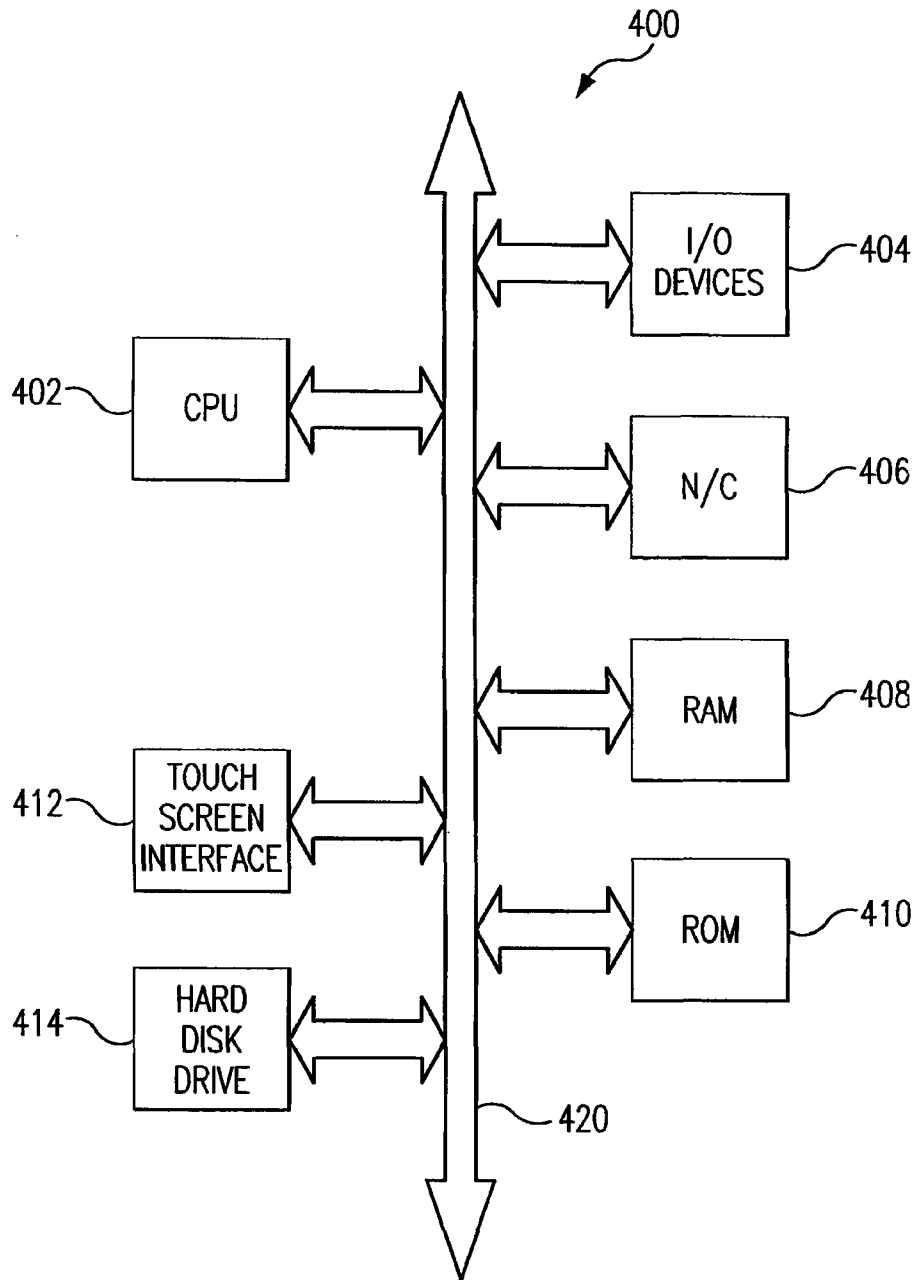


FIG. 4

1

COMMUNICATIONS SYSTEM FOR RESIDENTS OF SECURE FACILITY

This disclosure relates to a system for providing and arranging for communications with and between (1) residents of a detention environment, who use commercial, off-the-shelf or other communications terminals, and (2) persons who reside outside the facility, and who use cellular telephones or other terminals capable of using short message service (SMS), multimedia message service (MMS), instant messaging (IM), and the like electronic messaging protocols.

BACKGROUND

Because of security requirements and other considerations, residents of a detention environment are typically limited as to which persons outside of the environment they may communicate with. As such, direct, uncontrolled communications using standard telephone systems, including SMS and MMS messaging and IM, are unsuitable, and administrators of detention environments may go to great lengths to prevent such communications.

Persons wishing to communicate with individuals residing inside detention environments have limited methods and time-windows in which to have telephone and/or video calls. Outside persons normally cannot call inmates of detention environments, but can only leave voicemails, or use traditional mail or participate in visitation day. There is a need for a more convenient way for outside persons to communicate with inmates while maintaining the safety and security features that detention environments require.

Some of the limitations associated with detention environment communications result from the rules promulgated by the detention environments, some limitations result from limited availability of visitation rooms or telecommunications equipment, or funds available, while others result from conflicting schedules of the residents of the detention environment and those on the outside. Historically, staff personnel at detention environments have needed to be personally and individually involved in arranging visitations for the confined residents, and there are no suitably automated systems for managing and overcoming the above barriers.

SUMMARY

Persons residing inside detention environment, which may be a jail, prison, detention center, detention facility, or other secure facility, typically have extremely limited access to communications with persons outside the facility. Nevertheless, frequent communications with friends, family members, and others outside the facility have been shown to improve the morale of confined persons, reduce their recidivism, decrease their involvement with gambling, fighting, and other deleterious activities, and generally improve their chances of rehabilitation.

Consequently, it is desirable to provide a system for increasing the opportunity, convenience and frequency by which residents of a detention facility can communicate with people outside the facility. It is also desirable to provide for other communications capabilities that keep persons outside the facilities better apprised of the residents' status. In particular, it is highly desirable to provide a secure and controlled system by which residents of a secure facility can have more frequent and convenient contact with properly authorized persons outside the facility.

According to this disclosure, a system terminal (or kiosk) may be located inside the secure facility, computing clusters

2

may be located in a secure data center outside the facility, and interconnections may be provided within public telephone, cellular phone, and/or public Internet networks. The computing clusters may be configured, with suitable hardware and software, to manage communications between the residents of multiple secure facilities and persons outside the secure facilities.

This disclosure establishes a broad, yet focused set of communications tools that serve to increase communications between residents of secure facilities and their friends and family members residing outside such facilities. The communications may have the external convenience of typical SMS communications between two persons, even though they are converted from or to the public SMS or email networks to or from a separate communications system respectively using one or more terminals inside the detention environment. This disclosure is not limited, however, to SMS communications. Among other things, this disclosure may be used in connection with communications to and from uniquely addressed email addresses, including emails to and from detainees.

According to one aspect of this disclosure, automated communications (push notifications) may be initiated by computing clusters that serve the terminals that are inside the secure facilities. The push notifications may be generated automatically in response to events pertinent to the residents of the secure facilities, such as notifications about low bank or credit union account balances, upcoming court hearings and release dates, movement between facilities, gaps in communications, and requests (by any party) to establish communications through other channels.

This disclosure also relates to a system for originating manual and automated communications from wired or wireless terminals inside secure facilities, or data centers serving secure facilities, to public or private telephone networks and/or other networks such as the Internet. The system may be configured to verify that the resident is authorized to communicate with the recipient of an automated communication, prior to each such communication, and a communication may be pushed to the recipient only after the authorization is verified. The resident may be a prisoner or some other person who is detained within the detention environment.

This disclosure also relates to a method for accepting responses to multiple different queries originating from the same mobile telephone number or SMS short code and pertaining to a resident of a secure facility. As the method is performed, one or more unique sets of numbers or characters may be generated for each message requiring a response, and each set of numbers is made to be unique for a predetermined period of time for the end-user to which they are delivered, with respect to that query, even if repeated in multiple messages. The assigned response methods, keywords, characters, or numbers are guaranteed to be unique to the query within a specified time period.

According to one aspect of this disclosure, a phone number, email, SMS or MMS could have a unique string of characters that allow the system to route the communication to the intended individual, and the operator of the system could potentially bill (charge) for the transaction. For example, an SMS may have a @chr001 shortcode to route and bill the message correctly. An email to chr001@gettingout.com would route to the same detainee. The system may also be configured so that a caller calls a single 800 number and then after a prompt, enters a unique series of digits, for example, "5464548" to leave a voicemail without having to search a directory of detainees.

This disclosure also relates to a method by which a person outside a secure facility, with whom a particular resident of a

secure facility is authorized to communicate, can request an electronic communication with the resident via electronic message (e.g., SMS, MMS, IM or email). Moreover, this disclosure relates to a method by which a first person, who is outside a secure facility (or a resident of the secure facility) can request that a particular second person establish an elec- 5 tronic relationship with the first person.

This disclosure also relates to a method by which a person outside a secure facility can communicate with a resident of the secure facility using SMS, MMS, IM, email or similar electronic messaging. As the method is performed, messages are converted to a format suitable for delivery to and from terminals located inside the secure facility by a data center located outside the facility, and the system verifies that the resident is authorized to communicate with the outsider prior to each communication. 10

This disclosure also relates to a method by which a person outside a secure facility can post a message or the like, or upload photos, audio, videos, and other electronic multimedia to an electronic message board pertaining to a specific resident of the detention environment, or pertaining to all residents associated with the outsider. The uploading does not occur, however, until the automated system verifies that the detained resident is authorized to communicate with the outsider. If desired, the verification may occur before each such upload. 15

This disclosure is not limited to the communication of text and video messages but also relates to a system by which a person outside a secure facility can provide funds to a resident of the facility via an electronic message. According to one aspect of this disclosure, messages may be automatically generated when a bank or credit union account balance drops below a set threshold, such as a fixed dollar amount, or an amount sufficient to cover a visit of a specified duration. 20

The systems and methods described in this disclosure may be specifically tailored to providing two-way notifications between a first party residing inside a secure facility, and a second party residing outside the secure facility. Because the first party may not have access to a personally-owned telecommunications terminal and must rely on using a pool of terminals shared with other residents, different addressing and alerting schemes must be used. Because the first party also typically lacks direct access to funds, he is also dependent upon one or more parties on the outside to deposit funds into a remote visitation account. 25

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a schematic view of a communications system constructed in accordance with an embodiment of this disclosure; 30

FIG. 2 is another schematic view of the communications system of FIG. 1;

FIG. 3 is a perspective view of a communications device for the communications system of FIG. 1; and

FIG. 4 is a hardware diagram for the communications system of FIG. 1. 35

DETAILED DESCRIPTION

Referring now to the drawings, where like reference numerals designate like elements, there is shown in FIG. 1 a system 25 that is constructed in accordance with a first embodiment of this disclosure. The system 25 includes an interactive audio/video platform that has kiosks 102 for providing administrative services at multiple secure facilities 100. The platform also includes a processing center 150 that 40

is connected to one or more facilities 100 through a network such as, e.g., the Internet 190. The secure facilities 100 that utilize the system 25 may be any that require voice, video, and/or information services, especially those with strict security requirements and large traffic volumes, including secure facilities such as prisons and other government detention facilities. In a preferred embodiment, each facility 100 contains at least one kiosk 102. In other embodiments, one or more of the facilities 100 contains at least one kiosk. 45

Each kiosk 102 is connected to a router 104 via a networking link 120. The routers 104 are configured to communicate with the processing center 150, which may be distributed (151, 152, 153) across several locations. The routers 104 each transmit communications received from the kiosks 102 to the Internet 190, and exchange Internet protocol (IP) packets bidirectionally between the processing center 150 and the resident of the respective facility 100. The processing center 150 includes application hardware (FIG. 4) and software for data processing and other functions described below. 50

As illustrated in FIG. 1, the processing center 150 is distributed across multiple clusters 151, 152, 153, 154 (FIG. 2), which may or may not be geographically diverse. Each cluster 151, 152, 153, 154 hosts multiple nodes, including an applications node 257, a database node 258, and a call processing node 256. The clusters 151, 152, 153, 154 communicate with each other via the Internet 190 or dedicated connections 210, 212. Information in any one database node 256, 257, 258 can be shared among the clusters 151, 152, 153, 154. 55

Data storage and retrieval can be performed across the several clusters 151, 152, 153, 154, and the clusters 151, 152, 153, 154 can provide fail-over for one another. If desired, the router 104 at each facility 100 may be configured to communicate with another cluster 151, 152, 153, 154 if a primary cluster 151, 152, 153, 154 is or becomes unavailable. As illustrated in FIG. 2, one or more smart load balancers 255 may be used to manage the clusters 151, 152, 153, 154 such that the resources of the respective cluster nodes 256, 257, 258 (which may each include multiple computers) can be reallocated as processing needs require. 60

As illustrated in FIG. 1, the processing center 150 routes communications from facility residents, who use the kiosks 102, to outside parties 180, 181. That is, the processing center 150 routes voice, text and/or video traffic from facility kiosks 102 to and from their ultimate intended destinations. To route voice-communications traffic, the processing center 150 communicates via internet protocol (IP) to a VoIP-to-POTS provider 160, which converts voice over IP (VoIP) communications to plain old telephone service (POTS) communications, and vice versa. Companies who provide VoIP-to-POTS services include Paetech, Level 3, and Verizon. After converting the VoIP signal to a POTS signal, the VoIP-to-POTS provider 160 provides the communication to a telecommunications provider 170 which routes the call to the intended one of the called parties 180, 181. 65

The processing center 150 may also be used to route video and text communications. Communications that are received from the facility routers 104 may be stored or cached on web servers in the processing center 150 or on third-party web servers. In addition to storing communications routed through the processing center 150, the processing center 150 may be configured to receive and store recordings of local communications (e.g., local video communications) that have been recorded at the facilities 100. The communications that are stored at the processing center 150 can be accessed by an investigator or administrator 292 (or another authorized person 291 outside the secure facility 100) using a web browser on a computer connected to the Internet 190. The processing 70

5

center **150** also may be configured to receive a request for data from the routers **104**, such as hypertext transfer protocol (HTTP) requests, and return information for the routers **104**, such as information on a third-party website.

According to a preferred embodiment, each kiosk **102** is in the form of the interactive audio/video terminal shown in FIG. **3**. The illustrated kiosk **102** has an integrated camera **303** that can be used for video communications and/or for user authentication via facial recognition. The kiosk **102** also may have a touch screen **301** for displaying images and/or for detecting the presence and location of a user's touch within its display area. The touch screen **301**, may be, for example, a 15-inch capacitive or resistive touch screen display. In the illustrated embodiment, the screen **301** serves as the main kiosk interface with the user. A telephone handset **302** connected to the kiosk **102** may have a speaker and a microphone. The handset **302** can be used to issue voice commands and provide voice authentication as required, and it may be used for voice and video communications, among other things.

The illustrated handset **302** is optional, as the kiosk user may instead plug in headphones (not illustrated) with an in-line microphone using one or more stereo headphone jacks **305** (and/or a speakerphone). If desired, the headphone jacks **305** may be located to the side of the kiosk **102** or behind a movable panel **311**. The panel may be locked in a position exposing the jacks, or in a position blocking them, depending on the preferences of the secure facility. A USB interface (not illustrated) optionally located behind the movable panel may be used for system diagnostics by technicians or to synchronize files to an external device, such as a portable media player. The kiosk **102** also may have a speaker **304** that provides audio output.

In operation, the audio/video terminals **102** may serve several purposes aside from providing the video camera **303** and display **301** used to conduct visitations. Such purposes include sounding and/or displaying notifications of incoming calls and/or requests; and allowing residents of the secure facility **100** to initiate requests for immediate or scheduled visitations, and to send and receive text-, audio, and video-based messages or combinations thereof using the microphone, speaker, video camera **303**, and a keyboard displayed on the screen **301**.

Separately located at one or more of the secure facilities **100**, as an optional component, are facility-owned or -operated computer systems that operate a jail management system (JMS). A JMS has one or more databases, computer terminals, and other components that record, store, and update the status of residents of the secure facility, including but not limited to each resident's activity within the facility, intake and expected release dates, good and bad behavior records, medical records, pending charges, past convictions, known gang affiliations, legal representation, and authorized and/or prohibited visitors. The JMS typically has the ability to export some or all of this data to third-party computer systems via suitable Internet connections. The detention environment **100** may have access to and/or operate one or more of the location-based tracking systems described in U.S. patent application Ser. No. 13/842,437 (Location Based Tracking System; Inventors: Richard Torgersrud and Christopher Ditto, being filed concurrently herewith). The entire disclosure of the aforementioned U.S. patent application is incorporated herein by reference.

The processing center **150** may connect to the JMS to synchronize some or all of the information associated with each resident, so as to obtain data which can aid in the correct operation of the communications system **25** with respect to facility and court-mandated rules, specific to that facility,

6

and/or rules specific to each resident. Thus, according to one aspect of this disclosure, messages may be automatically generated whenever a calendar date with an event or action pertaining to the resident of the secure facility **100** approaches, or whenever the resident reaches a rehabilitation milestone, as established by the secure facility, such as a change to release date.

Referring again to FIG. **1**, requests for communications that are input at the audio/video kiosks **102** are transmitted to the processing center **150**, which processes the requests and transmits the requests to the intended recipient(s) **180**, **181**. The requests may be to initiate an audio and/or video call, initiate a text chat, or schedule a future call or chat with one or more persons **180**, **181** residing outside the secure facility **100**. In the case of text chats, the requests and subsequent actual chat may be transmitted as an electronic message, such as SMS or MMS messages, via the cellular telephone network directly, or through Internet application programming interfaces (APIs) or other services that relay the messages to the cellular telephone network, and ultimately to the terminal equipment (such as end-user cell phones) **180**, **181**, and transmit message traffic, requests and/or responses back to the processing center **150**.

In a preferred embodiment, the processing center **150**, using data provided by the JMS, verifies that all parties involved in communications and requested communications have been authorized to communicate with each other (that is, the resident of the detention facility is authorized to and/or not precluded from communicating with the one or more outside parties) and to communicate at that time, and verifies that the persons communicating are who they claim to be. The requests and/or responses transmitted from the kiosks **102** are then processed on the computing clusters **151**, **152**, **153**, **154** in order to schedule, modify, or cancel future visitations; transmit reminders about account balances, upcoming relevant dates, or other pertinent data, or other notifications.

Although remote video visitations may be scheduled and confirmed on a personal computer, individuals who are outside of secure facilities are not always near such a device, and thus the resident of the secure facility **100** may experience a significant delay in receiving a confirmation of a requested visit. Therefore, it is desirable to transmit visitation requests to a mobile terminal, such as a cell phone or a smart phone. As many people have the cell phones and smart phones turned on and located on or near their person continually, such devices represent an ideal platform with which to confirm a visitation request. For instance, the typically rapid delivery of SMS messages and the concomitant audible or vibratory alerts generated upon their receipt make them an ideal mechanism for reaching the party and thus minimizing delay in confirming visitation requests. Thus, according to one aspect of this disclosure, text messaging may be used to confirm a visitation with a resident of a secure facility.

When the system **25** sends reminder messages of upcoming scheduled visits, an SMS Validity Period attribute is preferably used to cancel message delivery and/or suppress display of messages that have not been received or read, respectively, prior to the scheduled start of the visit. Where available, the SMS message cancel feature may be used to cancel a message that already has been delivered, so that the likelihood of preventing display or receipt of messages past their useful or appropriate time period may be increased. According to one aspect of this disclosure, messages are marked with a validity period or expiration date and time, such that notifications for events that have passed or otherwise expired are not delivered or displayed.

When a reminder of an upcoming scheduled visit is sent in advance of the visit, it may take the form of an enhanced message service (EMS) message, and include a vCalendar entry, which, if supported by the telephony terminal, will cause an electronic event entry to be added to the device's calendar. It may also contain a vCard entry, which likewise will cause an electronic contact (e.g., business card) to be added to the terminal's address book. In other words, according to this disclosure, vCalendar or other electronic calendaring data, vCard or other electronic contact information data, may be distributed. If a reminder of an upcoming visit is sent prior to (or immediately prior to) the visit, at a point where one of the pool of numbers has been assigned to the scheduled visit, the message may include a telephone number at which the connection can be established. If supported by the device, the telephone number may be encoded in the SMS Call Back Number field.

Although the systems described herein preferably use one incoming number nationwide to support incoming telephone call visits at any and all facilities using the service, there may be occasions where it is desirable to direct callers to use different numbers. For instance, if any one person has communicated with more than one resident of detention environments using this service, providing a different direct-dial number specifically for each particular visit will serve to streamline connecting the call, by nature of the system expecting the next call to that number to be from the scheduled visitor and the specific resident.

Because it would be prohibitively expensive to maintain one direct-dial number for each resident of the secure facilities **100**, a much smaller pool of unique numbers—enough to cover peak active visits, plus additional numbers as a buffer, may be used. The system temporarily associates one of the direct inward dial (DID) numbers with a particular scheduled call, for the exact duration of the call plus a moderate buffer of time prior to and afterward. During that window of time, only incoming calls with a Caller ID or automatic number identification (ANI) number associated with the account scheduled for the call will actually be connected to the system, except for specified users.

According to another aspect of this disclosure, a message from an outside person may be manually recalled after having been sent. This disclosure is not limited to automated (scheduled) deadlines for deleting messages. For example, where an outside person asks for an electronic visit to occur very soon, but then becomes unavailable (for example, is called into a meeting), that outside person may cancel or change the visit request before the resident of the detention facility sees it.

Because sending an electronic message to the cellular telephone network requires at least one unique ID (typically a mobile telephone number, or sometimes a "short code"), and because these unique IDs are expensive to obtain and maintain, and because using multiple unique IDs for the same service (even if for different purposes) can confuse end-users (because of requiring that multiple address book entries be stored on the device, or multiple numbers for one address book entry), it is preferable to use just one unique ID for all aspects of the service. However, because at least some of the electronic messaging systems (in particular, SMS) do not provide any way to identify which one of several messages the end-user is replying to, a system for uniquely associating end-user replies to a particular query may be required.

According to this disclosure, uniquely associating end-user replies to a particular query can be accomplished by creating one or more random three-digit numbers or keywords to be used as responses by the end-user. The random numbers or keywords may be made to be unique in any rolling

72-hour window, so that multiple threads of requests and responses may be maintained at any one time.

For video visitations using a smart phone as one endpoint of the visit, the text message preferably includes a uniform resource identifier (URI) that is specific to and registered to the application used for visitation, so that the recipient may simply click on a link in the text message to launch the application and initiate the visit. For example, on Apple iOS devices, including the iPhone and iPad, this feature is known as a custom URL scheme. Thus, according to one aspect of this disclosure, a custom Internet address scheme may be configured to launch a specific mobile application with connecting information for a specific video visitation, telephone call, video conference, or other real-time electronic meeting.

Because it is desirable to maintain frequent contact between (1) residents of secure facilities and (2) their friends and family members residing outside such facilities, a system constructed in accordance with this disclosure may keep track of longer-than usual and desired lengths of time between communications, and then automatically generate a proactive reminder, suggesting that a telephone call or video visitation would be helpful. Thus, text messaging may be used to automatically suggest the recipient request a visit with a particular resident whenever a trigger event has occurred, such as when a pre-determined or calculated length of time without visits has elapsed. In addition, messages may be automatically generated when the resident will be unavailable for communications for a period of time. Prior to any text message reminders or requests, however, the system may re-verify that the resident is authorized to interact with the outsider.

FIG. 4 illustrates hardware **400** and other devices that may be employed within the processing center **150**. In a preferred embodiment, each cluster **151**, **152**, **153**, **154**, has a central processing unit **402** for operating the processing node **256**, a touch screen interface **412** and other input-output devices **404**, memory devices, including a hard disk drive **414**, a read-only memory **410** and a random access memory **408**, and a network device **406** for providing communication with other processors and databases within the processing center **150**, including the devices within the applications and database nodes **257**, **258**. In operation, the hardware devices **402**, **406**, **408**, **410**, **412**, **414** may be operated under the control of the CPU **402** via a suitable bus **420**.

While this disclosure provides specific examples and various embodiments, it should be readily understood by those skilled in the art that many modifications and adaptations of the examples and embodiments described herein are possible without departure from the spirit and scope of the invention as claimed hereinafter. Thus, it is to be understood that this disclosure is made only by way of example and not as a limitation on the scope of the invention claimed below.

What is claimed is:

1. A system for originating an electronic communication, said system comprising:
 - a terminal located inside a secure facility, wherein the terminal generates the electronic communication and further comprises an interactive audio/video platform;
 - a processing center comprising:
 - a database for storing data to verify that a resident of the secure facility who originates the electronic communication is authorized to communicate with an intended recipient of the electronic communication, wherein the database stores rehabilitation milestone information established by the secure facility; and
 - a processor that receives the data from the database, and to use the data to verify that the resident is authorized to communicate with the intended recipient, wherein

9

the processor generates an electronic message automatically in response to the rehabilitation milestone information; and

wherein the processing center converts the electronic message from an electronic messaging format to and from a different format suitable for delivery to and from a terminal located inside the secure facility, and wherein the terminal is used by a resident of the secure facility and others confined within the secure facility, and wherein the processing center verifies that the resident of the secure facility is authorized to communicate with the intended recipient; and

wherein the system pushes the electronic communication to the intended recipient only after verifying that the resident is authorized to communicate with the intended recipient.

2. The system of claim 1, where the electronic communication includes a text message, and wherein the system automatically prompts the recipient to request a visit with the resident in response to an occurrence of a time-related trigger event.

3. The system of claim 1, wherein the processor generates messages automatically when the resident will be unavailable for communications for a period of time.

4. The system of claim 1, wherein the database stores monetary threshold information for the resident, and wherein the processor generates a message automatically when an account balance drops below the monetary threshold, the message sent to a non-resident to alert the non-resident of the resident's low-fund balance and that a deposit to the resident is in order.

5. The system of claim 4, wherein the monetary threshold equals a cost of a visit of a specified duration.

6. The system of claim 1, wherein the database stores calendar date information pertaining to the resident, and wherein the processor generates a message automatically based on the calendar date information.

7. The system of claim 1, wherein the electronic communication is marked with a validity period or expiration date and time, such that notifications for events that have passed or expired are not delivered or displayed, or the electronic communication is permitted to be manually recalled or overridden.

10

8. The system of claim 1, wherein the electronic message contains electronic calendar data or contact information data.

9. The system of claim 1, wherein the electronic message contains an Internet address scheme for launching a mobile application with connecting information for a video visitation, telephone call or video conference.

10. A communications method, comprising:

a communications module generating an electronic message from a person outside a detention environment to a resident of the detention environment;

a processing center converting the electronic message from an electronic messaging format to and from a different format suitable for delivery to and from a terminal located inside the detention environment, and wherein the terminal is used by the resident of the detention environment and others confined within the detention environment and subsequently verifying that the resident of the detention environment is authorized to communicate with the person outside the detention environment, the processing center further comprising a database and a processor, the database storing rehabilitation milestone information established by the detention environment, and the processor generating a message automatically in response to the rehabilitation milestone information; and

subsequently, a transmission module transmitting the electronic message to a terminal located in the detention environment, wherein the terminal further comprises an interactive audio/video platform; and

wherein the electronic message refers to a communication for or with the resident of the detention environment.

11. The method of claim 10, wherein the electronic message includes a request for electronic communication between the resident of the detention environment and the person outside the detention environment.

12. The method of claim 10, further comprising a step of permitting the person outside the detention environment to upload photos, audio or videos to an electronic message board pertaining to the resident of the detention environment.

13. The method of claim 10, further comprising a step of using the processing center to provide funds to the resident of the detention environment via an electronic message.

* * * * *



(19) **United States**
(12) **Patent Application Publication**
SHAPIRO

(10) **Pub. No.: US 2013/0179949 A1**
(43) **Pub. Date: Jul. 11, 2013**

(54) **SECURE EXCHANGE OF DIGITAL CONTENT**

Publication Classification

(71) Applicant: **JPay, Inc.**, Miami, FL (US)
(72) Inventor: **Ryan Jacob SHAPIRO**, Bay Harbor Islands, FL (US)

(51) **Int. Cl.**
H04L 29/06 (2006.01)
(52) **U.S. Cl.**
CPC **H04L 63/08** (2013.01)
USPC **726/4**

(73) Assignee: **JPAY, INC.**, Miami, FL (US)

(57) **ABSTRACT**

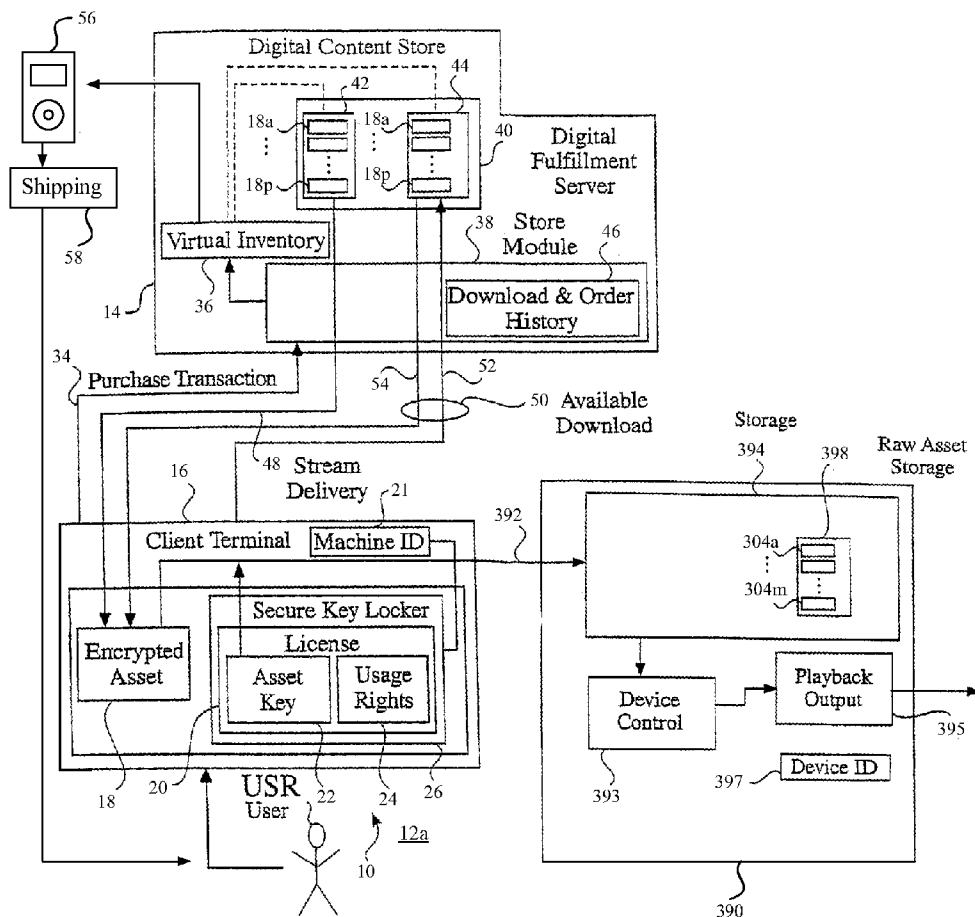
(21) Appl. No.: **13/783,863**

The invention includes delivering and monitoring digital content distributed to correctional facility inmates, giving supervisory authorities the ability to screen the incoming digital content. Digital content can include email, and stored and steamed video content, and can be scanned for keywords by supervisory authorities before delivery to an inmate. A computer kiosk can be used by inmates to view and record digital video content. A portable player is provided to inmates which can be used to play, and in some embodiments record, digital content. The player is issued to a particular inmate, and can only be used with respect to that particular inmate's digital content. The kiosk, and in some embodiments, the player, can be used to shop for items available at a store, for example a commissary.

(22) Filed: **Mar. 4, 2013**

Related U.S. Application Data

(63) Continuation-in-part of application No. 12/814,201, filed on Jun. 11, 2010, which is a continuation-in-part of application No. 11/041,431, filed on Jan. 21, 2005, now abandoned.
(60) Provisional application No. 60/538,933, filed on Jan. 22, 2004.



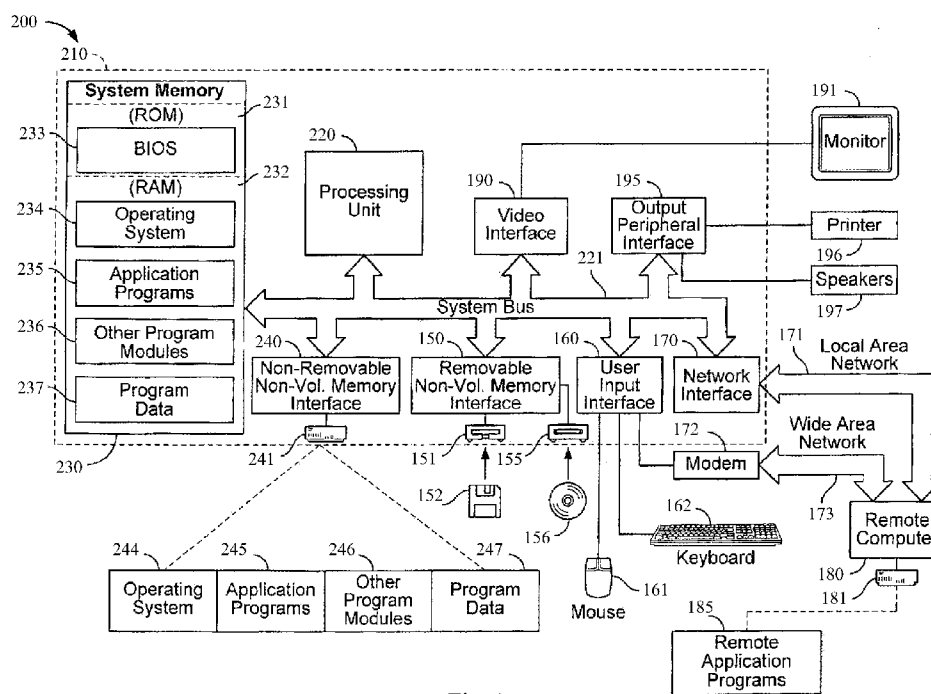


Fig. 1

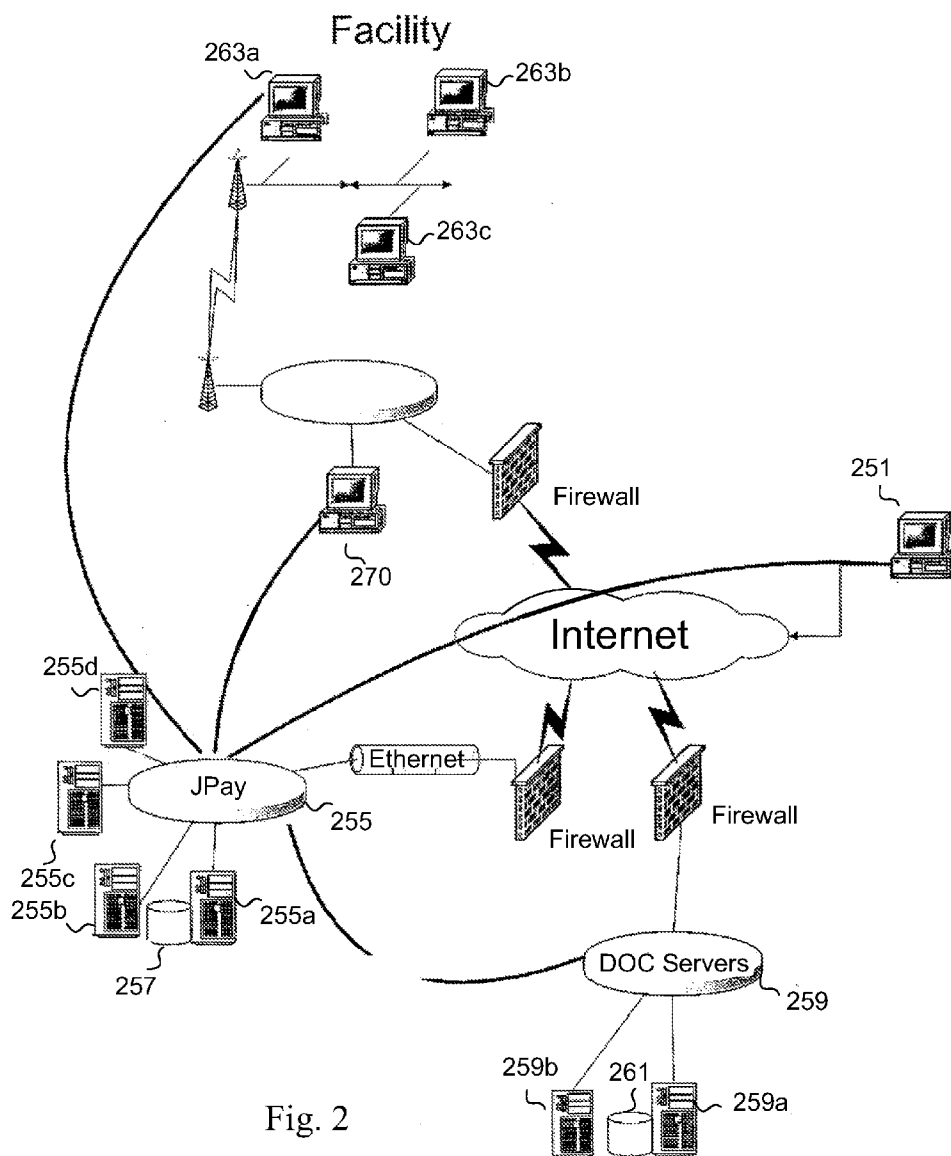


Fig. 2

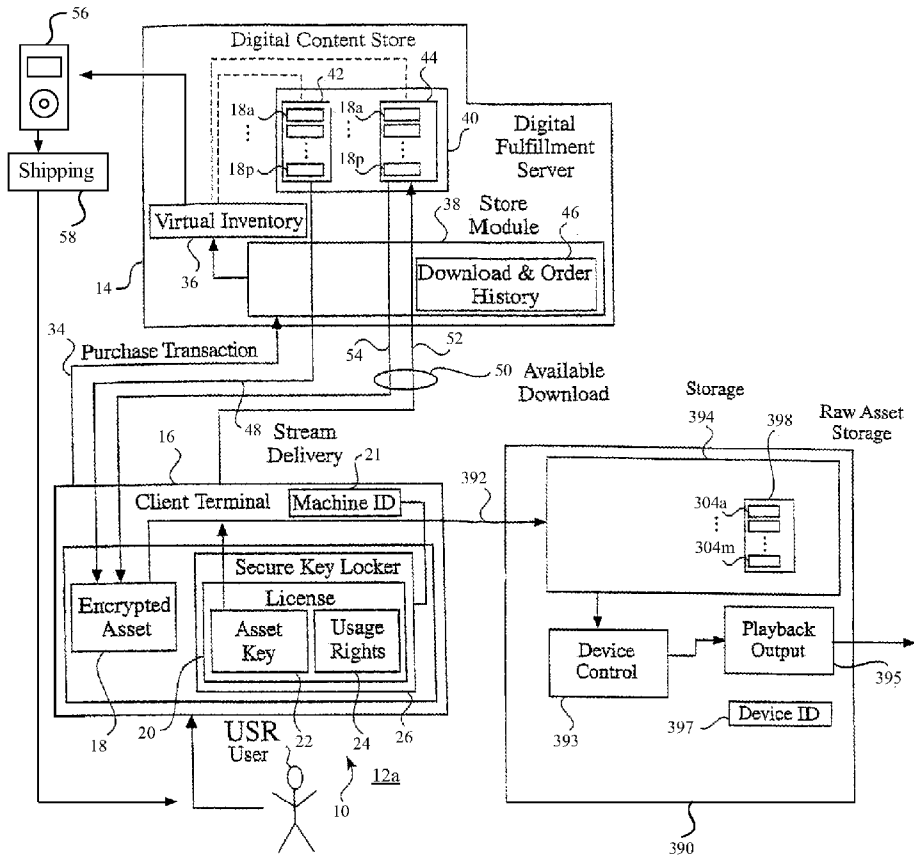


Fig. 3

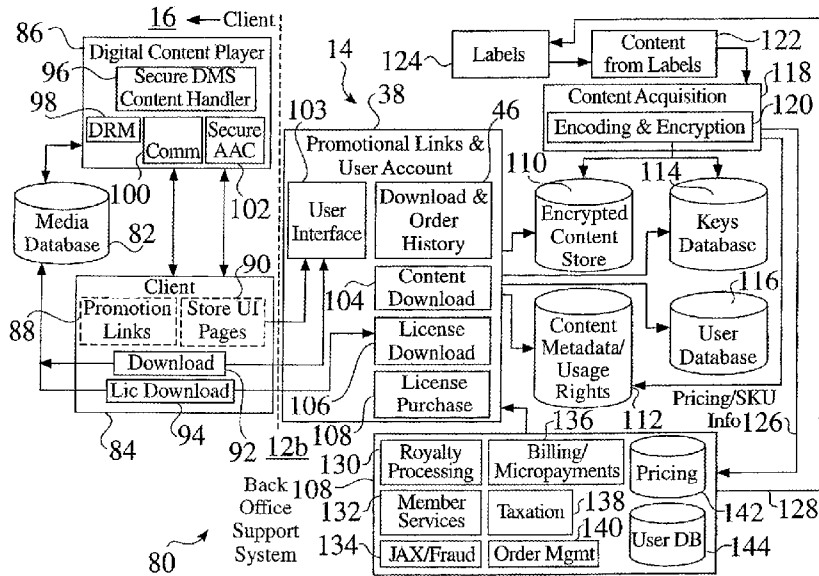


Fig. 4

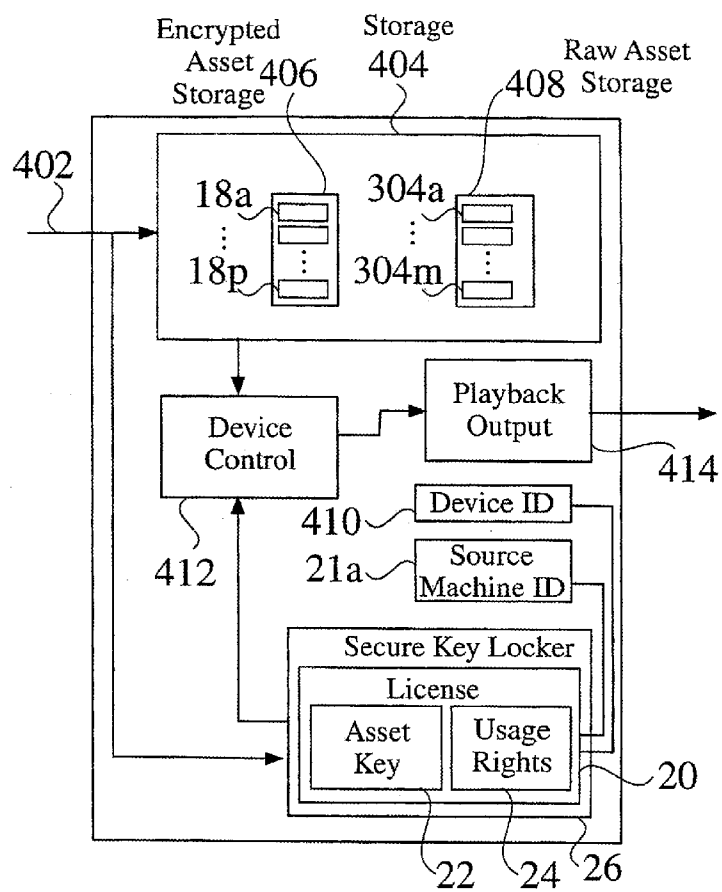


Fig. 5

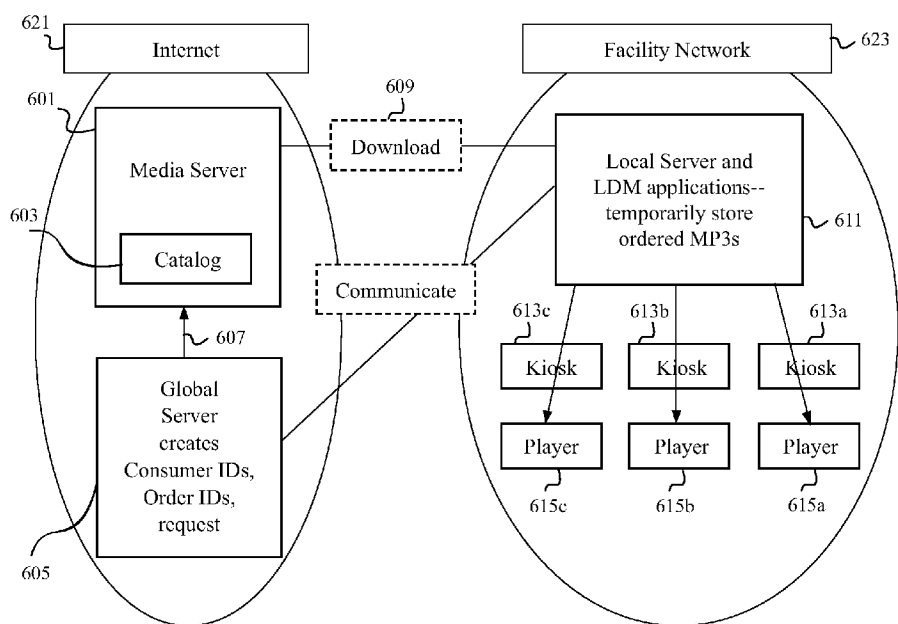


Fig. 6

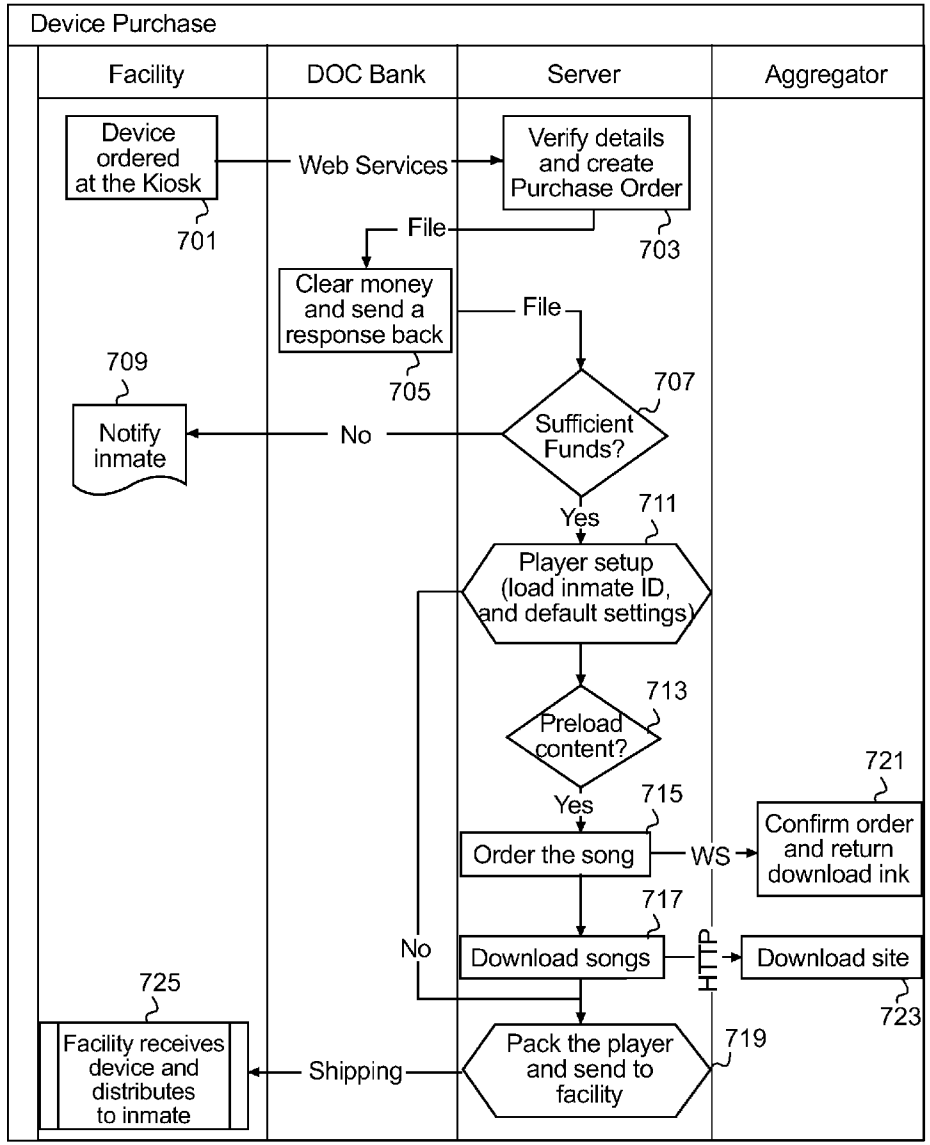


Fig. 7

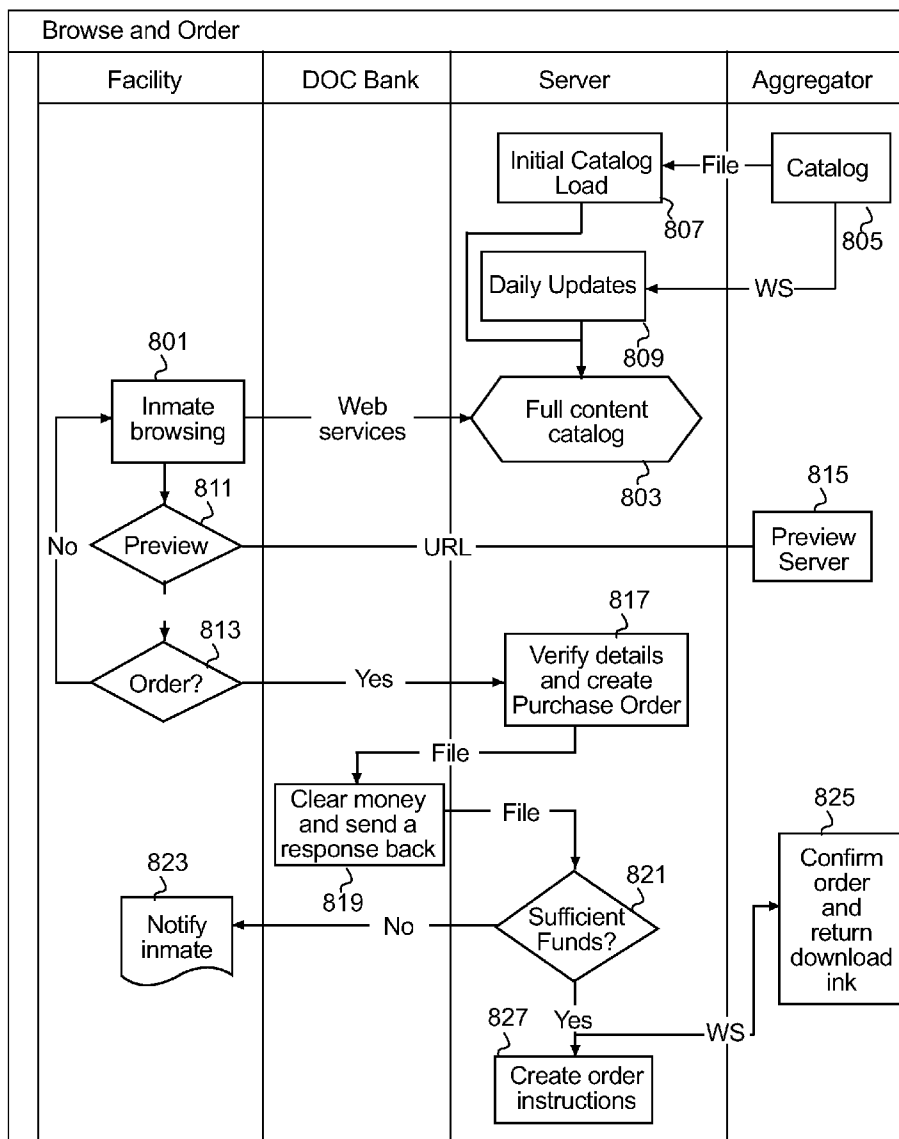


Fig. 8

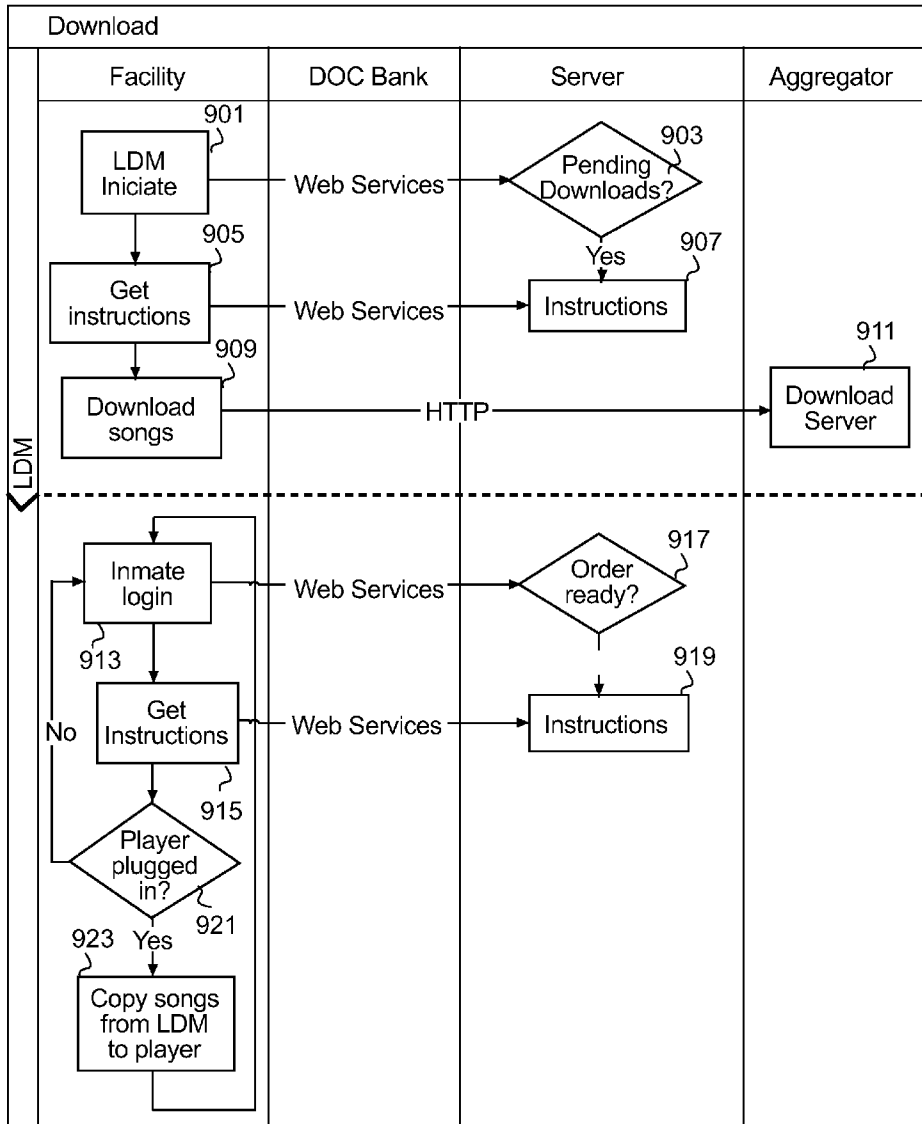


Fig. 9

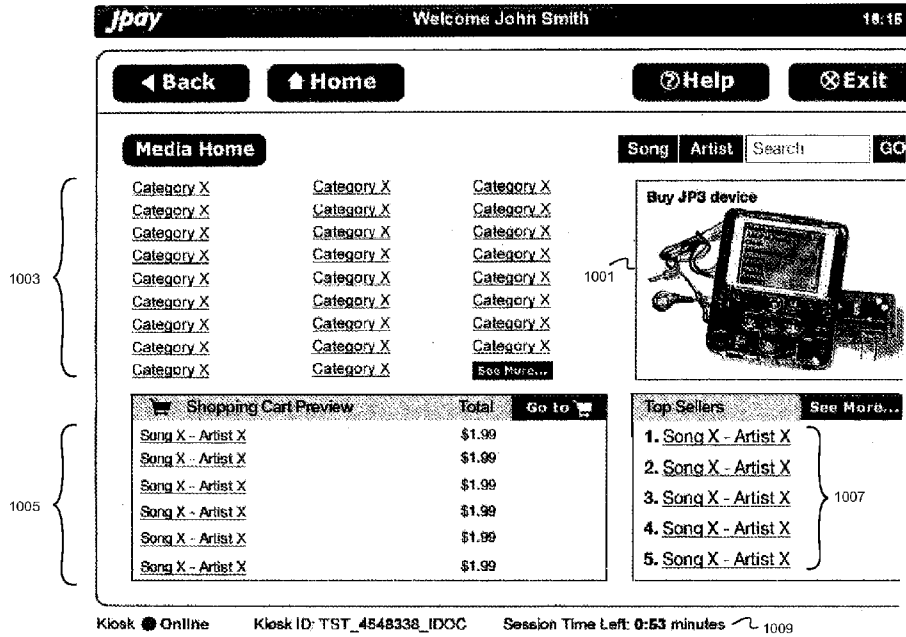


FIG 10

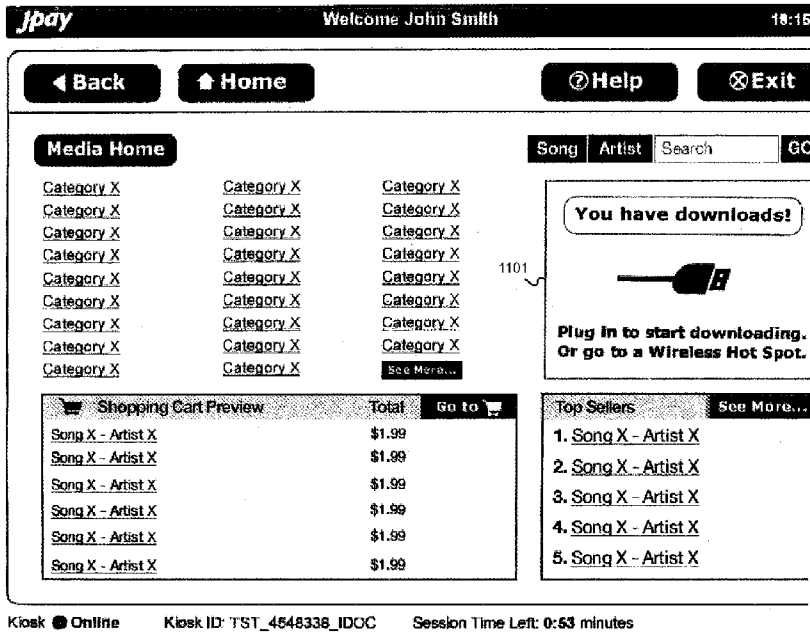


FIG 11

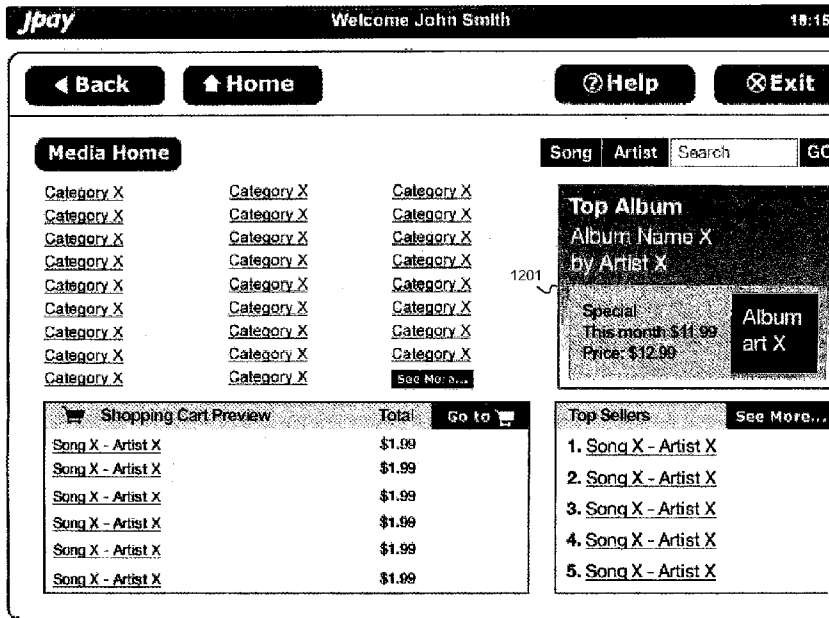
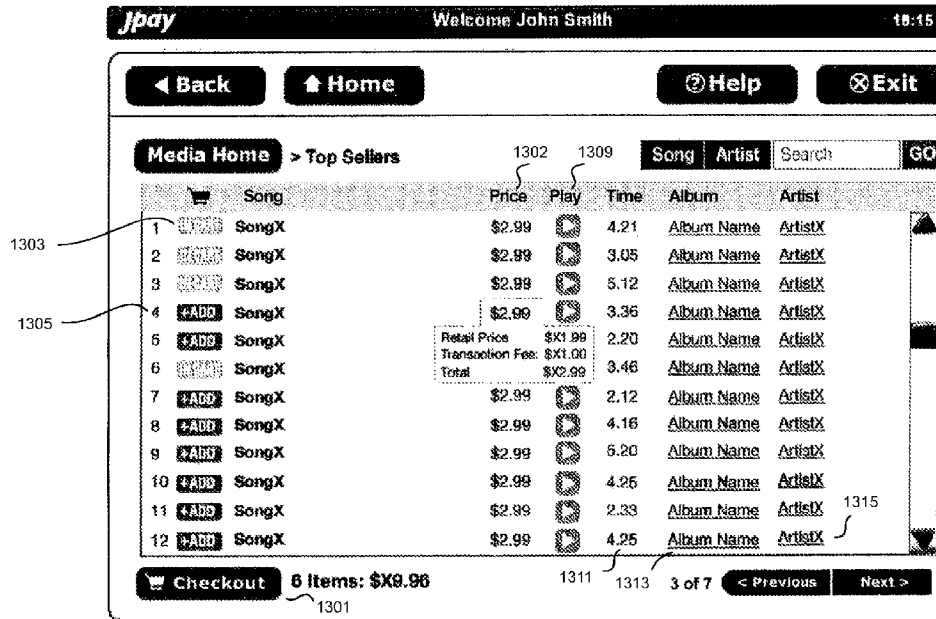


FIG 12

Kiosk Online Kiosk ID: TST_4548338_IDOC Session Time Left: 0:53 minutes

FIG 13



Kiosk Online Kiosk ID: TST_4548338_IDOC Session Time Left: 0:53 minutes

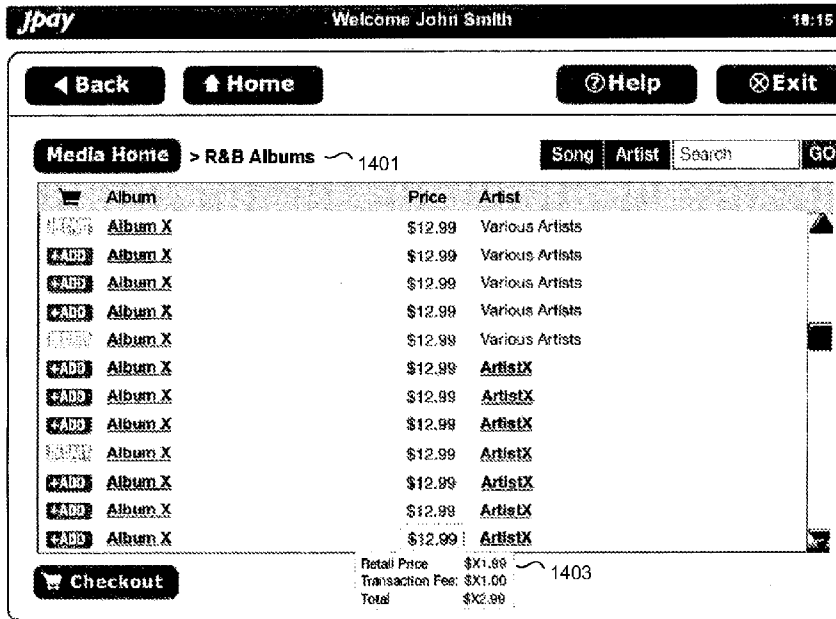


FIG 14

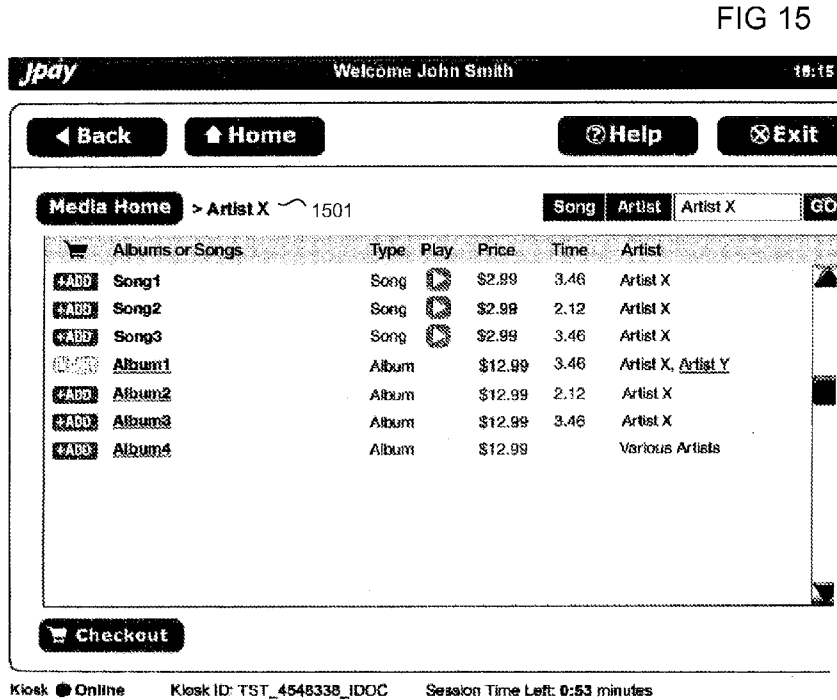


FIG 15

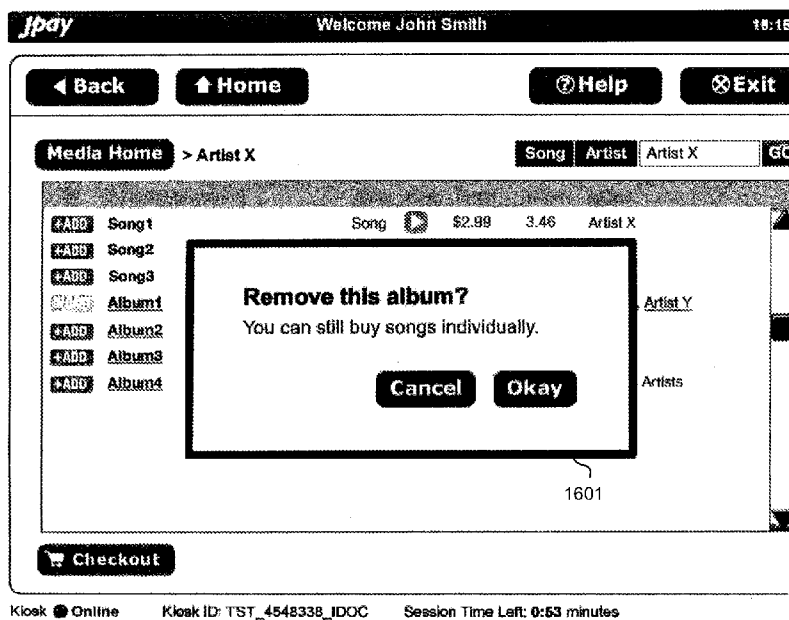


Fig. 16

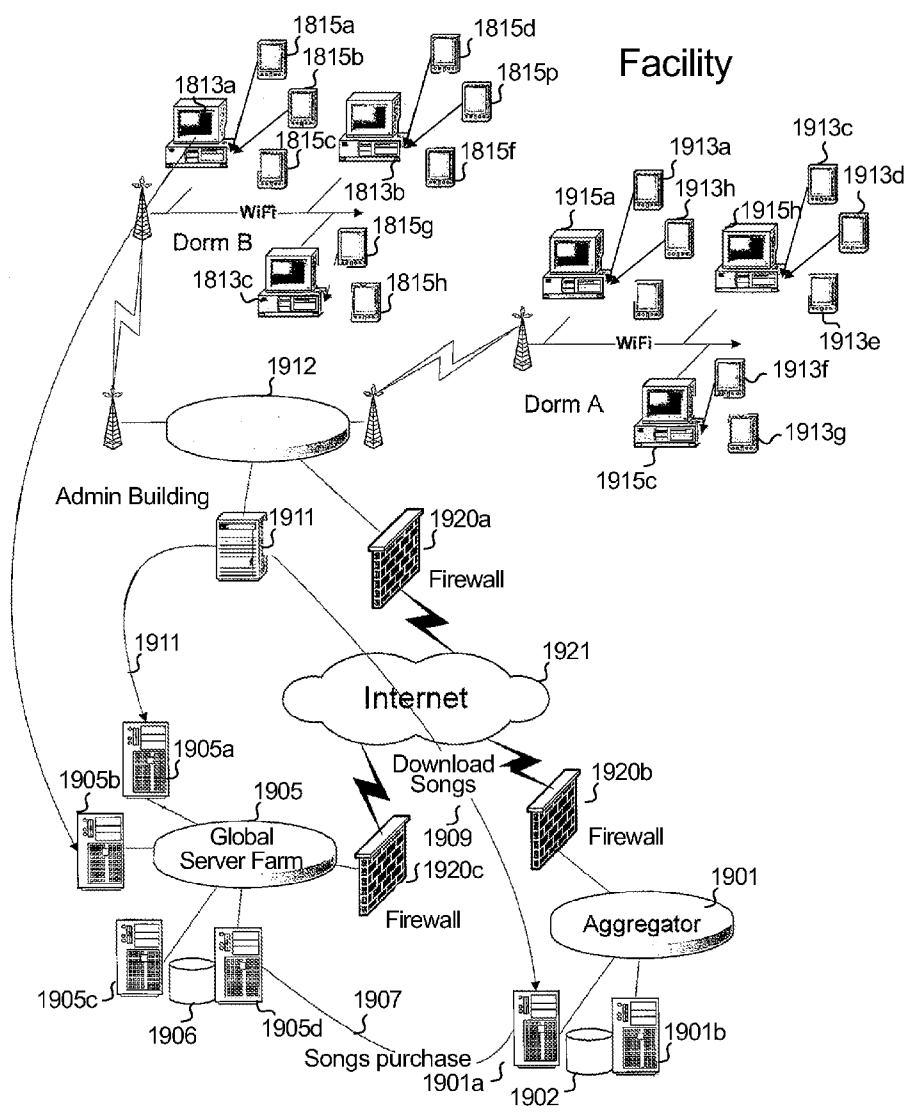
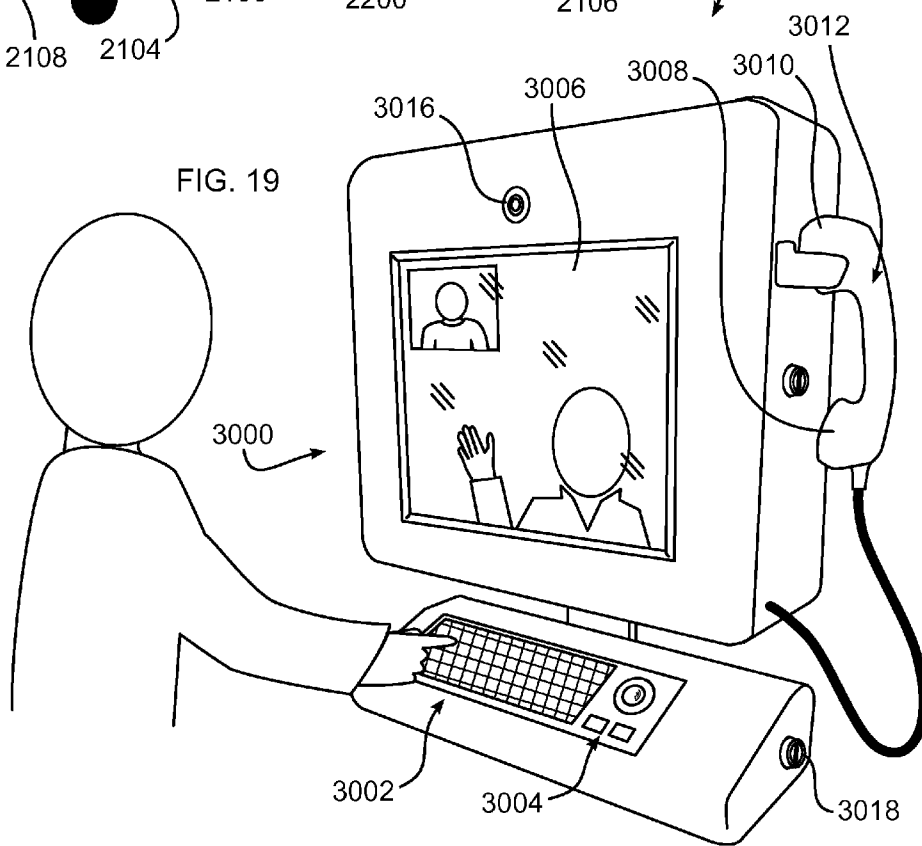
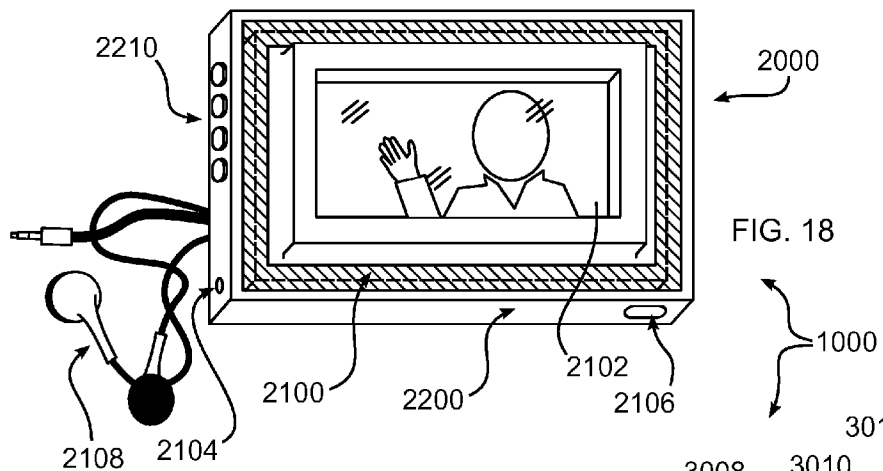


Fig. 17



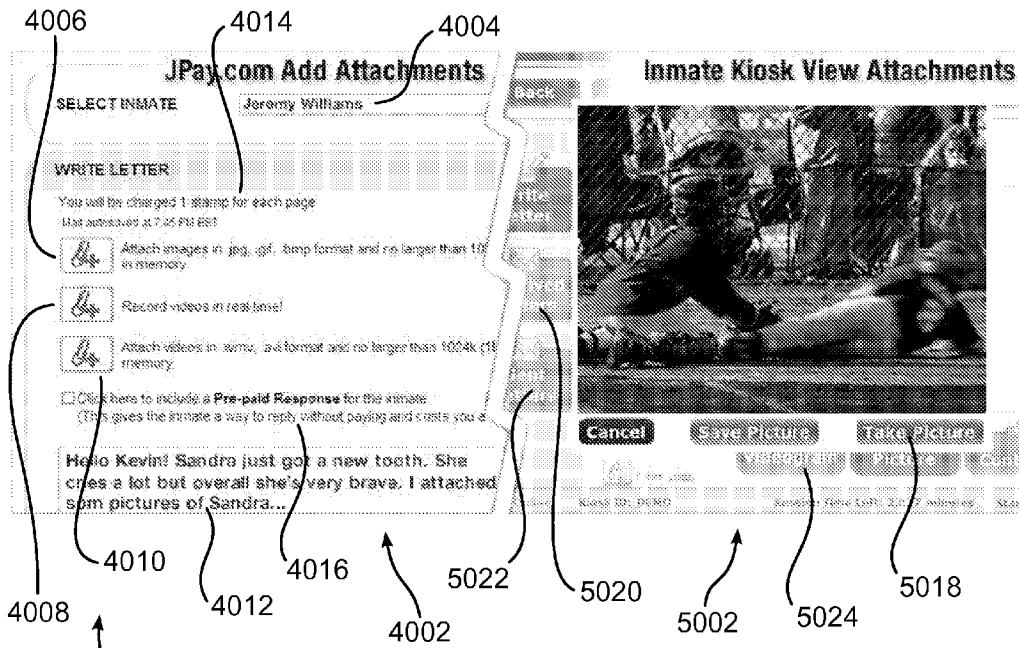
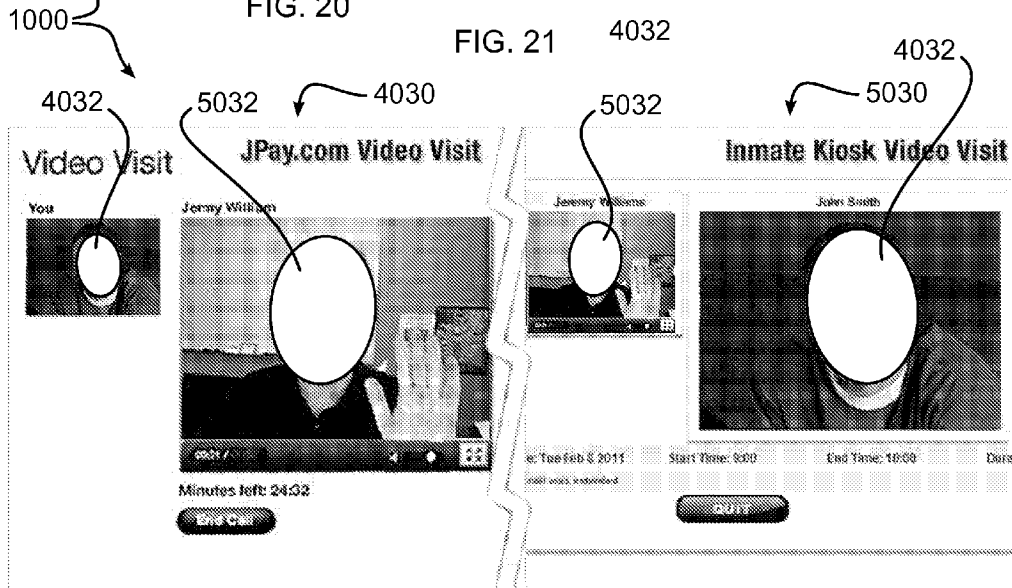


FIG. 20

FIG. 21



4006

4014

4004

4008

4010

4012

4016

4002

5022

5020

5002

5024

5018

1000

4032

4032

4032

5032

4030

5032

5030

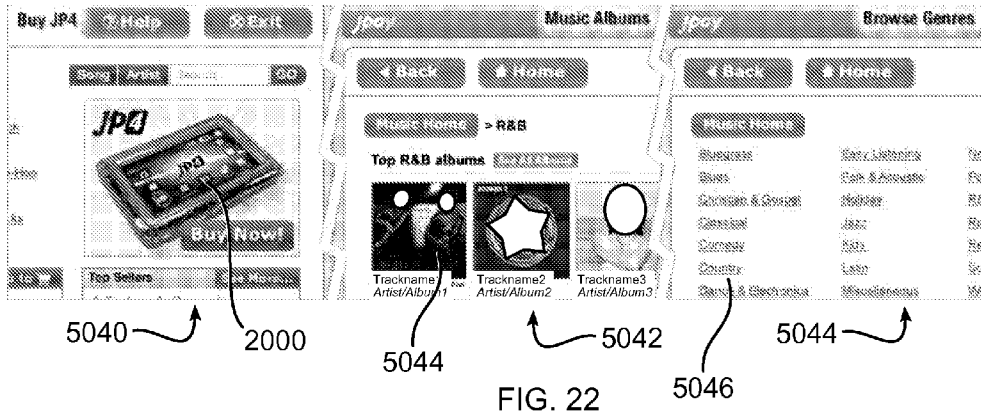


FIG. 22

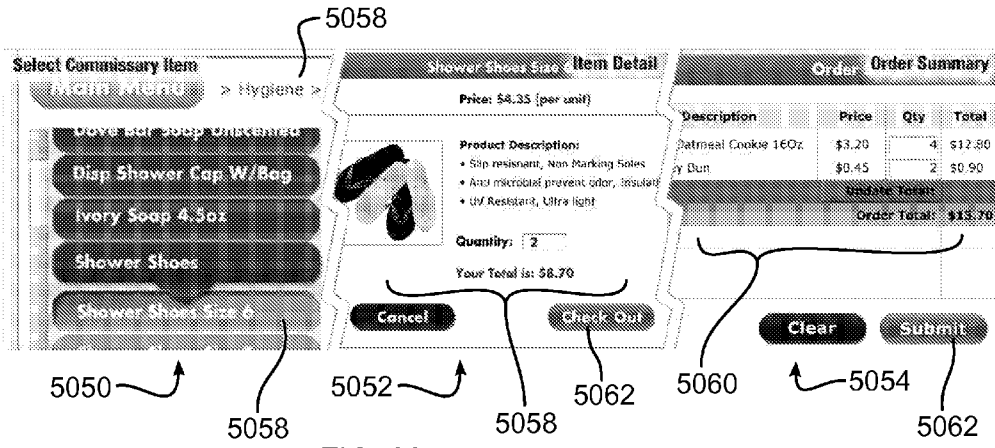


FIG. 23

FIG. 24

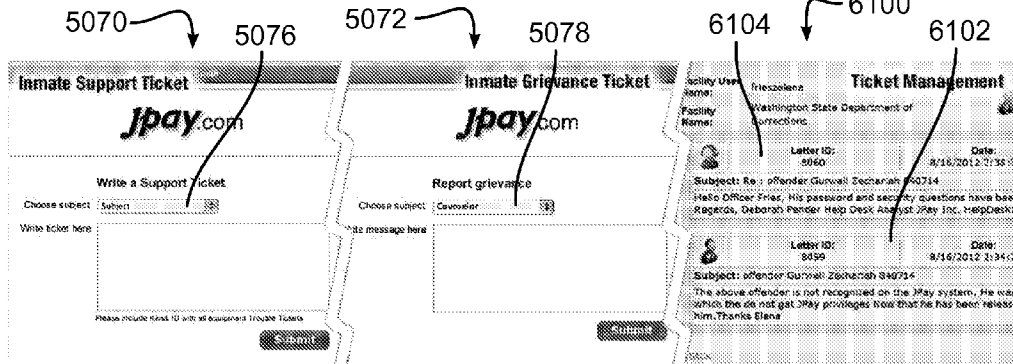


FIG. 25

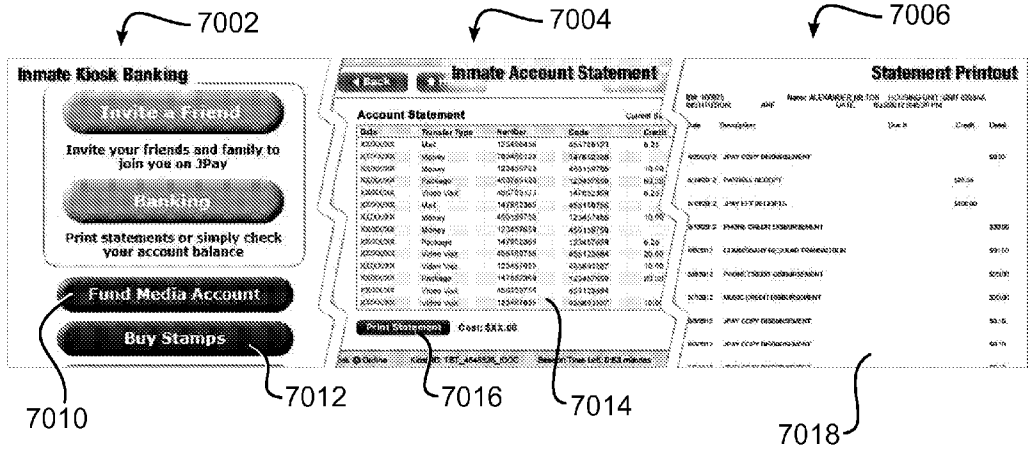
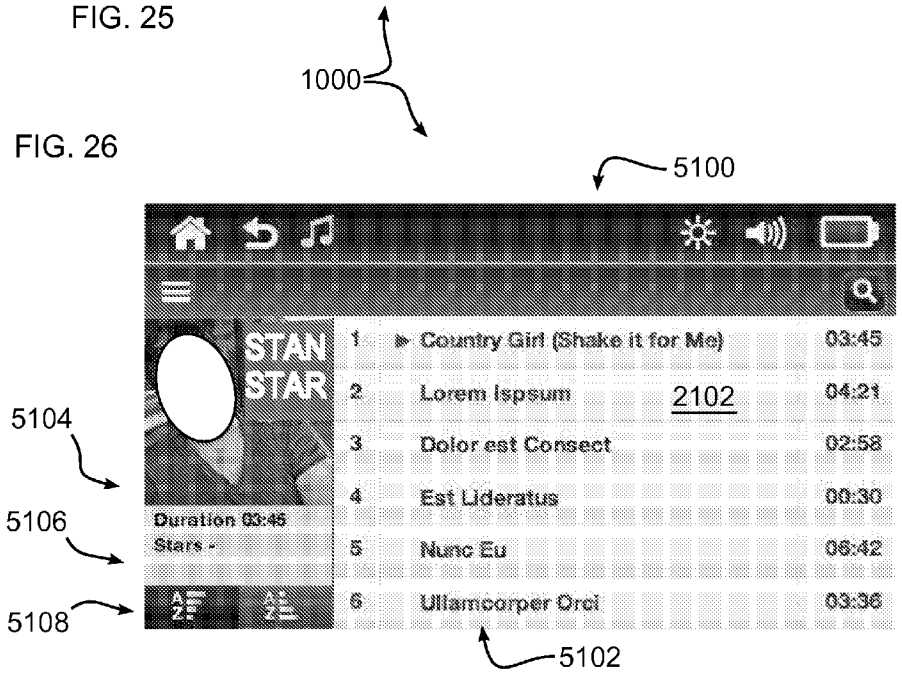


FIG. 25

FIG. 26



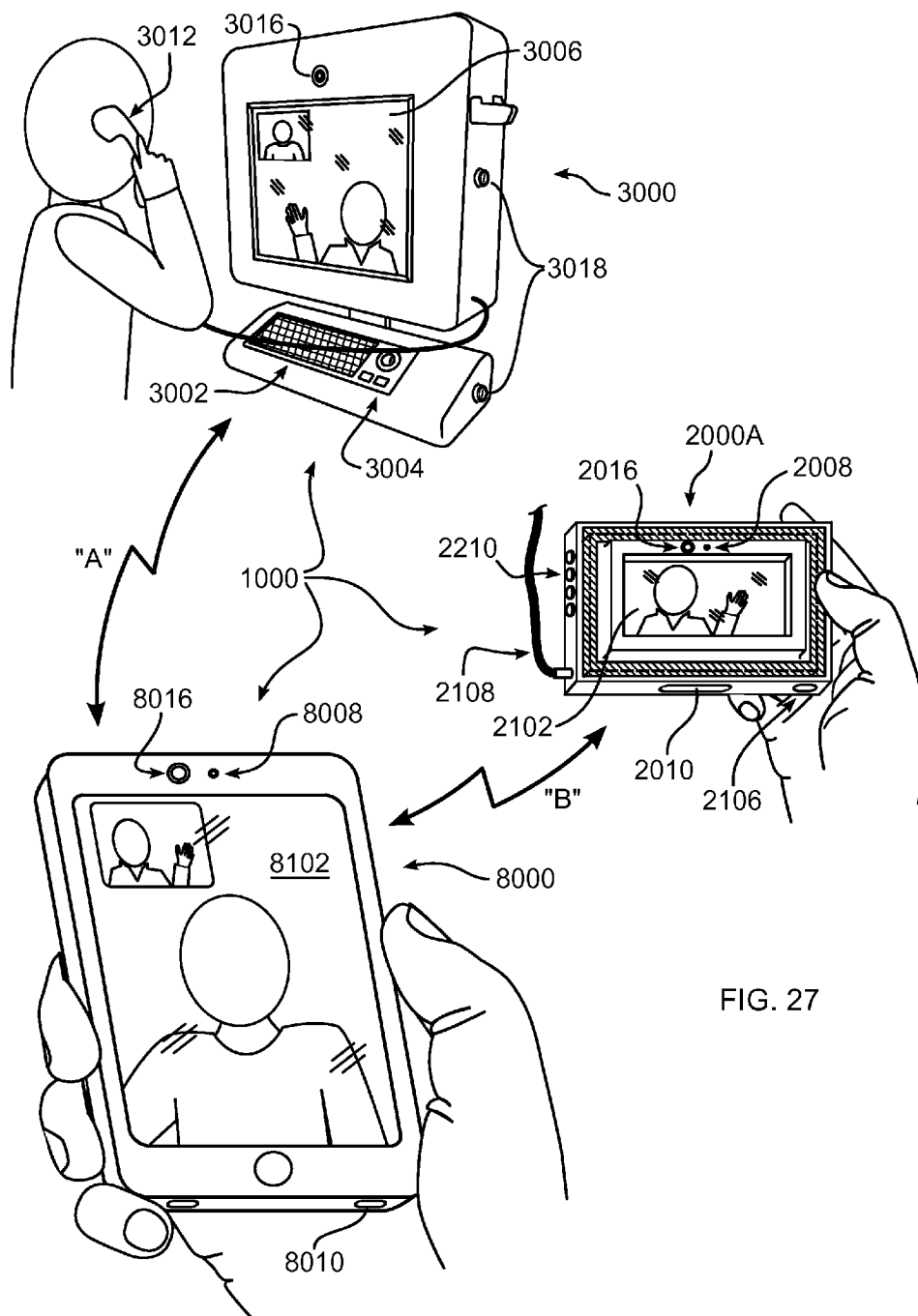


FIG. 27

Facility System
Sign Out

Admin Mail

Welcome WaDCOTest
Last Login: 07/04/2010 10:23AM EST

Letter Delivery Summary for the past 1 Months

Mail

- Letter Delivery
- Mail Reports
- Support Tickets Delivery
- Search
- Inbound Mail Operational Report
- Mail Operational Report
- Stamp Usage Report
- In Mail Discarded Material
- Recover Deleted Letters

Inbound

- Requires Approval (376)**
Click to view letters pending approval
- Ready To Release (24)**
Click to view ready to release and ready to print letters
- Printed (2)**
Click to view and reprint printed letters
- Released (727)**
Click to view released letters
- Sent To I&I (0)**
Click to view and approve letters sent to security
- Returned To Customer (0)**
Click to view letters returned to customers
- Rejected (0)**
Click to view censored letters

Outbound

- Requires Approval (598)**
Click to view letters pending approval
- Ready To Release (88)**
Click to view ready to release letters
- Released (1031)**
Click to view released letters
- Sent To I&I (0)**
Click to view and approve letters sent to security
- Rejected (0)**
Click to view censored letters
- Pending Print Items (52)**
Click to view pending print items
- Printed Items (1349)**
Click to view printed items

FIG. 28

FIG. 29

Facility System
Sign Out

Admin Mail

Welcome WaDCOTest
Last Login: 07/05/2010 10:23AM EST

<<Back | Main | Requires Approval | Pending | Printed | I&I | Returned | Rejected | Released |

Requires Approval (flagged words)

Next Mail > Last Mail >>

Mail

- Letter Delivery
- Mail Reports
- Support Tickets Delivery
- Search
- Inbound Mail Operational Report
- Mail Operational Report
- Stamp Usage Report
- In Mail Discarded Material
- Recover Deleted Letters

Letter ID JPMSL 10813431

Inmate Name : TIMOTHY TISCHLER
Inmate ID : 221083
Housing : H4 H4039L
Date : 07/05/2010 9:04AM EST
Customer : Denna Robinson
Customer ID : 2659730

Suspicious Content : 42 words are in Spanish
Word(s) Found : • Love
Attachment(s) :

Click here to discard letter content. Discarded letters will be saved in the Discarded Material Bucket

- Approve Letter
- Send To Sent To I&I
- Returned To Customer
- Send To Rejected
- Mail History
- Relocate Letter

9512
9514
9516

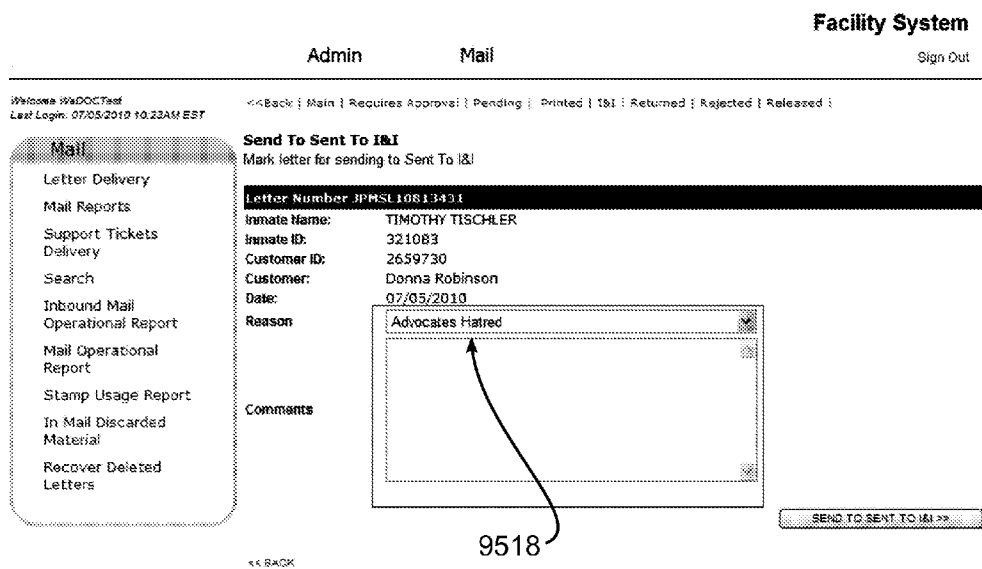


FIG. 30

SECURE EXCHANGE OF DIGITAL CONTENT

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a Continuation in part of U.S. application Ser. No. 12/814,201, filed Jun. 11, 2010, which is a Continuation in part of U.S. application Ser. No. 11/041,431, filed Jan. 21, 2005, now abandoned, which claimed the benefit of U.S. Provisional Application No. 60/538,933, filed Jan. 22, 2004, the contents of all of which are hereby incorporated by reference in their entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to the field of electronic communications. Specifically, the present invention relates to the delivery and access of electronic data by individuals in a restrained environment, such as correctional facility.

BACKGROUND OF INVENTION

[0003] Correction system authorities have found that receiving and distributing inmates' paper mail is a significant challenge. First, correction authorities frequently move inmates between correction facilities such as from a jail (where one is held prior to conviction) to a prison (where one is held after conviction). These movements, often on short notice, play havoc with conventional inmate mail. Conventional letters and other forms of correspondence, written on paper to be delivered to a physical address, are often lost or left "chasing" the inmate for years. This problem frustrates inmates, their families, attorneys and correction authorities.

[0004] Second, correction authorities read inmate mail, a difficult, time consuming and expensive task especially when the mail is handwritten. Opening and reading inmate mail costs the American corrections system over \$100 million per year. Third, correction authorities have no present way of storing and indexing inmate paper mail for later retrieval and analysis. Fourth, correction authorities inspect inmate mail for drugs or other forbidden substances, a difficult, time consuming and expensive task because some inmates may have clever cohorts outside of prison. Furthermore, drugs that remain undetected impose a large but unquantifiable cost on the incarceration system due to their deleterious impact on medical costs and violence. Fifth, as of December 2002, the United States federal, state and local authorities, most of whom are in budget deficit, incarcerated over two million people at a cost of more than \$40 billion per year.

[0005] These challenges are not limited to the delivery of letters. For example, correctional authorities spend more time inspecting packages with gifts to be delivered to inmates than they spend on inspecting letters.

SUMMARY OF THE INVENTION

[0006] In accordance with an embodiment of the disclosure, a system for managing an exchange of digital content between inmates in a correctional facility and non-inmates, comprises at least one computer server having a processor and connected to software stored on non-transitory media, the server software configured to obtain digital content from inmates or non-inmates, store the digital content until a staffperson of the correctional facility approves distribution of the digital content to an intended recipient, and distribute the

digital content to the intended recipient if approved; and at least one inmate device having a processor, a digital display, and controls, the inmate device including software stored on non-transitory media, the device software configured to read stored assignment data pertaining to an inmate authorized to use the particular inmate device executing the device software, connect to the at least one computer server and transmit information pertaining to the inmate authorized to use the particular inmate device executing the device software, obtain approved digital content distributed by the server software and intended for the particular inmate authorized to use the particular inmate device connected to the at least one computer server, and present the digital content.

[0007] In various embodiments thereof, the server software is further configured to analyze the digital content to create a result set of keywords in the digital content; report the result set to a staffperson of the correctional facility; the digital content is video content; the digital content is streaming audio content, the digital audio content stored by the server software for a delay period sufficient to enable correctional facility staff to monitor and interrupt the stream if non-authorized content is streamed; the digital content is streaming video content, the digital video content stored by the server software for a delay period sufficient to enable correctional facility staff to monitor and interrupt the stream if non-authorized content is streamed.

[0008] In another embodiment thereof, the inmate device software is further configured to: obtain information pertaining to commissary items available for sale from the at least one server; and enable an inmate to select and request items from the obtained information, using the inmate device.

[0009] In a yet further embodiment thereof, the inmate device software is further configured to: obtain information pertaining to digital content available for downloading into the inmate device; enable an inmate to select and request digital content for downloading; and connect to the at least one server to obtain the digital content.

[0010] In other variations thereof, the inmate device software is further configured to allocate credits assigned to the inmate to pay a cost of obtaining the digital content; the inmate device is configured to only carry out an exchange of digital content with at least one of the at least one server; and the inmate device is configured to be unopenable by an inmate without using tools.

[0011] In another embodiment of the disclosure, a system for managing an exchange of digital content between inmates in a correctional facility and non-inmates, comprises at least one computer server having a processor and connected to software stored on non-transitory media, the server software configured to obtain digital video content from inmates or non-inmates, delay distribution of at least a portion of the digital video content until a staffperson of the correctional facility approves transmission of the at least a portion of the digital video content to an intended recipient, and distribute the digital video content to the intended recipient if approved; and at least one inmate device having a processor, a digital display, and controls, the inmate device including software stored on non-transitory media, the device software configured to read stored assignment data pertaining to an inmate authorized to use the particular inmate device executing the device software, connect to the at least one computer server and transmit information pertaining to the inmate authorized to use the particular inmate device executing the device software, obtain the distributed digital video content distributed

by the server software and intended for the particular inmate authorized to use the particular inmate device connected to the at least one computer server, and present the video digital content.

[0012] In various embodiments thereof, the server software is further configured to analyze the video digital content to create a result set of keywords in the digital content; the server software is further configured to report the result set to a staffperson of the correctional facility; the delay is sufficient to enable correctional facility staff to monitor and interrupt the video digital content if the digital video content contains non-authorized content; the digital content is streaming video content, the digital video content stored by the server software for a delay period sufficient to enable correctional facility staff to monitor and interrupt the stream if non-authorized content is streamed.

[0013] In an embodiment thereof, the inmate device software is further configured to: display information pertaining to commissary items available for sale from the at least one server; and enable an inmate to select and request items from the obtained information, using the inmate device.

[0014] In another embodiment thereof, the inmate device software is further configured to: obtain visual information pertaining to digital content available for downloading into the inmate device; enable an inmate to view, select and request digital content for downloading; connect to the at least one server to obtain the digital content.

[0015] In a yet further embodiment, the inmate device software is further configured to allocate credits assigned to the inmate to pay a cost of obtaining the digital content.

[0016] In a further embodiment of the disclosure, a method for managing an exchange of digital content between inmates in a correctional facility and non-inmates, comprises using at least one computer server having a processor and connected to software stored on non-transitory media, the server software configure to obtain digital video content from inmates or non-inmates, delay distribution of at least a portion of the digital video content until a staffperson of the correctional facility approves transmission of the at least a portion of digital video content to an intended recipient, and distribute the digital video content to the intended recipient if approved; and providing to at least one inmate a device having a processor, a digital display, and controls, the inmate device including software stored on non-transitory media, the device software configured to read stored assignment data pertaining to an inmate authorized to use the particular inmate device executing the device software, connect to the at least one computer server and transmit information pertaining to the inmate authorized to use the particular inmate device executing the device software, obtain the distributed digital video content distributed by the server software and intended for the particular inmate authorized to use the particular inmate device connected to the at least one computer server, and present the video digital content.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] The accompanying figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views, and which together with the detailed description below are incorporated in and form part of the specification, serve to further illustrate various embodiments and to explain various principles and advantages all in accordance with the present disclosure, in which:

[0018] FIG. 1 illustrates an exemplary computing environment that may be used to implement a server in accordance with an embodiment of the present invention;

[0019] FIG. 2 illustrates a system in for routing electronic correspondence accordance with one embodiment of the present invention;

[0020] FIG. 3 illustrates a communications environment which may be used to deliver digital content in accordance with one embodiment of the present invention;

[0021] FIG. 4 illustrates a client and server architecture that may be used to implement a digital content store system in accordance with one embodiment of the present invention;

[0022] FIG. 5 illustrates a functional block diagram of a digital music player;

[0023] FIG. 6 illustrates a system for delivery of digital content in accordance with one embodiment of the present invention;

[0024] FIG. 7 illustrates the processing of a purchase order for a content player using a kiosk application in accordance with one embodiment of the present invention;

[0025] FIG. 8 illustrates a process for ordering and browsing content through a kiosk application in accordance with one embodiment of the present invention;

[0026] FIG. 9 illustrates content download processes in accordance with one embodiment of the present invention;

[0027] FIGS. 10-16 illustrate screenshots displayed by a kiosk terminal to allow a user to browse and purchase content and a content player in accordance with one embodiment of the present invention;

[0028] FIG. 17 illustrates a system for delivery of digital content in accordance with another embodiment of the present invention;

[0029] FIG. 18 illustrates a portable player in accordance with the disclosure, operative to securely present digital content;

[0030] FIG. 19 illustrates a user kiosk in accordance with the disclosure, operative to securely present and create digital content;

[0031] FIG. 20 illustrates an email application of the disclosure, executable upon an embodiment of a player or kiosk of the disclosure;

[0032] FIG. 21 illustrates a video stream between a web app and a local app of the disclosure;

[0033] FIG. 22 depicts three display images of a local executable application of the disclosure, illustrating an offer to purchase a player, or music;

[0034] FIG. 23 illustrates three display images of a local executable application of the disclosure, illustrating purchase of supplies from a local commissary;

[0035] FIG. 24 illustrates two display images of a local executable application, and a single display image of an administrative application of the disclosure, illustrating support and grievance reporting and administration;

[0036] FIG. 25 illustrates three display images of a banking system application of the disclosure;

[0037] FIG. 26 illustrates a screen image of music playing software of the disclosure;

[0038] FIG. 27 depicts applications of the disclosure in use between an outside user using a cellphone, and a kiosk and a player of the disclosure;

[0039] FIG. 28 depicts a display generated by an admin app of the disclosure, for administrating email;

[0040] FIG. 29 depicts a screen image generated by the admin app of FIG. 28, for approval of digital content; and

[0041] FIG. 30 depicts a screen image generated by the admin app of FIG. 28, illustrating a disposition of digital content.

DETAILED DESCRIPTION OF THE INVENTION

[0042] As required, detailed embodiments are disclosed herein; however, it is to be understood that the disclosed embodiments are merely examples and that the systems and methods described below can be embodied in various forms. Therefore, specific structural and functional details disclosed herein are not to be interpreted as limiting, but merely as a basis for the claims and as a representative basis for teaching one skilled in the art to variously employ the present subject matter in virtually any appropriately detailed structure and function. Further, the terms and phrases used herein are not intended to be limiting, but rather, to provide an understandable description of the concepts.

[0043] The terms “a” or “an”, as used herein, are defined as one or more than one. The term plurality, as used herein, is defined as two or more than two. The term another, as used herein, is defined as at least a second or more. The terms “including” and “having,” as used herein, are defined as comprising (i.e., open language). The term “coupled,” as used herein, is defined as “connected,” although not necessarily directly, and not necessarily mechanically.

[0044] In accordance with the disclosure, a system and method for reducing inmate mail costs, eliminating the problems associated with an inmate’s conventional physical address, improving delivery speed, eliminating drug and forbidden substance smuggling, and allowing better recordkeeping of incoming packages is provided.

[0045] This description and the annexed drawings set forth in detail certain illustrative aspects of the invention. These aspects are indicative, however, of but a few of the various ways in which the principles of the disclosure may be employed, and the present disclosure is intended to include all such aspects and their equivalents. Other advantages and novel features of the invention will become apparent from the following detailed description of the invention when considered in conjunction with the drawings.

[0046] In accordance with one aspect of the disclosure, one or more databases, residing in one or more servers, may be used as repositories of electronic data to be delivered to individuals, for example inmates, in a constrained environment and/or restricted-access location, such as a jail, prison, or other correctional facility. One aspect of the invention involves delivering and monitoring electronic letters to correctional facility inmates while giving supervisory authorities the ability to screen the incoming mail. This may be achieved by providing a database having an entry for each inmate and having a plurality of fields, wherein the fields include inmate name, correction system identification code, inmate identification code, correction system facility code, wherein the facility code maps to a specific corrections facility; and by scanning an original letter to produce an electronic letter and storing each electronic letter sent to a specific inmate in a relational database management system (RDMS) table, wherein the RDMS table includes fields for inmate name, inmate identification number and lists of corrections facilities.

[0047] In another aspect of the disclosure, a computer-operated kiosk, such as a walk-up or other workstation for multiperson use, may be used by individuals (e.g., inmates) in a restrained environment/restricted-access location (e.g., a

prison) to browse through a catalog of available digital media, such as music, to compose outgoing mail, to conduct video visitation, or to create prerecorded videograms, all as described further herein. They may purchase the digital media, for example, with credits earned based on work performed, or bought through some other means, for example with money deposited by family members of the inmate. The kiosk may include means for limiting access to the operating system or other modules in the kiosk computer so that inmates are blocked from accessing other machines with sensitive information that may be connected to the kiosk computer. After the user has browsed the catalog of digital content or media, selected the desired content (e.g., songs) and paid for the same, the purchased content may be downloaded to a digital content player device. The digital content player device may also be used to display digital media of any type, including digital correspondence, to inmates.

[0048] The present disclosure may be implemented in one or more servers, one or more client devices, including computer terminals or portable client devices, or a combination thereof. The data to be accessed by end users in a restrained environment may be stored in one or more databases.

[0049] An exemplary computing device for implementing a server is illustrated in FIG. 1. For example, the computing environment illustrated in FIG. 1 may be used to implement a database server, an email server, a DNS server, a POP/IMAP server, a digital fulfillment server, a media server, a local server, a global server, etc.

[0050] FIG. 1 illustrates an example of a suitable computing system environment 200 on which features of the disclosure may be implemented. The computing system environment 200 is only one example of a suitable computing environment and is not intended to suggest any limitation as to the scope of use or functionality of the disclosure. Neither should the computing environment 200 be interpreted as having any requirement relating to any one or combination of components illustrated in the exemplary operating environment 200.

[0051] The disclosure is operational with numerous other computing system environments or configurations. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the disclosure include, but are not limited to, personal computers, server computers, hand-held or laptop devices, smartphones, multi-processor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0052] The disclosure may be described in the general context of computer-executable instructions, such as program modules, being executed by one or more computing devices. Generally, program modules include routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types. The disclosure may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices.

[0053] With reference to FIG. 1, an exemplary system that may be used for implementing the disclosure includes a computing device 210 which may be used for implementing a

server. Components of computing device 210 may include, but are not limited to, a processing unit 220, a system memory 230, and a system bus 221 that couples various system components including the system memory to the processing unit 220. The system bus 221 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnect (PCI) bus also known as Mezzanine bus.

[0054] Computing device 210 typically includes a variety of computer readable media. Computer readable media may be defined as any available media that can be accessed by computing device 210 and includes both volatile and non-volatile media, removable and non-removable media. By way of example, and not limitation, computer readable media may include computer storage media. Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by computing device 210. Combinations of the any of the above should also be included within the scope of computer readable media.

[0055] The system memory 230 may include computer storage media in the form of volatile and/or nonvolatile memory such as read only memory (ROM) 231 and random access memory (RAM) 232. A basic input/output system 233 (BIOS), containing the basic routines that help to transfer information between elements within computing device 210, such as during start-up, is typically stored in ROM 231. RAM 232 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 220. By way of example, and not limitation, FIG. 1 illustrates operating system 234, application programs 235, other program modules 236, and program data 237.

[0056] The computing device 210 may also include other removable/non-removable, volatile/nonvolatile computer storage media. By way of example only, FIG. 1 illustrates a hard disk drive 240 that reads from or writes to non-removable, nonvolatile magnetic media, a magnetic disk drive 151 that reads from or writes to a removable, nonvolatile magnetic disk 152, and an optical disk drive 155 that reads from or writes to a removable, nonvolatile optical disk 156 such as a CD ROM or other optical media. Other removable/non-removable, volatile/nonvolatile computer storage media that can be used in the exemplary operating environment include, but are not limited to, magnetic tape cassettes, flash memory cards, digital versatile disks, digital video tape, solid state RAM, solid state ROM, and the like. The hard disk drive 241 is typically connected to the system bus 221 through a non-removable memory interface such as interface 240, and magnetic disk drive 151 and optical disk drive 155 are typically

connected to the system bus 221 by a removable memory interface, such as interface 150.

[0057] The drives and their associated computer storage media discussed above and illustrated in FIG. 1, provide storage of computer readable instructions, data structures, program modules and other data for the computing device 210. In FIG. 1, for example, hard disk drive 241 is illustrated as storing operating system 244, application programs 245, other program modules 246, and program data 247. Note that these components can either be the same as or different from operating system 234, application programs 235, other program modules 236, and program data 237. Operating system 244, application programs 245, other program modules 246, and program data 247 are given different numbers here to illustrate that, at a minimum, they are different copies. A user may enter commands and information into the computer 20 through input devices such as a keyboard 162 and pointing device 161, commonly referred to as a mouse, trackball or touch pad. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 220 through a user input interface 160 that is coupled to the system bus, but may be connected by other interface and bus structures, such as a parallel port, game port or a universal serial bus (USB). A monitor 191 or other type of display device may also be connected to the system bus 221 via an interface, such as a video interface 190. In addition to the monitor, computers may also include other peripheral output devices such as speakers 197 and printer 196, which may be connected through an output peripheral interface 195.

[0058] The computing device 210 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 180. The remote computer 180 may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the computing device 210, although only a memory storage device 181 has been illustrated in FIG. 1. In one embodiment of the present disclosure this computer 180 may be used to implement a kiosk for delivering digital media to an inmate or as a terminal for displaying correspondence to an inmate. The logical connections depicted in FIG. 1 include a local area network (LAN) 171 and a wide area network (WAN) 173, but may also include other networks. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

[0059] When used in a LAN networking environment, the computing device 210 is connected to the LAN 171 through a network interface or adapter 170. When used in a WAN networking environment, the computer 210 typically includes a modem 172 or other means for establishing communications over the WAN 173, such as the Internet. The modem 172, which may be internal or external, may be connected to the system bus 221 via the user input interface 160, or other appropriate mechanism. In a networked environment, program modules depicted relative to the computing device 210, or portions thereof, may be stored in the remote memory storage device. By way of example, and not limitation, FIG. 1 illustrates remote application programs 185 as residing on memory device 181. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0060] The present disclosure includes one or more databases, residing in one or more servers, which may be used as repositories of electronic data to be delivered to individuals in a restrained environment and/or restricted-access location, such as inmates. In general, a typical database is an organized collection of information structured such that a computer program, for example, can quickly search and select data. Traditionally, data stored within a database is organized via one or more tables, wherein respective tables comprise sets of records and a record comprises a set of fields. Records are commonly indexed as rows within a table and the record fields are commonly indexed as columns such that a row/column pair can reference particular datum within a table.

[0061] The database systems in accordance with embodiments of the present disclosure are not limited to relational database systems and organizing information in tables, although the disclosure will be described with respect to the usage of tables. For example, a database system in accordance with the present disclosure may generally store data in one or more data containers, each container potentially including one or more records, and the data within each record potentially being organized into one or more fields. In the context of relational database systems, these containers may be referred to as tables, the records may be referred to as rows, and the fields may be referred to as columns. In the context of object oriented databases, the data containers may be referred to as object classes, the records may be referred to as objects, and the fields may be referred to as attributes. A person of ordinary skill in the art would recognize that other database architectures may use other terminology. For the purpose of explanation of the disclosure, the examples and the terminology used herein shall be that typically associated with relational databases. Thus, the terms “table”, “row” and “column” shall be used herein to refer respectively to the data container, record, and field. The present disclosure is not limited to any particular type of data container or database architecture.

[0062] A database server, in accordance with the present disclosure, retrieves and manipulates data in response to receiving a database statement conforming to a database language, such as for example, Structured Query Language (SQL). The database statement may specify a query operation, a data manipulation operation, or a combination thereof. A database statement that specifies a query operation is referred to herein as a query. The present disclosure is not limited to database statements that specify a particular type of operation. Database security mechanisms to restrict or expand access to a database have been described in U.S. Pat. No. 7,346,617 to Wong, incorporated herein by reference, and U.S. Pat. No. 7,661,141 to Dutta et al., incorporated herein by reference. One function of a database server in accordance with the present disclosure is to control access to database data.

[0063] FIG. 2 illustrates a system in accordance with one embodiment of the present disclosure for routing electronic correspondence, such as letters and mail, to correction facility inmates that eliminates the delays, costs and risks associated with the current correction facility paper or hard copy mail system. The system and method of the disclosure routes letters and other digital correspondence by using, for example, a table in database 257 that indicates the inmate's name, correction system code, inmate identification code and facility location code. Correctional facility staff can print the digital content using a printing device connected to a computer, or can view the digital content using an electronic display device

such as a personal computer or a visual display terminal (263a, 263b, 263c), while enabling supervisors to screen the incoming digital content using a computer terminal 270. One or more walk-up kiosks or terminals 263a, 263b can be provided for inmates to access preapproved digital content.

[0064] Aspects of one embodiment of the present disclosure may include providing a database 257 having an entry for each inmate and having a plurality of fields, with the fields in turn including inmate names, correction system identification codes, inmate identification codes, correction system facility codes which indicates a specific correction facility; and storing each electronic letter sent to a specific inmate in a relational database management system (RDMS) table, the RDMS table including fields for inmate name, inmate identification code and lists of corrections facilities. The database 257 may also include a table that includes entries for all inmates in a correction system or a correction facility.

[0065] The database may be maintained by periodically downloading a file from the correction authority central computer server farm 259 (including, for example, servers 259a-b) for such changes as new inmates, inmate releases and inmate movement between facilities. In one embodiment of the present disclosure, the downloading step is performed daily and the database may be arranged to provide for correction authority letter search and retrieval by the inmate name, inmate identification code, date, facility or keyword. In one embodiment, the database table includes at least three fields selected from the following group: (1) an inmate's last name, (2) an inmate's first name (3) an inmate's identification code, (4) an inmate's correction system code, (5) an inmate's correction system facility code and (6) other information if needed.

[0066] The present disclosure includes a letter creation and transmission website that may be maintained by server farm 255 (including, for example, servers 255a-d and database 257) that can be used by a person desiring to write letters to an inmate and that optionally assesses a fee for each letter sent. The website may be configured so that the writer can store and review his or her letter drafts digitally. The writer may receive email notification at computer 251 when his or her letter has been printed in the inmate's facility and delivered to the inmate and/or viewed by the inmate through a computer terminal (e.g., 263a, b, c) at the inmate facility, or viewed through a digital content player, such as a handheld device designed to be sufficiently small, and configured, to be held and operated using one hand of a user. In an alternative embodiment, the writer may scan the desired correspondence or document through use of a scanner and upload the scanned document to the website for forwarding to the inmate. In yet another alternative embodiment, a message delivered to an inmate may include photos or videograms attached thereto, which may be displayed at a kiosk or digital content player at the inmate's facility. Conversely, an inmate may use a kiosk or digital content player to create outbound messages directed to family members, for example, and distributed through use of the communications architecture of the present disclosure.

[0067] Aspects of another embodiment of the present disclosure include (a) providing, in database 257, one or more tables having a plurality of fields, with the plurality of fields including at least two fields selected from a group consisting of inmate name, inmate identification code or other identifier, and inmate facility name or facility code; (b) providing an electronic interface accessed through computer 251 for a writer, wherein the electronic interface allows the writer to

specify the inmate or inmates that are the intended recipient (s) of the writer's communication, space for text of the mail or correspondence; and (c) a system enabled by server farm 255 for purchasing "postage" to transmit the mail or correspondence; and maintaining a database table, the database table including (i) a list of letters sent by a specific writer, (ii) a list of letters that the inmate has received, and (iii) a list of privileged writers. The database table may also include a table entry indicating whether that letter has been previously read by the correction authorities and by whom; a table entry indicating which letters have as yet not been reviewed; and/or a table entry indicating who has been using the process to send letters to which inmates and at which facilities.

[0068] The database table may also include a table entry allowing authorities to search scanned letters for certain keywords. The database table can further comprise a table entry indicating privileged writers, such as attorneys, whose communications may be marked as privileged when printed or displayed and whose letters will be marked as not for correction authority inspection. The database table can further comprise a table entry indicating keywords that are of interest to the correction authorities. The database table can further comprise a table entry indicating to whom each writer is sending letters.

[0069] The system of the disclosure and method provides an electronic letter routing software system that can be implemented on a network, including the Internet. Routing of mail is described in U.S. Pat. No. 7,647,380 to Gillum et al. which is incorporated herein by reference. In an embodiment of the system and method of the disclosure, several database tables are created in database 257, including but not limited to: an inmate table that identifies the inmates and related information; a facility table that identifies the facilities and related information; a writer table that identifies the writers and related information; a credit card table that identifies the credit cards that the writer uses; a letter table that identifies the letters and related information; a privileged writer table that identifies the writer as a privilege communicator; and a keyword table that lists the keywords of concern to the prison authorities.

[0070] Inmate Location

[0071] The system of the disclosure and method creates, via regular downloads from the correction authorities' database (e.g., 261) associated with a correction authority's central computer (e.g., 259a, b), a table that includes inmate names, correction system identification codes, inmate identification codes, correction system facility codes, and optionally other information.

[0072] The correction system identification code uniquely identifies a particular correction system such as a state, county or federal system. The inmate identification code uniquely identifies a particular inmate within a particular correction system such as a state, county or federal system. The correction system facility code uniquely identifies the correction facility within the correction system that holds that particular inmate. This facility code thereby determines which letters will be placed into that facility's mail file during the next mail delivery (or download).

[0073] Inmate Location

[0074] The system of the disclosure encodes the correction facility internally, for example as a four character sequence, where the first two characters identify the state and the second two characters identify the facility within that state. As a non-limiting example, New York's Dannemora prison is

coded as "NYDA" while the Federal government's prison at Danbury, Conn. is coded as "FDDA". The facility code can be case insensitive. Such an encoding scheme allows for 1,296 (36 squared (letters A-Z number 0-9) facilities within a corrections system (e.g., AA through 99).

[0075] An inmate table can include the following fields in a database: inmate's last name; inmate's first name; inmate's identification code; inmate's correction system state, county or federal code; inmate's correction system facility code; and other information if needed, such as device ID for the digital content player.

[0076] Facility Setup

[0077] A facility is added to the system of the disclosure via an input screen. Input data requested can include, but is not limited to, facility code, facility name, mail delivery times and other information if needed. Advantageously, the facility location is further included, or the inmate location (i.e., cell block) within a particular facility.

[0078] The system of the disclosure then performs validity checks. Such validity checks may include, for example, determining if the facility is already in the table. If the data are valid the facility is added to the database table.

[0079] The Facility Table

[0080] A facility table comprises at least one field selected from the group including: a four (4) character alphanumeric facility identifier, the facility name, the facility address, facility mail delivery times, and other information if needed.

[0081] Writer Registration

[0082] Before sending an initial letter, a writer first opens an account by filling out an input form that requires data, such as a username, a password and an optional email address. A password system can be used to further let the writer enter a hint question so that if he forgets his password he can be reminded. For example, the writer might enter a password of "lion" and have a question to remind him of that password that asks, "What is my favorite animal?"

[0083] The process or software then performs various validity checks (such as email verification or credit card verification with name and address). If a writer proves to be a valid writer, the writer is added to the writer table and assigned a unique identification number.

[0084] The Writer Table

[0085] The writer table comprises at least one field selected from the group including: writer's username; writer's password; writer's password hint; writer's email address (optional); writer (system assigned) unique identifier; and amount of postage writer has remaining.

[0086] Purchasing "Postage"

[0087] In order to send a letter the writer buys "postage" by entering his or her credit card information. The amount of the postage is stored in the writer's table. The process creates a unique credit card/username identifier for each writer.

[0088] The Credit Card Table

[0089] The Credit Card table includes: writer unique identifier card name (e.g. VISA, MASTERCARD, AMEX, etc. . . .); card number expiration; unique credit card/username identifier; and unique credit card validation number.

[0090] Billing Records

[0091] The billing table displays the amount and date of postage purchased on that credit card.

[0092] The Billing Table can include: unique credit card identifier, transaction date, and transaction amount.

[0093] It should be understood that the field descriptions provided herein, for the various tables, are exemplary, and can

be used to carry out the disclosure. Additional or fewer fields may be used, and the field names may be different.

[0094] Sending Letters

[0095] To compose a letter the writer uses a letter-input screen. This screen can resemble a standard letter with the writer's address on the upper right and recipient's address on the lower left, for example. The writer can insert the inmate's address into the letter in different ways, as follows. In one embodiment, the writer can select the name of one or more recipients using a Recipient Table, presented for example in the form of a dropdown list.

[0096] First, the writer can identify the inmate's corrections system. If the inmate is incarcerated in New York, for example, the writer can specify that state by typing NY or by using a "pull down" menu. The writer can then enter the inmate's identification code, and the inmate's name and address will automatically fill in.

[0097] Alternatively, the writer can address the letter by entering the inmate's last name. If several inmates share that last name, the system will list all inmates with that last name, their first names, their inmate identification codes, and their facility locations. The writer then selects the correct inmate, and the address automatically fills in.

[0098] The writer can then enter the text of the letter, and click the send button. The letter is added to the letter table, and the writer is informed of the next mail delivery. The writer may then exit the process, or write another letter.

[0099] Storing the Letters

[0100] The inmate letters are stored on the server **255**. The status of each letter is also stored.

[0101] Such status indicates whether the letter has already been downloaded and read, whether the letter should be held for review, and which keywords may have been detected.

[0102] In an exemplary embodiment, fields include: a unique inmate identifier; a unique writer identifier; a facility code; the time and date the letter was created; the time and date the letter was delivered; correction review (yes/no); a hold/release flag; keyword triggers; and the text of the letter.

[0103] Writer Interaction

[0104] The writer interaction process includes a screen that enables the writer to review his activity. First, the writer can see a detailed list of the inmates to whom he has sent letters. Second, the writer can see a list of the letters that he has sent to a particular inmate. Third, the writer can read a letter that he has previously sent.

[0105] Corrections Authorities—Getting the Mail

[0106] The facility mail file may be stored on the server and may be retrieved by the facility mailroom. Alternatively, the file may be emailed to the facility.

[0107] In one embodiment, facility mailroom employees retrieve the mail file via a web page that allows them to create the mail file dynamically from the letter table. The mailroom employee enters name and password. Thereupon, to create the mail file, the process creates a list of letters for that facility in preferred order (e.g. alphabetized by inmate name), and a cover sheet listing the letters. The process then creates a download file that includes the cover sheet followed by the letters in the specified or preferred order.

[0108] Once the download is completed, the letter table is updated to indicate that the letters have been downloaded at the facility. The writers are then emailed that the letters have been printed.

[0109] Correction Authorities Interaction

[0110] Correction authorities read inmate mail, except for privileged correspondence, for example between an attorney and his or her (inmate) client. First, correction authorities can see a chronological list of letters sent to the inmate and can print inmates' letters either individually or collectively. Second, correction authorities are alerted if inmate letters contain prohibited keywords. Third, correction authorities can read letters and indicate in the letter table that a particular letter has been reviewed and if held for review subsequently released to the inmate. Fourth, correction authorities can search across all inmate letters in the correction system for commonalities and keywords.

[0111] Delivery of Digital Content

[0112] Another embodiment of the present disclosure includes the delivery of digital content, such as music or video content, videograms (prerecorded video messages or other user generated content), and video visitation (video streaming, one or two-way), to inmates. FIG. 3 illustrates a communications environment, parts of which may be used in the implementation of the digital content delivery aspect of the present disclosure. FIG. 3 is a basic schematic diagram **10** of a digital content store system **12a** implemented between a digital content store **14** and a client machine **16**. A user USR at a client machine **16** may access the digital content store **14** through a store link and account module **38**, such as through a user interface **103** (FIG. 4). The store module **38** is typically associated with a selectable inventory **36** of assets (e.g., songs), which are typically accessible **42, 44**, upon purchase or other redemption, as encrypted assets **18**, e.g., **18a-18p**, such as through a digital fulfillment center **40**. The content store **14** may also maintain a history of ordered and downloaded assets **46**.

[0113] A user USR at a client machine **16** may purchase encrypted assets **18** (e.g., encrypted songs), through the entry of purchase information **34**, whereby the encrypted assets **18** are delivered, such as through downloading **50**, which may include a download prompt **52** and download delivery **54**, wherein the download delivery **54** comprises both asset delivery and license delivery to the client **16**. In another embodiment of the present disclosure the assets need not be encrypted.

[0114] In some system embodiments **12**, the user USR may also use the system to purchase physical inventory of content **56**, e.g., an MP3 player pre-loaded with songs, which are then shipped **58** to the intended user USR. Upon purchase **34**, some system embodiments comprise both delivery of physical content **56**, along with downloading of encrypted digital content **18**, whereby the intended user USR can quickly access content **18**, such as songs, movies, games, or other content **18**.

[0115] As seen in FIG. 3, license information **20** for an encrypted asset **18** includes the asset rights for the encrypted content **18**, and may include both an asset key **22** and usage rights **24**, which are retained within a secure key locker **26**. In one embodiment, the asset key **22** is bound to the client machine **16**, such as through machine fingerprinting or in conjunction with the machine identification **21**.

[0116] Usage of the encrypted asset **18** typically includes writing or uploading **392** the asset **18** and license information (e.g., key **22** and usage rights **24**) to a digital content player **390**. The digital content player includes a device control **393** module to direct the operations of the player **390**, a unique device ID **397**, and a module **395** for outputting content in a format that can be played or further modified such that a user

can perceive. The player **390** may also include the capabilities of decrypting the assets and moving the raw assets **304** to a raw asset storage area **398** within the player's memory **394**.

[0117] The player may also store encrypted assets in memory **394** and playback the encrypted assets **18** by retrieving the asset rights **20**, whereby the asset key **22** operates upon the asset **18**, such as through decryption, decoding and/or rendering. The enabled asset is then played as desired by the user USR, in compliance with the usage rights **24**.

[0118] An authorized use of the encrypted asset **18** may include an authorized transfer **29** of the asset **18** to media or storage on a player **390**, e.g., an MP3 player, or to another machine **16**, as allowed by usage rights **24**. In conjunction with an authorized transfer **392**, a modified license **20** may be included with the encrypted asset **18**, such as comprising an asset key **22** which is unbound from the primary client machine **16**, and a portion of appropriate usage rights **24**, e.g., such as for authorizing use of physical media **56**.

[0119] FIG. 4 is a detailed schematic diagram of client and server side architecture within a digital content store system **12b**. This environment or parts thereof may be used to implement certain features of the present disclosure. Client software **84** provides communication functionality to server **14**, and to a digital content player **86**, e.g., a music player. A media database **82** may reside in the client computer and may store assets, such as acquired encrypted assets **18**, and may be used to store other assets, such as unencrypted assets and/or associated metadata.

[0120] The client software **84** typically comprises a download module **92**, a license download module **94**, and may also comprise other functionality, such as stored user interface pages **90** and/or promotional links **88**, e.g., for a digital content store **14**.

[0121] The digital content player **86** may include a secure digital content/music store (DMS) content handler **96**, digital rights management (DRM) **98**, dedicated communications module **100**, and secure advanced audio coding (AAC) **102**.

[0122] On the server side **14**, promotional links and user account **38** typically comprise a user interface **103**, download and order history **46**, content download **104**, license download **106**, and license purchase **108**. An encrypted content store **110** stores encrypted content **18**, such as is available for purchase within the digital content store system **12**. Other server storage comprises content metadata and usage rights **112**, keys database **114**, and a user database **116**.

[0123] As seen in FIG. 4, raw content **122**, such as from labels **124**, is sent to content acquisition **118**, wherein the incoming raw content **122**, which may include raw assets and associated metadata, may be processed within an encoding and encryption module **120**.

[0124] The back office support system **108** shown in FIG. 4 comprises pricing **142**, a user database **144**, royalty processing **130**, member services **132**, billing and micropayments **136**, taxation **138**, order management **140**, and jax/fraud **134**. Pricing/SKU information **126** is typically sent to the back office support system **108**, such as from metadata **306** received at content acquisition **118**. As well, royalty reporting or other output information **128** is typically sent from the back office support system **108** to the labels **124**.

[0125] As seen in FIG. 4, content and associated license information is sent from the server **14** to the client machine **16**, through the client software **84**. Encrypted content **18** is transferred to the media database **82**, where it is retrievable for usage through the digital content player **86**. As needed, the

digital content player **86** may interact through the client software **84**, such as to communicate with the server **14**, e.g., to update usage information, or to prompt the user USR to acquire or extend asset rights **20**.

[0126] During playback of acquired assets, the digital content player playback engine extracts the asset key **22** from the secure key locker **26**, and then decrypts, decodes, and renders the asset **18**. The media pipeline is protected up until the handoff to the sound card.

[0127] If the digital content player **86** detects that the key **22** is missing, or is not valid for the machine **16** in question, the digital content player **86** may first play a sample of the song **18**, e.g., such as a 30 second clip, and then the digital content player **86** presents the user USR with a purchase opportunity. If the user USR chooses to purchase **34**, the user is taken to the digital music store **14** to complete the process **34**. The entire key mechanism is advantageously seamless to the user experience.

[0128] FIG. 5 is a functional block diagram of an alternative digital music player **400** including asset security for encrypted assets **18**. Encrypted content **18a-18p** is typically transferred from a client machine **16**, in compliance with allowed usage rights **24**. Some embodiments of the player **400** additionally provide storage and playback of raw, i.e., unencrypted assets **304a-304m**. As seen in FIG. 4, the player **400** typically comprises similar internal digital rights management capabilities, such as a secure key locker **26**, and an extended license **20**, comprising asset keys **22** and usage rights **24** for the encrypted content **18**. The player may typically store one or more device IDs **21**, to track the source machine **16** from which content **18** is received. The device may also include a device ID **410**, which is used for machine-bound content management. In some embodiments of the secure content player **400**, the player **400** is considered to be a client machine **16**, such as for licensing purposes. The player **400** may be considered to be an independent player, such as for licensed usage allowed for a user USR of one or more client machines **16**.

[0129] The system and method of the present disclosure allow inmates to buy digital media, including individual songs, albums and eBooks, from an Inmate Kiosk and download it to a personal portable player of digital content (the "Player") securely while ensuring the protection of content owner rights. The system of the present disclosure in accordance with one embodiment (FIG. 6) may include the following components:

[0130] Global Server **605**: Administers services to an online store running in server **601** and eCommerce over the Internet **621**.

[0131] Inmate Kiosks **613a-c**: Allow inmates to securely interact with local server **611** over a secure facility network **623**. In one embodiment, the kiosk terminals **613a-c** do not allow localized storage or access to regular Windows-level folders. Each kiosk terminal may run a kiosk application to prevent the inmates from treating the terminal as a regular PC with OS access. The kiosk application ensures that the kiosk is solely used as a window into the local server **611** and local download manager (installed in the server **611**) and only connects to the web for specific pre-approved functions within the media store (run by server **605**), such as listening to song previews from the content provider's server **601**. Software specifically designed to prevent tampering, for example accessing the operating system, is advantageously used in

combination with software of the disclosure. Alternatively, such service is included in software of the disclosure.

[0132] Local download manager (“LDM”): This application may run on the Local Server **611** and administers the synchronization of media delivery between the Global Server **605**, Inmate Kiosk (e.g., **613a**), and a Player (e.g., **615a**). Content resides on the Local Server **611** and LDM, which is then delivered to Player **615a-c** through the corresponding kiosks **613a-c**.

[0133] Digital Content Player (or Player): The portable digital content player may be purchased by an inmate. An inmate synchs the Player and downloads files securely through a kiosk after purchase of content using a personal account created and maintained at the Global Server **605**. The Player may be implemented as a custom-made device for the corrections industry that allows delivery only of approved content via specific USB codes which prevent unauthorized connections. All inmate interaction with the Global Server **605** and the Media Server **601** is conducted using a unique inmate ID to ensure security and prevent cross-pollination or abuse of account information or purchased media.

[0134] In one embodiment of the disclosure, the digital content includes music and may be maintained in a catalog **601** by a content aggregator (specializing in obtaining licensing for large catalogs of digital content) at a Media server **601**. In an alternative embodiment the system administrator for server **605** may also administer the media server **601**. In another embodiment of the disclosure, the player displays inmate correspondence.

[0135] In one embodiment, the content aggregator obtains the content from the different music labels to update the catalog **603** and uniformly funnels the content catalog over the Internet to the Global Server **605** as XML files. The Server **605** loads the catalog **603** from the MEDIA SERVER **601** and processes it to fit any general or specific restrictions. The catalog may include links to previews and album art which reside on the Aggregator’s site at all times and are provided through a direct link from the kiosk.

[0136] The Global Server **605** may get daily updates to the catalog from the media server **601** using SOAP API. To purchase a song from the Aggregator, the Global Server **605** also may use SOAP API. After a purchase is made, the Global Server **605** sends download instructions to the local server **611** to download the songs. The inmate then connects to the kiosk which in turn copies the files from the local server **611** to the digital content player.

[0137] The Local Download Manager (LDM) may be implemented as a standalone executable used to manage the content downloads between the Local Server **611** and Players **615a-c** (using the kiosks **613a-c** as enabling pass-through units). In one embodiment, the LDM centralizes management of all tasks, for example content downloads, local storage, etc., in one location per inmate facility, and the Local Server **611** runs separately and is not physically accessible to inmates. The LDM may include predefined settings which provide general information about the Aggregator’s site (URL, user name, password etc.). The LDM transfers information about processed orders into a file system in the local server **611** before a content download begins. The order for content contains inmate ID, song name, and access instructions. Each completed delivery of content to the Player is reported back to the Global Server **605** and the Local Server **611** and stored on a file system locally at Local Server **611**. The kiosk deletes the content file copy from the local server

611 after it is transferred from the local server network drive directly to the Player (i.e., after successfully copying the files to the digital content player).

[0138] In one embodiment of the present disclosure, the LDM communicates with the global server **605** over Web Services and LDM acts as the client (e.g., LDM will pull information from global server **605**). The LDM may be accessed through a management console with HTTP based user interface (“UI”) and may also have a local text based log file to describe main actions.

[0139] The LDM may obtain specific downloaded instructions from the Global Server **605**. Local Server **611** downloads the content from the media server **601**, stores the content on its local file system, and provides the kiosk access to the stored content to retrieve songs, for example, and deliver them onto the Player. Each inmate may have a directory on the local file system with subdirectories for downloads and galleries and can only access his or her own account.

[0140] In one embodiment of the present disclosure, a kiosk terminal **613** has pre-defined settings to access the local server **611** file system root directory using a share drive mechanism. The local server **611** notifies the kiosk **613** when content is ready to be downloaded to the player **615**, after which the inmate will be allowed to start downloading media directly to a registered Player. The Player may connect to the kiosk through a standard USB port.

[0141] After connecting the player to the kiosk, the kiosk identifies the player, for example, based on the inmate id or other identification parameters embedded in the player during the fulfillment process. Unrecognized players/devices are not immediately served. When the kiosk matches the inmate id to the Player and session id, the player is allowed to download content. At the start of the download, the kiosk accesses the inmate directory on the local server file system and copies all new files in this directory directly to the Player (one-way synch process). Download includes copy or, if configured, moves the content files from the inmate folder on the LDM directory to the player. In one embodiment, files will not be saved on the kiosk file system. Advantageously, the player should not be disconnected from the kiosk while downloading content. The kiosk may display a message to the inmate such as “Downloading, do not disconnect.” The Kiosk application disables an auto logout feature during download and resumes when the download is complete.

[0142] After download of content is complete the following can occur: (1) a summary message is displayed to the inmate (songs, price, etc); (2) a status change notification of a completed download is sent to the local server; and (3) the kiosk application collects the player’s statistics (number of songs and available space) and sends it back to the local server.

[0143] When the kiosk is in the process of authenticating an inmate, if the kiosk does not match the inmate id to the Player and session id, the kiosk can stop serving the player and perform the following actions: (1) the kiosk sends a notification back to the local server **611** to be propagated to the appropriate facility user—this prevents the inmate from continuing to use the unauthorized device by either moving all songs from the player to the inmate directory on the LDM or disabling the Player; and (2) the kiosk displays a message to the user and marks his account as “Locked.”

[0144] In addition to facilitating the downloading of content into the player, the kiosk application is responsible for the Player maintenance and control, in accordance with one embodiment of the disclosure. Each Player is registered to

one inmate and includes a unique ID to be matched with a specific inmate ID. Each kiosk can only access the inmate's account on the Local Server **611**.

[0145] Player access to the kiosks may be restricted by "burning" an individual inmate ID into the player device's memory. In one embodiment, the kiosk allows downloads for inmates that authenticate themselves at the kiosk and then connect a Player with a matching ID. If the Player is NOT verified the kiosk sends a "lock" command to the Player to prevent further use.

[0146] In one embodiment of the disclosure, there are two specific methods of communication with the Player. In a first method of communication, a specific driver allows interaction between the kiosk and the player only if the driver is loaded to the kiosk terminal (this eliminates unauthorized PC connections). The "mass-storage" capabilities may be excluded from the driver to eliminate the risk of using the player as a flash drive. In one embodiment of the disclosure, the driver allows the player and player software to communicate with the kiosk application, so if the driver is not loaded the player cannot communicate with the kiosk.

[0147] In a second method of communication between the kiosk and the player, a .COM object or .NET assembly is loaded in real-time by the kiosk application or software library and is compiled to the kiosk application with the following functions:

[0148] Int GetInmateID (string PassKey)—return inmate id or -1 if wrong passkey or inmate id is not available. Passkey may be defined as a predefined string used for security purposes. Int PutInmateID (string PassKey, string id)—store a new id on the device. Bool ChangePassKey (string currenPassKey, string newPassKey)—change the passkey. Int GetDevice serialID (string PassKey)—get a unique serial id (optional).

[0149] The following functions lock the player if the special driver is not available. The kiosk application locks the player after download and unlocks it again before the next download. Bool LockDevice (string PassKey)—disable the device from receiving any files until unlock function is called (Bool UnLockDevice (string PassKey)—enable device for receiving any files. Bool RemoveLock (String passkey)—remove the locking (i.e. allow receive files from any source).

[0150] The .NET object or wrapper serves as a translator between the kiosk application and the player software.

[0151] FIG. 7 illustrates a method for processing a purchase transaction for a player using the kiosk application. At step **701** the inmate places an order using the kiosk terminal. The order is communicated to the global server via web services. At step **703** the global server verifies details of the order and creates a purchase order. The global server verifies that the order amount can be cleared by the Department of Corrections ("DOC") Bank. At step **705** the DOC Bank sends a response to the global server to notify whether there are sufficient funds in the account associated with the inmate making the request. An inmate account can be replenished through deposits made on behalf of the inmate by family or friends, or in the alternative, through work programs established by the corrections facility, for example. At step **707**, if the global server determines that there are not sufficient funds, then the inmate is notified through the kiosk terminal, for example.

[0152] If the global server determines that there are sufficient funds, then global server creates a player setup file. This file includes the inmate ID and other default settings. The file

is then uploaded into the ordered player. If the inmate does not select an option to preload the player with content, then the player is packed and shipped to the inmate's facility (step **719**).

[0153] If the inmate selects an option to preload content into the player (step **713**), then global server requests the pre-required content (e.g., songs), from the media server. This request may be made over web services. At step **721** the media server confirms the order for purchase of a song, for example, and in response to the request returns a link for downloading the content. After receiving the link, the global server downloads the songs (step **717**) over an http connection from a download site (e.g., the media server). After the player is preloaded with content, the player is packed and shipped to the inmate's facility (step **719**). At step **725** the player is distributed to inmates.

[0154] FIG. 8 illustrates a process for ordering and browsing content through the kiosk terminal. At step **801** the inmate initiates browsing through the kiosk terminal. The local server may communicate with the global server over web services to access the catalog (step **803**). The catalog residing in the global server is first uploaded **807** from the media server **805** over an Internet connection. Daily catalog updates may be transmitted to the global server over web services **809**.

[0155] In step **811** the kiosk presents an option to preview the catalog. The preview may be accessed directly by clicking on a URL link to the media server, for example (step **815**). Either after previewing content or skipping the preview option, the inmate may use the kiosk terminal to order content (step **813**). The kiosk sends a request for selected content to the global server and the global server verifies details of the order and creates a purchase order (step **817**). The global server verifies that the order amount can be cleared by the DOC Bank. At step **819** the DOC Bank sends a response to the global server to notify whether there are sufficient funds in the account associated with the inmate making the request. At step **821**, if the global server determines that there are not sufficient funds, then the inmate is notified through the kiosk terminal (step **823**), for example.

[0156] If the global server determines that there are sufficient funds, then global server sends a request to the media server to confirm the order and the media server returns confirmation and a link for downloading the content (step **825**). The global server also creates order instructions to the local download manager including inmate ID, location, download URL, and download time, for example.

[0157] FIG. 9 illustrates content download processes in accordance with one embodiment of the present disclosure. At step **901** the LDM running in the local server initiates the content download process by first checking whether there are any pending downloads. The LDM initiates and sends a startup message to the global server over web services and in response to the request the global server verifies whether the local download manager has new pending downloads (step **903**). If there are pending downloads, at step **907** the global server creates instructions for downloading content that include instructions to finish pending downloads. For example, if there are pending downloads, the global server creates instructions so that at the next communication cycle the local download manager will retrieve the instructions and download the content. Otherwise at step **907** creates download instructions that do not include pending downloads. At step **905** the LDM obtains download instructions from the global server, again communicating with the global server

over web services. At step **909** the LDM initiates download of content, for example music, from the media server by establishing an http connection with the media server. At step **911** the content is downloaded from the media server.

[0158] At step **913** the kiosk terminal displays a login screen to an inmate. After log in, the kiosk checks whether an order for content is ready. The kiosk sends a request to the global server over web services and in response to the request the global server verifies whether the inmate order for content is ready (step **917**). If the order is ready, at step **919** the global server creates instructions for authorizing delivery of content to the player. At step **915** the kiosk obtains the order instructions from the global server, again communicating with the global server over web services. For example, the global server may direct the kiosk to access the local download manager to copy content awaiting to be downloaded by inmates.

[0159] At step **921** the kiosk determines whether the content player is plugged in to the kiosk, and if it is not the inmate may be taken back to the login screen. If the player is connected, then content is copied from the LDM to the kiosk and then to the player at step **923**. After the download is complete, the kiosk displays a login screen again.

[0160] Other aspects of browsing and ordering content will be described below with reference to FIGS. **10-16**. Generally, the local server provides the kiosk with specific offerings per inmate based on restrictions set by the facility. Inmates log into the kiosk and then browse through the catalog of specific offerings.

[0161] The searchable catalog may be organized based on artists, albums or genres. Content length, cost and position in the album may be displayed at the song level.

[0162] Song previews may be played and listened to at the kiosk (via LDM connection to the Internet and onto the media server site), and album covers may be displayed, as well as artist images when available. Previews may be available per song by routing the requests for previews in real time to the media server. The preview may be secured behind a Flash button to prevent a localized download of the preview clip. After accessing previews inmates may order a number of songs, based on their account balance, or purchase a full album. Once the order is complete a confirmation appears notifying the inmate about cost of order and order processing time. Inmates may check on their order status at any given time during the download process. The global server keeps a status record of every order for audit purposes. For example, each component in the system may send a status update of the content (e.g., pending, purchased, downloaded, copied, etc.) to the global server.

[0163] FIG. **10** illustrates an exemplary screenshot that may be displayed by the kiosk terminal. The kiosk may display an image of a content Player which inmates can order through the kiosk (**1001**). The kiosk may display categories of music (**1003**). These categories may include rock, rap, R&B, etc. The kiosk may also display the content items that an inmate has already selected for purchase (**1005**). The kiosk may also display the top selling songs **1007**.

[0164] FIG. **11** illustrates a screenshot similar to that in FIG. **10** except that the kiosk displays a message that content is ready to be downloaded. The content may be downloaded by the inmate physically connecting the Player to the kiosk, or in an alternative embodiment, by wirelessly connecting the player to the kiosk by moving the player to a wireless hotspot. FIG. **12** illustrates advertisements that may be dis-

played by the kiosk. In the illustrated exemplary display, the inmate is presented with an offer to buy a top selling album (**1201**).

[0165] FIG. **13** illustrates a screenshot of the kiosk displaying top selling songs. The kiosk may display whether the songs have already been added to a shopping cart (**1303**) or not (**1305**). Other information related to each song may also be displayed, for example, the price **1302**, the length of the song **1311**, the album **1313**, and the artist **1315**. An option to play a clip of the song may also be displayed **1309** as well as an option to checkout **1361**.

[0166] FIG. **14** illustrates a screenshot of songs displayed by the kiosk under the R&B category **1401**. The kiosk also displays the price per song, transaction fee, and the total price **1403**. FIG. **15** illustrates a screenshot of songs displayed by the kiosk under the Artist category **1501**. FIG. **16** illustrates a screenshot of the kiosk displaying an option to remove content previously added to the shopping cart **1601**.

[0167] The system of the present disclosure in accordance with another embodiment (FIG. **17**) may include the following components:

[0168] Global Server Farm **1905**: The Global Server Farm **1905**, including servers **1905a-d** and a database **1906**, administers services to an online store running in Aggregator **1901** and eCommerce over the Internet **1921**. The Aggregator **1901** may include servers **1901a-b** and a database **1902**.

[0169] Inmate Kiosks **1813a-c** and **1913a-c**: Allow inmates to securely interact with local server **1912** and LDM **1911** over a secure facility network. In one embodiment, the kiosk terminals do not allow localized storage or access to regular Windows-level folders. Each kiosk terminal may run a kiosk application to prevent the inmates from treating the terminal as a regular PC with OS access. The kiosk application ensures that the kiosk is solely used as a window into the local server **1912** and local download manager **1911** and only connects to the web for specific pre-approved functions within the media store (run by global server farm **1905**), such as listening to song previews from the content provider's Aggregator **1901**. To prevent OS access, software such as siteKiosk from Provisio may be used.

[0170] Local download manager ("LDM"): This application may run on the Local Server **1912** or may run on a separate machine **1911**. The LDM administers the synchronization of media delivery between the Global Server Farm **1905**, Inmate Kiosk (e.g., **1913a**), and a Player (e.g., **1915a**). Content resides on the Local Server **1912** and the LDM **1911**, which is then delivered to Players through the corresponding kiosks.

[0171] Digital Content Player (or Player): The portable digital content player may be purchased by an inmate. An inmate synchs the Player and downloads files securely through a kiosk after purchase of content using a personal account created and maintained at the Global Server Farm **1905**. The Player may be implemented as a custom-made device for the corrections industry that allows delivery only of approved content via specific USB codes which prevent unauthorized connections. All inmate interaction with the Global Server Farm **1905** and the Aggregator **1901** is conducted using a unique inmate ID to ensure security and prevent cross-pollination or abuse of account information or purchased media.

[0172] In one embodiment of the disclosure the digital content includes music and may be maintained in a catalog by the content aggregator **1901**. In an alternative embodiment the

system administrator for Global Server Farm **1905** may also administer the Aggregator **1901**. In another embodiment of the disclosure, the player displays inmate correspondence, including pictures and videograms.

[0173] In one embodiment, the aggregator **1901** obtains the content from the different music labels to update the catalog and uniformly funnels the content catalog over the Internet to the Global Server Farm **1905** as XML files. The Global Server Farm **1905** loads the catalog from the Aggregator **1901** and processes it to fit any general or specific restrictions. The catalog may include links to previews and album art which reside on the Aggregator's site at all times and are provided through a direct link from the kiosk.

[0174] The Global Server Farm **1905** may get daily updates to the catalog from the Aggregator **1901** using the SOAP API. To purchase a song from the Aggregator **1901**, the Global Server Farm **1905** also may use SOAP API. After a purchase is made, the Global Server Farm **1905** sends download instructions to the local server **1912** to download the songs. The inmate then connects to the kiosk which in turn copies the files from the local server **1912** to the digital content player.

[0175] The Local Download Manager (LDM) may be implemented as a standalone computer **1911** used to manage the content downloads between the Local Server **1912** and Players (using the kiosks as enabling pass-through units). In one embodiment, the LDM **1911** centralizes management of all tasks, for example content downloads, local storage, etc., in one location per inmate facility, and the Local Server **1912** runs separately and is not physically accessible to inmates. The LDM **1911** may include predefined settings which provide general information about the Aggregator's site **1901** (URL, user name, password etc.). The LDM **1911** transfers information about processed orders into a file system in the local server **1912** before a content download begins. The order for content contains inmate ID, song name, and access instructions. Each completed delivery of content to the Player is reported back to the Global Server Farm **1905** and the Local Server **1912** and stored on a file system locally at Local Server **1912**. The kiosk deletes the content file copy from the local server **1912** after it is transferred from the local server network drive directly to the Player (i.e., after successfully copying the files to the digital content player).

[0176] In one embodiment of the present disclosure, the LDM **1911** communicates with the Global Server Farm **1905** over Web Services and LDM **1911** acts as the client (e.g., LDM **1911** will pull information from Global Server Farm **1905**). The LDM **1911** may be accessed through a management console with HTTP based user interface ("UI") and may also have a local text based log file to describe main actions.

[0177] The LDM **1911** may obtain specific downloaded instructions from the Global Server Farm **1905**. Local Server **1912** downloads the content from the Aggregator **1901**, stores the content on its local file system, and provides the kiosk access to the stored content to retrieve songs, for example, and deliver them onto the Player. Each inmate may have a directory on the local file system with subdirectories for downloads and galleries and can only access his or her own account.

[0178] In one embodiment of the present disclosure, a kiosk terminal (e.g., **1813a-c** or **1915a-c**) has pre-defined settings to access the local server **1912** file system root directory using a share drive mechanism. The local server **1912** notifies the kiosk when content is ready to be downloaded to the player, after which the inmate will be allowed to start downloading

media directly to a registered Player. The Player may connect to the kiosk through a standard USB port.

[0179] After connecting the player to the kiosk, the kiosk identifies the player, for example, based on the inmate id or other identification parameters embedded in the player during the fulfillment process. Unrecognized players/devices are not immediately served. When the kiosk matches the inmate id to the Player and session id, the player is allowed to download content. At the start of the download, the kiosk accesses the inmate directory on the local server file system and copies all new files in this directory directly to the Player (one-way synch process). Download includes copy or, if configured, moves the content files from the inmate folder on the LDM directory to the player. In one embodiment, files will not be saved on the kiosk file system. Advantageously, the player should not be disconnected from the kiosk while downloading content. The kiosk may display a message to the inmate such as "Downloading, do not disconnect." The Kiosk application disables an auto logout feature during download and resumes when the download is complete.

[0180] After download of content is complete, the following can take place: (1) a summary message is displayed to the inmate (songs, price, etc); (2) a status change notification of a completed download is sent to the local server; and (3) the kiosk application collects the player's statistics (number of songs and available space) and sends it back to the local server.

[0181] When the kiosk is in the process of authenticating an inmate, if the kiosk does not match the inmate id to the Player and session id, the kiosk will stop serving the player and perform the following actions: (1) the kiosk sends a notification back to the local server **1912** to be propagated to the appropriate facility user—this prevents the inmate from continuing to use the unauthorized device by either moving all songs from the player to the inmate directory on the LDM or disabling the Player; and (2) the kiosk displays a message to the user and marks his account as "Locked."

[0182] In addition to facilitating the downloading of content into the player, the kiosk application is responsible for the Player maintenance and control in accordance with one embodiment of the disclosure. Each Player is registered to one inmate and includes a unique ID to be matched with a specific inmate ID. Each kiosk can only access the inmate's account on the Local Server **1912**.

[0183] Player access to the kiosks may be restricted by "burning" an individual inmate ID into the player device's memory. In one embodiment, the kiosk allows downloads for inmates that authenticate themselves at the kiosk and then connect a Player with a matching ID. If the Player is not verified the kiosk sends a "lock" command to the Player to prevent further use.

[0184] In an embodiment of the disclosure, there are two specific methods of communication with the Player. In a first method of communication, a specific driver allows interaction between the kiosk and the player only if the driver is loaded to the kiosk terminal (this eliminates unauthorized PC connections). The "mass-storage" capabilities may be excluded from the driver to eliminate the risk of using the player as a flash drive.

[0185] In a second method of communication between the kiosk and the player, a .COM object or .NET assembly is loaded in real-time by the kiosk application or software library and is compiled to the kiosk application with the following functions:

[0186] Int GetInmateID (string PassKey)—return inmate id or -1 if wrong passkey or inmate id is not available.

[0187] Passkey may be defined as a predefined string used for security purposes. Int PutInmateID (string PassKey, string id)—store a new id on the device. Bool ChangePassKey (string currenPassKey, string newPassKey)—change the passkey.

[0188] Int GetDevice serialID (string PassKey)—get a unique serial id (optional).

[0189] The following functions lock the player if the special driver is not available. The kiosk application locks the player after download and unlocks it again before the next download:

[0190] Bool LockDevice (string PassKey)—disable the device from receiving any files until unlock function is called; and

[0191] (Bool UnLockDevice (string PassKey)—enable device for receiving any files. Bool RemoveLock (String passkey)—remove the locking (i.e. allow receive files from any source).

[0192] With reference to FIGS. 18-19, additional embodiments of a system 1000 for enabling purchasing, recording, displaying, and managing visual and video media in digital format, include a portable player system 2000, and a general access kiosk system 3000. The following described elements of system 1000 can implement all of the features described hereinabove for corresponding elements of the invention, including the features as described below.

[0193] With reference to FIG. 18, portable player 2000 is sized and shaped to be easily carried by a person, for example an inmate. In one embodiment, player 2000 is sized to fit in an ordinary pants or shirt pocket, for example less than 7×5×1 inches in dimension and 1 pound in weight. In another embodiment, player 2000 is sized larger than a typical pocket, but still sufficiently small to be easily carried about using one hand of a person, for example having a dimension of less than 10×15×2 inches, and less than 5 pounds in weight. In either size embodiment, a typical dimension and weight may be substantially smaller than the exemplary dimension and weight given, for example half of this dimension and weight or less. Player 2000 can be provided to inmates, and if permitted, used within an inmate's cell.

[0194] Player 2000 includes an electronic computing player device 2100 having a video display 2102, for example a TFT LCD, IPS LCD, OLED, or AMOLED type display. Display 2102 can be touch sensitive, for example including capacitive or optically sensitive elements (not shown), configured to pass information to a processor 2014 within device 2100, indicative of a location of a pointing object moved upon or near display 2102.

[0195] In the embodiment shown in FIG. 18, player device 2100 is wholly or partially contained within a housing 2200, operative to protect player device 2100. For example, housing 2200 may prevent access to the constituents of player device 2100, to prevent misuse of these components by inmates. Additionally, or alternatively, housing 2200 provides cushioning for shock, for example from dropping player 2000, and can protect player device 2100 from exposure to moisture, heat, or other environmental hazard. In one embodiment, only display 2102 is exposed exterior of housing 2200, although housing 2200 may additionally include a transparent layer covering display 2102.

[0196] One or more control switches or buttons 2210 located on an exterior surface of housing 2200 can be pro-

vided, communicative with corresponding switches, buttons, or other control feature or function of player device 2100, for example using a mechanical actuator, or electrical signal. Similarly, one or more electrical ports or outlets may be provided in an external surface of housing 2200, electrically communicative with a corresponding port within player device 2100, for example an audio port 2204 connectible to a sound transducer 2108, or a data exchange/charging port 2106, connectable to another computing device.

[0197] Player 2000 can be powered by a rechargeable battery, for example a lithium based battery, which may be recharged for example by connecting player 2000 to a power source. Alternatively, player 2000 may be powered by replaceable batteries, or solely by a power cord connectable to a power source, for example a wall outlet or power converter. There are security considerations attendant with each option, which can be considered by correctional facility staff. Player 2000 can provide storage of digital information by any known or hereinafter developed method, including flash memory or magnetic media. In one embodiment, player 2000 includes 8 GB of storage, although 16 GB or 32 GB may be provided as options, for example, or in the future, much higher storage quantities may become available, with considerations given to cost, size, and power requirements. Because player 2000 is permanently sealed, in one higher security embodiment, memory or batteries may not be replaced after player 2000 is configured and finally assembled. Herein, correctional facility staff includes all agents authorized to conduct acts on behalf of, or for the benefit of, the correctional facility.

[0198] With reference to FIG. 19, a computer system to which player 2000 may be connected includes stationary computer system, or kiosk 3000. The connection between player 2000 and kiosk 3000 may be established using data port 2106 and a cable connected to a corresponding port (not shown) within kiosk 3000, or by any other known or hereinafter developed means, including Bluetooth (a registered trademark of Bluetooth SIG, Inc., a Delaware corporation) or other form of wireless connection. One or more human interface devices can be provided, for example a keyboard 3002, which may be substituted with a touchscreen keyboard, for example, and a pointing device 3004, for example a trackball, also replaceable with a pointer moveable upon a touchscreen. Kiosk 3000 further includes an internal processor 3014 (not shown). A video display 3006 is provided, as well as a microphone 3008, one or more speakers 3010, which can be provided as a handset 3012, or as separate components connected to kiosk 3000, and a video camera recorder 3016. One or more locks or security devices 3018 can be provided, operative to secure from access, turn off, configure, or disable one or more functions or components of kiosk 3000. Kiosk 3000 can be fabricated from rugged materials which cannot be broken or opened without tools.

[0199] One or many kiosks 3000 may be provided at each correctional facility, for example in each dormitory. Each kiosk executes software, which can be stored upon non-volatile memory or other digital storage medium, the software operative to carry out the instructions and functions described herein. Some instructions may be executed remotely, using another computer and a network, for example a LAN or WAN, including the internet. Players 2000 and Kiosks 3000 may be configured to support video visitation, described further herein, as well as email, online banking, and a digital store, provided all forms of digital content, including music,

books, and videos. In addition, inmates and other users may order from a commissary associated with the correctional facility. Further, educational materials, including prerecorded and live instructions can be provided. Not all applications which can be provided by player **2000** and or kiosk **3000** would be deemed suitable for all inmates at all times, but such functionality can be provided for workers or visitors to correctional facilities, and can include games, gaming, and other forms of entertainment. All applications may be provided on both player **2000** and kiosk **3000**, or the range of applications on each may be different. Individual application may differ between each of player **2000** and kiosk **3000**.

[0200] In one embodiment, all computing applications and functions available to inmates may be carried out by one or both of player **2000** and kiosk **3000**, and people associated with an inmate can participate with the inmate for all such applications and functions using a single website which hosts corresponding functionality.

[0201] In one embodiment, a player provides login information to access functionality of player **2000** or kiosk **3000**, for example a username and password. As kiosk **3000** may be a general use device, both a username and password may be required. Both a username and password may be required when using player **2000**, as well, or alternatively, if player **2000** is uniquely associated with a single user, for example using an internal chip identification, player **2000** can be configured to require a password only.

[0202] With reference to FIG. **20**, an email application **4002**, executable upon one or both of player **2000** and kiosk **3000**, enables an inmate to read email messages from approved senders, the incoming email subject to preapproval by correctional facility staff. An inmate may also compose, and send emails to approved recipients, such emails also subject to review and approval by correctional facility staff. Incoming and outgoing email may be flagged or identified for review by containing keywords generated by correctional facility staff, and may also be flagged, blocked, or screened for whether content may be exchanged between particular senders and receivers. The keyword list may be generated using keywords found in other inmates' emails, where certain words were found to be associated with non-approved activity. In accordance with the disclosure, the collection, monitoring, and distribution of digital content is carried out within a closed system. More particularly, the digital content, including email and video data, is under the control of software of the disclosure, so that it may not be altered, and so that its origin and contents may be known, and that the digital content cannot be altered once collected by the system.

[0203] At left in FIG. **20**, a portion of a web application image, or web image **4002**, of a web correspondence application, or web app **4000**, designed to be used by a person not an inmate (an outside user), is illustrated. To the right of FIG. **20**, separated from web app **4002** by a divider, is shown a portion of a local executable application image, or local image **5002**, of a local correspondence local executable application, or local app **5000**, useable by the inmate. In one embodiment, web app **4000** can be implemented by a web browser (e.g. CHROME, SAFARI, or FIREFOX), supported by a web server application.

[0204] Local app **5000** can be an executable program running natively on player **2000** or kiosk **3000**, for example an application written in C++, although an application running in an execution environment, such as JAVA or .NET, may also provide a suitable alternative. Local app **5000** is additionally

supported by a local server **9000** (including, as noted, local server **611**), for example a server situated upon a LAN connected to player **2000** or kiosk **3000** by a wired or wireless connection. Accordingly, the term "local" is used only for convenience, and aspects of local app **5000** may be run by a remote processor, and the local server may be very remotely located with respect to a machine executing local app **5000**.

[0205] The web server or local server provides functionality which can include generating images or visible content; performing calculations; storing, retrieving, forwarding, and manipulating data; implementing security and limiting access rights; communicating with other servers, for example a payment server; and other functions, as described herein and as understood within the field. It should be understood that some or all functions of a web server or local server may be carried out by one or more of a kiosk **3000**.

[0206] An advantage to providing a web style application for outside users is that there may be many outside users, and not all of them may wish to install an executable style application on their computer. Further, by providing a web application, outside users can communicate with inmates wherever they may be located, without a requirement of having access to a computer upon which a corresponding executable is stored. An executable is advantageous for inmates using player **2000** or kiosk **3000**, because it is imperative that only a predefined set of activities are possible, and a self contained executable program provides the greatest level of control and security. Additionally, the set of computers upon which these functions are to be carried out is limited and known in advance, enabling deployment of an executable to be expeditious. Notwithstanding the foregoing, it is still possible for either or both of the inmate systems or outsider systems to use either a browser based application or an executable application.

[0207] Although web app **4000** and local app **5000** are shown together, it should be understood that they operate independently, the product of each stored until it can be delivered to the other, unless there is real time communication being carried out between the applications, as described further herein. It may be seen that web image **4002** illustrates services for adding attachments, a subset of the functionality of web app **4000**. An inmate name, to whom the communication is to be directed, is shown selected **4004**. This name may be typed in, or may be selected using a search and or drop-down list functionality.

[0208] An outside user may additionally select an image attachment function **4006** for attaching one or more images in any of a plurality of formats, and record videos, e.g. to produce a videogram, in real time. With respect to the latter, the sender may select a record video function **4008**, at which time they will have an opportunity to record a video message for sending to the inmate using a video camera within, or connect to, their computer. Alternatively, an outside user can select an attach video function **4010** to send one or more previously recorded videos in any of a plurality of formats. An outside user may additionally enter the text of the message **4012**, as well.

[0209] As may further be seen, there can be a charge for each message or attachment, here a value of "1 stamp" for each page. A stamp can be assigned a monetary value in a previous agreement with a system user, separately, or a value can be established when composing the message. In accordance with the disclosure, an outside user can pay for communications for and on behalf of the inmate. Similarly, an

inmate can pay, as well, although due to security restrictions, the inmate allocates credits assigned to the inmate within the system 1000 of the disclosure, to make payments. In this manner, it may be controlled what an inmate is buying. Inmates can acquire credits through their services rendered within the correctional facility, for example, or as paid for by an outside user. An outside user may provide credit for the inmate separately from using web app 4000, or may provide credit as shown in the Pre-paid Response section 4016, or other portion of web app 4000 not shown in FIG. 20.

[0210] Local app 5000, running on player 2000 or kiosk 3000, can have the same functionality as described herein for web app 4000, and vice versa, with particular functionality shown for web image 4002 or local image 5002 for convenience, and not to suggest the functionality is exclusive to one application or the other, unless stated otherwise. In FIG. 20, Local image 5002 shows a 'Take Picture' function 5018, wherein an inmate may take a picture (snapshot image) of the prerecorded or streaming video being shown to the inmate, and may save this image to an inmate storage area, for example within player 2000. An outside user may save such an image to their local computer or handheld device. Additionally illustrated is a function to view received letters 5020 and to view sent letters 5022, and to create a videogram 5024, which may be a recorded video, or which may initiate a streaming video teleconference between an inmate and an outside user, where each may view each other while speaking in full duplex.

[0211] A video stream between web app 4000 and local app 5000 is illustrated in FIG. 21. It should be understood that in order to accomplish streaming video capture using web app 4000, it may be necessary to have a helper application, or web app 4000 may need to have access to certain underlying functionality of the computer that may not normally be accessible to a browser application. A typical helper application, for example, can be ADOBE FLASH, although other such applications which provide access to other hardware are available, and may become available in the future. In one embodiment, web app 4000 enables a user to enable or disable the use of hardware needed for video visitation during an ongoing web session.

[0212] In FIG. 21, in local image 5030 of local app 5000 is illustrated at right, in which an inmate 5032 is using kiosk 3000. At left, a web image 4030 of web app 4000 is illustrated, in which an outside user 4032 is using a browser and the internet to execute web app 4000 to communicate with local app 5000. In one embodiment, the inmate and outside user can see a relatively smaller image of themselves, and a relatively larger image of the other system user, the images updating at a speed sufficient to approximate real time movement of themselves and the other user. Video and sound are synchronized, as may best be implemented by the particular hardware and connection speed available, when web app 4000 and local app 5000 are executing in mutual communication.

[0213] In accordance with the disclosure, images, text, video, and any other inbound data sent to an inmate is reviewable by correctional facility staff before it is available to the inmate. Similarly, images, text, video, and any other outbound digital content, is reviewable by correctional facility staff before it is delivered to the intended recipient. To carry out this review, correctional facility may use software tools of the disclosure which execute upon player 2000, kiosk 3000, local servers, or remote servers, to digitally prescreen content to improve efficiency. For example, keywords generated from

reviewing digital content from one or many inmates may be compared with keywords present in the digital content to be reviewed. The generated keywords typically represent prohibited activities or subjects, and digital content containing such keywords may be redacted prior to delivery, or may be blocked from being received or sent.

[0214] In one embodiment, software of the disclosure places digital content in a queue or separate location, where it may be reviewed as time is available by correctional facility staff. If later approved, it may be moved to a different queue or location, for subsequent delivery. If later rejected, it may be moved to a different queue or location, for quarantine or deletion.

[0215] Digital prescreening for keywords, which herein includes phrases, images, sounds, or any other type of digitally encoded content, can be carried out by software, upon text, encoded text or data such as word processing or pdf files, video files, images, or any other digital format known or hereinafter developed. Software of the disclosure can include software modules or routines which can parse or interpret different types of digital content, for example using artificial intelligence or other methods, to detect text or image patterns or other data which may include the keyword content.

[0216] By implementing email, photo sharing, video visitation (streaming two way video sessions), and other digital data exchanges between inmates and visitors, a correctional facility significantly reduces the burden and risk of moving inmates between physical visitation locations and their cells, and minimizes potential physical contact between inmates and visitors. As the system 1000 of the invention provides prescreening, acceptable communications between inmates and outside users do not burden correctional facility staff. Further, system 1000 reduces the burden upon correctional staff to physically open and inspect paper mail, which may include contraband.

[0217] Additionally, communications between inmates and outside users which are blocked or non-allowed for an inmate can be managed by system 1000, which can implement a rules based system of enabling or disabling particular types of communication with particular individuals, or communications with approved individuals outside of a prescribed time period, or beyond an approved duration. Such rules can be established by correctional staff, and can also be established by software of system 1000. Such unapproved communications can be terminated, for example after an early warning of impending termination, or abruptly after an initial exchange of unapproved content/keywords. System 1000 can then block further communication between the inmate and outside user until further communication is approved by correctional staff.

[0218] In one embodiment, video visitation is a two way real time video and audio streaming conference, which can be schedule by the inmate or an outside user using system 1000. Video visitation can be implemented with security rules enforced by system 1000. For example, the inmate must be available during the scheduled time, and must have privileges for video visitation, the duration of the visitation session must not exceed a maximum allowable period, for example 30 minutes, particularly when using a general use kiosk, and the outside user must be preapproved for communicating with the inmate.

[0219] In accordance with the disclosure, a schedule may be made available to inmates, correctional facility, and outside users, illustrating scheduled digital data exchanges, and

particularly for audio and video streaming visitations. Security requirements of a correctional facility may require that all real time streams are scheduled, so that correctional staff can monitor such streams as they take place, or optionally with a time delay. Accordingly, the amount of time an inmate may participate can be limited, to ensure there are adequate staff available, and to control use of available resources, including for example equipment and personnel. In one embodiment, all potential participants can propose scheduled times; however, an ability to schedule a time may be restricted by participant, time, duration, subject matter, style of stream (e.g. chat, audio, or video), availability of particular monitoring staff, past conduct of an inmate, or other factors.

[0220] Referring now to FIG. 22, three local executable application display images, or local images 5040, 5042, 5044, illustrate visible portions of instances of local app 5000 executing on either a player 2000 or kiosk 3000, the images being separated by a divider in FIG. 22. In local image 5040, an offer to purchase a player 2000 is presented, the player purchasable using credits of the inmate, within system 1000.

[0221] Music may be selected and purchased, as detailed elsewhere herein. In local image 5042, it may be seen that album artwork 5046 can be viewed, together with other information, which can include the track name, artist name, and album name, and other related information about any aspect of the track, for example duration and cost. An inmate may search for music within the available music library by keyword relating to the music of interest, and may search by genre 5046, as shown in local image 5044. Purchased music may be stored on player 2000, or may be played using kiosk 3000. In one embodiment, a purchase of music must be completed on kiosk 3000, which has access to a music library or depository, and which can be updated regularly, for example daily, although a direct purchase from player 2000 can also be implemented. In addition, other digital content such as books, videos, shows, movies, news, or educational content may be provided in a like manner as described for music. Some content may be provided at no cost or charge, for example health, safety, or facility regulations, which may pertain to the correctional facility providing system 1000.

[0222] In one embodiment, music samples or segments of songs or other digital content may be listened to by an inmate prior to purchase. This is particularly important to avoid confusion, particularly if the content library or catalog from which the inmate may select contains millions of songs or videos, many of which may have similar names.

[0223] In one embodiment, illustrated in three local executable application images, or local images 5050, 5052, 5054 of FIG. 23, inmates may purchase products, for example using credits, from an approved supply location, for example a commissary of the correctional facility. In local image 5050, an inmate may search by category 5056, then may select a size 5058 of an item within the category, although any shopping cart style implementation can be used. In this embodiment, once an item is selected, more information 5060 can be displayed, for example images of the item, the quantity desired, a description of the item, the price, a total, and an opportunity to check out 5062, or summarize the purchase transaction. In local image 5054, a summary 5064 of information pertaining to the items to be purchased is shown, and an inmate may click or indicate 'select' 5066 to complete the transaction, which can result in credits of an inmate's account being deducted, or credited if returns are permitted.

[0224] In an embodiment, the inventory available is the same as product currently available in an existing commissary system of the correctional facility, or alternatively, may include product which is available elsewhere, and is supplied to a local commissary or package distribution department, for distribution to the inmate. System 1000 can be electronically integrated with a local commissary system, and as described herein, can manage a system of credits allocated to an inmate, including accepting transfers of money by outside users, to allocate credits for inmates. All aspects of system 1000 are thus advantageously integrated, to avoid duplication of work, and to obtain synergy and reliability of the whole, including the integration of purchasing, communication between inmates and outside users (including correctional staff), allocation of credit to inmates, storage of digital content purchased by inmates, and review, analysis, and storage of inmate communications.

[0225] In FIG. 24, two local executable application images, or local images 5070 and 5072 are illustrated. In local image 5070, an inmate may submit a request for support pertaining to the use of system 1000. As with other communications by inmates, these communications can be prescreened by system 1000 for keywords, and may also be screened, and responded to, by correctional staff. Support ticket requests may also be routed to an administrative support organization associated with an implementer or provider of system 1000.

[0226] In local image 5072, an inmate may submit a grievance, request, or notification to correctional staff, who can answer within system 1000. As in all aspects of system 1000, inmates and outside users, which includes correctional facility staff, can be notified by email, or other alert, for example an alarm within system 1000, or a text message sent to the users cell phone, of events within the system. Further, system 1000 can integrate with and accept data from email and text messaging, whereby outside users can submit communications to system 1000 using these methods, or other communication methods available to outside users, generally. A drop down text box 5076 enables the inmate (or if web app 3000 an outside user) to select from a list of possible subjects.

[0227] The grievance request can pertain to problems an inmate is having with system 1000, or any other problem, concern, or notification the user wishes to communicate to correctional staff. As with local image 5072, a drop down text box 5078 enables a selection of possible grievance subjects. As with all communications within system 1000, limits can be placed on size, content, and frequency of communication, by inmates, outside users, and or staff.

[0228] Admin image 6100 is a portion of a screen image generated by an administration software application, or admin app 6000, of system 1000. Admin app 6000 provides a central administration system for managing support and grievance requests, as well as any other matters described herein which are managed by correctional staff, and or an administrator of system 1000. Admin app 6000, among other functions, enables a support or grievance ticket, representing a support or grievance request 6102, to be reviewed and responded to 6104 by appropriate staff. In the example of admin image 6100, a correctional staffperson is resolving a question of an inmate, in a communication with an administrative staffperson associated with system 1000.

[0229] With reference to FIG. 25, a banking system application, or bank app 7000 for use by inmates is illustrated. In accordance with the disclosure, negotiable funds in currency are converted to credits which may be allocated by the inmate

for the purchase of authorized items or services within system **1000**. Portions of two banking images **7002** and **7004**, illustrative of screens generated by banking app **7000**, are shown. In banking image **7002**, an inmate may allocate credits or funds from a first account to a media account **7010**, for the purchase of digital content as described herein. In one embodiment, an inmate may also allocate credits or funds from a first account to purchase “stamps” **7012**, as described herein, which may be used for particular activities, including for example digital correspondence or inbound package or mail shipments. In banking image **7004**, an inmate may view a summary or detail **7014** of activity affecting their account, and may request a printout **7016** of their account, if a printer is available. A portion of the printout **7018** appears in image **7006**. Bank app **7000** can provide a complete trust account banking and accounting system for inmates, or can supplement or complement a trust account system of a correctional facility.

[0230] In FIG. 26, music image **5100** depicts a screen image generated by music playing software of local app **5000**, in this example executing upon player **2000**. A plurality of fields **5102** indicate information pertaining to the track currently playing, and can additionally display the total number of tracks available and the duration of the current track **5104**, and or the rating **5106** given by the inmate. It can further be possible to sort available tracks **5108**. Many other functions not shown in the figures, but known in the art or hereinafter developed, may be supported by player **2000** and kiosk **3000**. Further, while the images are in black and white, as required herein, it should be understood that displays **2102** and **3006** can display color. In an embodiment, other tasks of player **2000** or kiosk **3000**, as described herein, may be carried out while music is being played. Player **2000** can further include, for example, an FM radio application and receiver, a clock, and games.

[0231] In one embodiment, player **2000** includes a setting section of local app **5000** which contains or encodes identification information, for example the inmate name and or an identification number, for the inmate to whom the player **2000** was assigned. This identification can be displayed on a home or startup screen, as well, so that correctional staff can quickly ensure the player belongs to the inmate who is in possession of it. Further, the identification information cannot be changed by the inmate, and is used by the kiosk or local server when communicating with player **2000**, to ensure content is delivered only to the appropriate player and inmate. Local app **5000** configured for player **2000** further ensures that player **2000** cannot be connected to any other than devices of system **1000**, for example kiosk **3000** or local server **9000**, which devices will preserve and observe encoded security measures. An attempted connection to another device can trigger a failure message upon the display, and can activate an alarm sound or communication of the event to local server **9000** and or kiosk **3000**, for example the next time player **2000** is connected thereto.

[0232] In one embodiment, when an inmate wishes to use kiosk **3000**, they can be required to enter a username, for example their offender ID#, and a corresponding password. Accordingly, a preregistration and assignment of a password can be required to be carried out before use of a kiosk **3000**. System **1000** may assign an initial password, after which an inmate can be required to change the password. Support can also be provided for a lost or compromised password, and optionally notification to correctional staff of the event.

[0233] The foregoing description of possible implementations consistent with the present disclosure does not represent a comprehensive list of all such implementations or all variations of the implementations described. The description of only some implementation should not be construed as an intent to exclude other implementations. Artisans will understand how to implement the disclosure in many other ways, using equivalents and alternatives that do not depart from the scope of the following claims. Moreover, unless indicated to the contrary in the preceding description, none of the components described in the implementations are essential to the disclosure.

[0234] More particularly, in accordance with another embodiment of the disclosure, and with reference to FIG. 27, outside users of system **1000** can conduct video visitation using a commercially generally available mobile computing device **8000**, including a cellphone, handheld tablet, or laptop. Mobile device **8000** executes software which is a part of system **1000**, and accordingly mobile device **8000** forms part of system **1000**, and enforces the security measures described herein. More particularly, a mobile software application, or mobile app **8100**, stored within mobile device **8000** and executing within mobile device **8000**, submits all digital content for preapproval by correctional staff, and no digital content is forwarded to an inmate until it has met all security requirements, which can include approval of the sender, approval of the digital contents, approval of the time, and authorization of the inmate, for example. Herein, all streaming content is subject to real time review by correctional staff, who can discontinue the stream if an attempt is made to exchange non-allowed content.

[0235] While it is advantageous to carry out the disclosure using a small lightweight device, such as mobile device **8000**, which is optimized to be easily used while being held in one hand, it should be understood that the discussion herein with respect to mobile device **8000** can also apply to laptops and desktop computing devices, as well.

[0236] In one embodiment, correctional staff can optionally impose a streaming time delay if deemed necessary, whereby staff has time to block content before it is heard by a user. The time delay can be imposed in one or both directions, whereby content provided by either the outside user or the inmate can be subject to pre-review. When the time delay is imposed, the sending user must wait at least for the time delay period in order to receive a corresponding reply from the receiving user.

[0237] To produce quality results, it is advantageous for the mobile computing device to be connected to a network in communication with player **2000** or kiosk **3000** of sufficient bandwidth to produce the appearance of smooth, timely motion and sound for each participant. This may typically be accomplished with, for example, a 3G, 4G, or wired or wireless internet connection, where the internet connection has sufficient bandwidth, for example at least 1 Mbps.

[0238] With further reference to FIG. 27, it may be seen that an inmate can communicate with an outside user using mobile device **8000** from a kiosk, using a network indicated by arrow “A”. In one embodiment of the disclosure, it can also be possible for an inmate to communicate with an outside user using a player **2000A**, which is similar to player **2000**, but includes a video camera recorder **2016** and a microphone **2008**, and optionally a speaker **2010**, using a network indicated by arrow “B”. In one embodiment, an inmate cannot use player **2000** to communicate unless correctional staff autho-

size such use using system **1000**, for example authorizing communication during a particular time period, for communicating with a particular outside user, and optionally only when correctional staff are available to monitor the communication. Software of system **1000**, executing within player **2000**, enforces these rules, for example obtaining such authorization wirelessly from a local server of system **1000**.

[0239] Networks “A” and “B” are typically non-wired over at least a portion of the communication channel, for example between mobile device **8000** and a cellular network. Kiosk **3000** is typically connected to the internet using a wired connection, and therefore the remainder of network “A” could be wired. In the case of network “B”, player **2000** or **2000A** can communicate wirelessly using an internal transmitter and receiver, but may communicate to a local server which is wired to the internet. Alternatively, it is possible for kiosk **3000** to have a wireless transmitter and receiver, and player **2000**, **2000A** to be connected by port **2106**, and accordingly, either network “A” or “B” may be all or partly wireless, or all or partly wired.

[0240] In one embodiment, player **2000** or **2000A** plays streaming or prerecorded video generated by correctional facility staff, in a one way transmission. In another embodiment, a two way communication with between one or a plurality of correctional staff, and one or a plurality of inmates is enabled by system **1000**. An example of one correctional staff and one inmate communicating is a counseling session. An example of a plurality of correctional staff and a plurality of inmates is a “town hall” meeting. Other examples, including uses for communication between a plurality of staff and a single inmate, or a plurality of inmates and a single staffperson, would be apparent to one skilled in the art. In all such implementations of system **1000**, it is not necessary for the inmate and the staffperson to be in the same room, which is likewise the case for communication between inmates and outside users. In all cases, the burdens of moving inmates between locations, and the attendant security issues, are eliminated. In accordance with an embodiment, a plurality of correctional staff can either participate in, or simply monitor a data stream.

[0241] In another embodiment, a plurality of outside users can participate in a group data stream with an inmate, or an inmate together with correctional staff. The data stream can include one or a mix of chat, email, audio only, or video with audio, each participant selecting the modality of their choice. In all embodiments where multiple participants are involved, a plurality of windows may be presented on a display of a user’s system **2000**, **3000**, **2000A**, or **8000/9000** (discussed below), each window containing information pertaining to a different stream, for example different video visitation streams.

[0242] In a further embodiment, some or all video visitation or other communication sessions are stored, for later review by, for example, correctional facility staff, justice department employees, counselors, attorneys, the inmate, or the outside user. In one embodiment, participants may obtain digital content controlled by system **1000** at any time, including after an inmate is released. A fee can be charged, collected for example using system **1000**, to cover the cost of storage, or such content can be archived and made available for a profit. Moreover, all of the functionality and services described herein with respect to system **1000**, including the provision of hardware and software, digital content, bandwidth, support, archiving, data warehousing and mining, and customization,

can be made available for a fee chargeable to some or all users of system **1000**, for example according to use, relieving the correctional facility of administrative burdens and system costs, and enabling the implementation and maintenance of system **1000** over time.

[0243] In accordance with a further embodiment, inmates and or outside users can be notified, or be able to determine, when other system users are available for text chat, streaming video, or other form of communication. For example, local app **5000** can be informed when a mobile device **8000** is online and available for an exchange of digital content, for example using information pertaining to the mobile phone number, MAC address, or other identification provided by mobile app **8100** or native app **8200**, advantageously with prior approval from the outside user. In one embodiment, such notification may be enabled only after authorization by correctional staff. System **1000** enables and fosters an ability of inmates to communicate with the outside world, when appropriate, in order for inmates to be better prepared to ultimately successfully reintegrate into society.

[0244] As noted above, an outside user can use web app **4000** or mobile app **8100**. Additionally, an outside user can use software of system **1000** executing on a desktop computer or any other computing device, whether intended to be mobile or not, the software written specifically for the particular hardware environment, and not executing within a browser. Such natively executing software, or native app **8200**, can be implemented in a native language, such as C++, or may execute within a programming environment developed for the computing device, such as JAVA or .NET. Advantages of a native app can include, in some circumstances, real time toggling of different audio and video devices, near real-time detection of and reaction to fluctuating bandwidth, different sizing options (including full screen), and prioritization of frame-rate/resolution.

[0245] Additionally, the native app **8200** can more easily enable a local server **9000**, or a remotely connected server, to detect when, for example, an outside user is logged into native app **8200**. An inmate using kiosk **3000** will then be able to see that the outside user is connected to the server, and will be able to initiate a video visit using funds from the inmate’s media account. The length of the visit will be limited by the remainder of the time left on the inmate’s session, or other duration limit set within system **1000** by correctional staff.

[0246] A cellular type mobile device executing mobile app **8100**, can sometimes have different capabilities than, for example a tablet type device executing mobile app **8100**, or native app **8200**. Mobile app **8100** and native app **8200** are thus available in one or more versions, which can self configure to best utilize available hardware. In one embodiment, for example, an inmate using a cellular device could be enabled to see a particular outside user as being online, and could similarly be enable and authorized to initiate a video visit. In this event, the customer, if using mobile app **8100**, could toggle between front and back facing cameras, or alternatively, could turn off video support. Headset support can also be enabled. Tablet class mobile devices, for example, can be enabled to support resizing of a video stream, and can further be configured to prioritize a frame rate and or a resolution. Mobile device **8000** can include one or more of a video camera **8016**, microphone **8008**, speaker **8010**, display **8102**, and processor **8014** (not shown).

[0247] A desktop computing system (not shown) **9800** can also be used by an outside user, and can run a desktop app

9900 which functions as described for mobile app **8100**, and which executes software designed for a particular hardware environment, which can take optimal advantage of an ability to control hardware of the desktop computer (not shown), including toggling enablement of a camera or microphone, changing video resolution or frame rate, and engaging in other optimizations to improve the quality of streaming digital data, including video visitation data. For example, a desktop system can analyze available bandwidth, and self configure software and hardware to produce effective results, for example smooth motion and acceptable sound quality when bandwidth is low, and superior results, for example high definition video and sound, when bandwidth is high.

[0248] More particularly, mobile app **8100** or desktop app **9900** can, in one embodiment, detect bandwidth from each participant, for example at the kiosk device as well as at the mobile device **8000** or desktop system **9800**, and modify input/output to be supportable at the lowest bandwidth of either. Further, if during a streaming session, should bandwidth for one user drop, software of system **1000** executing on both ends, for both users, reconfigures to adapt for the new, lower bandwidth, advantageously within a few seconds of the bandwidth change. Specifically, the video resolution can be reduced, and can be increased again if bandwidth improves. Detection of the bandwidth change can be carried out efficiently, without using large amounts of bandwidth in the process, thereby negatively impacting available bandwidth. Bandwidth can be determined, for example, by measuring upload speed from a device.

[0249] By providing natively executing applications **8100**, **9800**, an ability to detect when a particular outside user is connected to the server is facilitated. For example, apps **8100**, **9800** can periodically poll for such data, or can be remotely notified. In this manner, an inmate at a kiosk **3000**, for example, can see who is available at a computer, and then initiate data exchange with an available outside user. As an inmate may have a limited opportunity to communicate using system **1000**, this greatly increases an inmate's ability to have positive communication with the outside, and to ultimately successfully reintegrate into the outside world. Security can be enabled as described herein for system **1000**, to restrict such communication to outside users permitted for a particular inmate. Such communication, which includes audio streaming, email, image exchange, and video visitation, can replace burdensome aspects of maintaining communication for inmates. For example, system **1000** can replace traditional phone systems, and phone visitation facilities, reduce in-person visits, and replace much written correspondence.

[0250] With reference to FIG. 28, a portion of a display generated by an administration application, or admin app **9500**, of system **1000** is illustrated. While the example shows 'mail' and 'letters', it should be understood that 'mail' or 'letters' herein refers to any digital data or content, including prerecorded emails, chats, audio messages or conversations, and video messages or conversations, all of which can be reviewed prior to distribution to an inmate, or to the intended outside user recipient. As may be seen in the column entitled "Mail" at left, there are portions of admin app **9500** for a variety of functions, including: lists of letters delivered; summary reports of all mail sent and received, which may be used to select letters, whereupon additional detail is provided; lists of support tickets delivered; searching, for example for keywords, which include text as well as sounds and images, for example sounds corresponding to words, or images corre-

sponding to people or prohibited objects or activities; mail operational reports, for all mail or focused upon inbound mail, including activities taken, and current status of particular letters; stamp usage reports; lists and detail for discarded inbound digital content; and deleted digital content that has been recovered, or that is recoverable.

[0251] At the center, in FIG. 28, are links to portions of admin app **9500** pertaining to various functions associated with inbound mail, including lists of mail pending approval; mail ready for release and delivery; selection of mail for printing; lists of mail that has been released; lists of mail that has been routed for further security checks (Inspections and Investigations); mail that has been returned to a "customer", or outside user; and mail that has been rejected for delivery, e.g. for improper content, wrong addressee, or other defect. At right, in FIG. 28, are links to portions of admin app **9500** pertaining to functions corresponding to inbound mail, but for outbound mail to outside users, for example.

[0252] FIG. 29 illustrates a screen image generated by admin app **9500** when the 'Requires Approval' item in FIG. 28 is selected. Details regarding an email are illustrated, showing the results of a keyword search performed automatically by system **1000**, in which suspicious content is summarized **9512**, in this example foreign language words flagged as requiring attention by a Spanish speaking staffperson. Additionally, a particular word **9514** is flagged by the system for further inspection. Keywords in each example may have been established by being identified in historical digital content which was problematic, the keywords added to a master list by staffpeople, or preprogrammed within system **1000**. In FIG. 29, the reviewing staffperson can read the entire message, and take an action **9516** as indicated at right.

[0253] FIG. 30 illustrates a screen image generated by admin app **9500** when the item "Send to 'Sent to I&I'" is selected in FIG. 29. In this example, the review selects from a drop down list **9518** of reasons for forwarding the digital content for additional investigation. In subsequent steps, other correctional staff can quickly understand why the digital content was forwarded to them for additional investigation, and staff can take appropriate action. Access to the digital content giving rise to the investigation is centrally stored, so that it may be access by all staffpersons involved in the initial review and follow-on investigation.

[0254] Non-Limiting Examples

[0255] Although specific embodiments of the subject matter have been disclosed, those having ordinary skill in the art will understand that changes can be made to the specific embodiments without departing from the spirit and scope of the disclosed subject matter. The scope of the disclosure is not to be restricted, therefore, to the specific embodiments, and it is intended that the appended claims cover any and all such applications, modifications, and embodiments within the scope of the present disclosure.

1. A system for managing an exchange of digital content between inmates in a correctional facility and non-inmates, comprising:

- at least one computer server having a processor and connected to software stored on non-transitory media, the server software configure to—
- obtain digital content from inmates or non-inmates,
- store the digital content until a staffperson of the correctional facility approves distribution of the digital content to an intended recipient, and

distribute the digital content to the intended recipient if approved; and

at least one inmate device having a processor, a digital display, and controls, the inmate device including software stored on non-transitory media, the device software configured to—

read stored assignment data pertaining to an inmate authorized to use the particular inmate device executing the device software,

connect to the at least one computer server and transmit information pertaining to the inmate authorized to use the particular inmate device executing the device software,

obtain approved digital content distributed by the server software and intended for the particular inmate authorized to use the particular inmate device connected to the at least one computer server, and

present the digital content.

2. The system of claim 1, the server software further configured to analyze the digital content to create a result set of keywords in the digital content.

3. The system of claim 2, the server software further configured to report the result set to a staffperson of the correctional facility.

4. The system of claim 1, wherein the digital content is video content.

5. The system of claim 1, wherein the digital content is streaming audio content, the digital audio content stored by the server software for a delay period sufficient to enable correctional facility staff to monitor and interrupt the stream if non-authorized content is streamed.

6. The system of claim 1, wherein the digital content is streaming video content, the digital video content stored by the server software for a delay period sufficient to enable correctional facility staff to monitor and interrupt the stream if non-authorized content is streamed.

7. The system of claim 1, wherein the inmate device software is further configured to:

obtain information pertaining to commissary items available for sale from the at least one server; and

enable an inmate to select and request items from the obtained information, using the inmate device.

8. The system of claim 1, wherein the inmate device software is further configured to:

obtain information pertaining to digital content available for downloading into the inmate device;

enable an inmate to select and request digital content for downloading; and

connect to the at least one server to obtain the digital content.

9. The system of claim 1, wherein the inmate device software is further configured to allocate credits assigned to the inmate to pay a cost of obtaining the digital content.

10. The system of claim 1, wherein the inmate device is configured to only carry out an exchange of digital content with at least one of the at least one server.

11. The system of claim 1, wherein the inmate device is configured to be unopenable by an inmate without using tools.

12. A system for managing an exchange of digital content between inmates in a correctional facility and non-inmates, comprising:

at least one computer server having a processor and connected to software stored on non-transitory media, the server software configured to—

obtain digital video content from inmates or non-inmates,

delay distribution of at least a portion of the digital video content until a staffperson of the correctional facility approves transmission of the at least a portion of digital video content to an intended recipient, and

distribute the digital video content to the intended recipient if approved; and

at least one inmate device having a processor, a digital display, and controls, the inmate device including software stored on non-transitory media, the device software configured to—

read stored assignment data pertaining to an inmate authorized to use the particular inmate device executing the device software,

connect to the at least one computer server and transmit information pertaining to the inmate authorized to use the particular inmate device executing the device software,

obtain the distributed digital video content distributed by the server software and intended for the particular inmate authorized to use the particular inmate device connected to the at least one computer server, and

present the video digital content.

13. The system of claim 12, the server software further configured to analyze the video digital content to create a result set of keywords in the digital content.

14. The system of claim 12, the server software further configured to report the result set to a staffperson of the correctional facility.

15. The system of claim 12, wherein the delay is sufficient to enable correctional facility staff to monitor and interrupt the video digital content if the digital video content contains non-authorized content.

16. The system of claim 12, wherein the digital content is streaming video content, the digital video content stored by the server software for a delay period sufficient to enable correctional facility staff to monitor and interrupt the stream if non-authorized content is streamed.

17. The system of claim 12, wherein the inmate device software is further configured to:

display information pertaining to commissary items available for sale from the at least one server;

enable an inmate to select and request items from the obtained information, using the inmate device.

18. The system of claim 12, wherein the inmate device software is further configured to:

obtain visual information pertaining to digital content available for downloading into the inmate device;

enable an inmate to view, select and request digital content for downloading;

connect to the at least one server to obtain the digital content.

19. The system of claim 12, wherein the inmate device software is further configured to allocate credits assigned to the inmate to pay a cost of obtaining the digital content.

20. A method for managing an exchange of digital content between inmates in a correctional facility and non-inmates, comprising:

using at least one computer server having a processor and connected to software stored on non-transitory media, the server software configure to—
obtain digital video content from inmates or non-inmates,
delay distribution of at least a portion of the digital video content until a staffperson of the correctional facility approves transmission of the at least a portion of digital video content to an intended recipient, and
distribute the digital video content to the intended recipient if approved; and
providing to at least one inmate a device having a processor, a digital display, and controls, the inmate device including software stored on non-transitory media, the device software configured to—
read stored assignment data pertaining to an inmate authorized to use the particular inmate device executing the device software,
connect to the at least one computer server and transmit information pertaining to the inmate authorized to use the particular inmate device executing the device software,
obtain the distributed digital video content distributed by the server software and intended for the particular inmate authorized to use the particular inmate device connected to the at least one computer server, and
present the video digital content.

* * * * *



US 20140280559A1

(19) **United States**

(12) **Patent Application Publication**
Torgersrud

(10) **Pub. No.: US 2014/0280559 A1**

(43) **Pub. Date: Sep. 18, 2014**

(54) **INMATE NETWORK PRIMING**

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

(71) Applicant: **TELMATE LLC**, San Francisco, CA
(US)

CPC **H04L 67/22** (2013.01)

USPC **709/204**

(72) Inventor: **Richard Torgersrud**, San Francisco, CA
(US)

(57) **ABSTRACT**

(73) Assignee: **TELMATE LLC**, San Francisco, CA
(US)

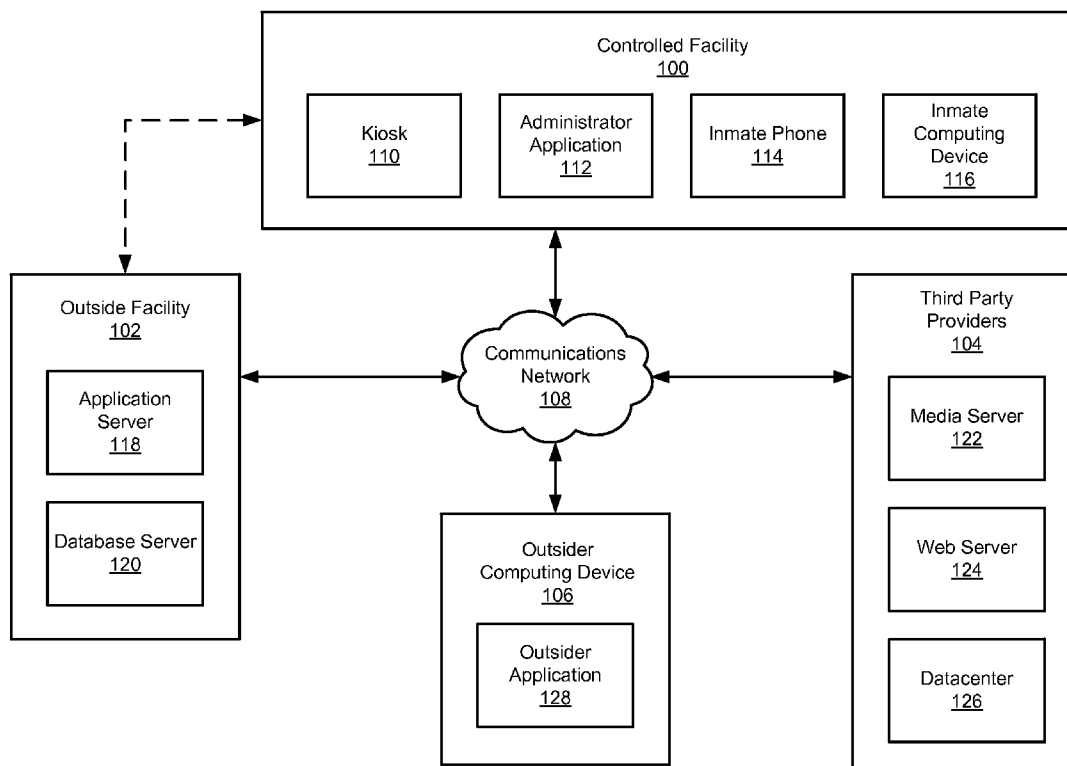
A method for network priming for an inmate of a controlled facility includes receiving authentication credentials for the inmate to access a third party social network, importing social network contacts from the third party social network, filtering the social network contacts for prohibited contacts, presenting the inmate with the social network contacts, receiving, from the inmate, a selection of social network contacts to obtain selected social network contacts, and populating a secure social network list of the inmate with the selected social network contacts.

(21) Appl. No.: **13/842,031**

(22) Filed: **Mar. 15, 2013**

Publication Classification

(51) **Int. Cl.**
H04L 29/08 (2006.01)



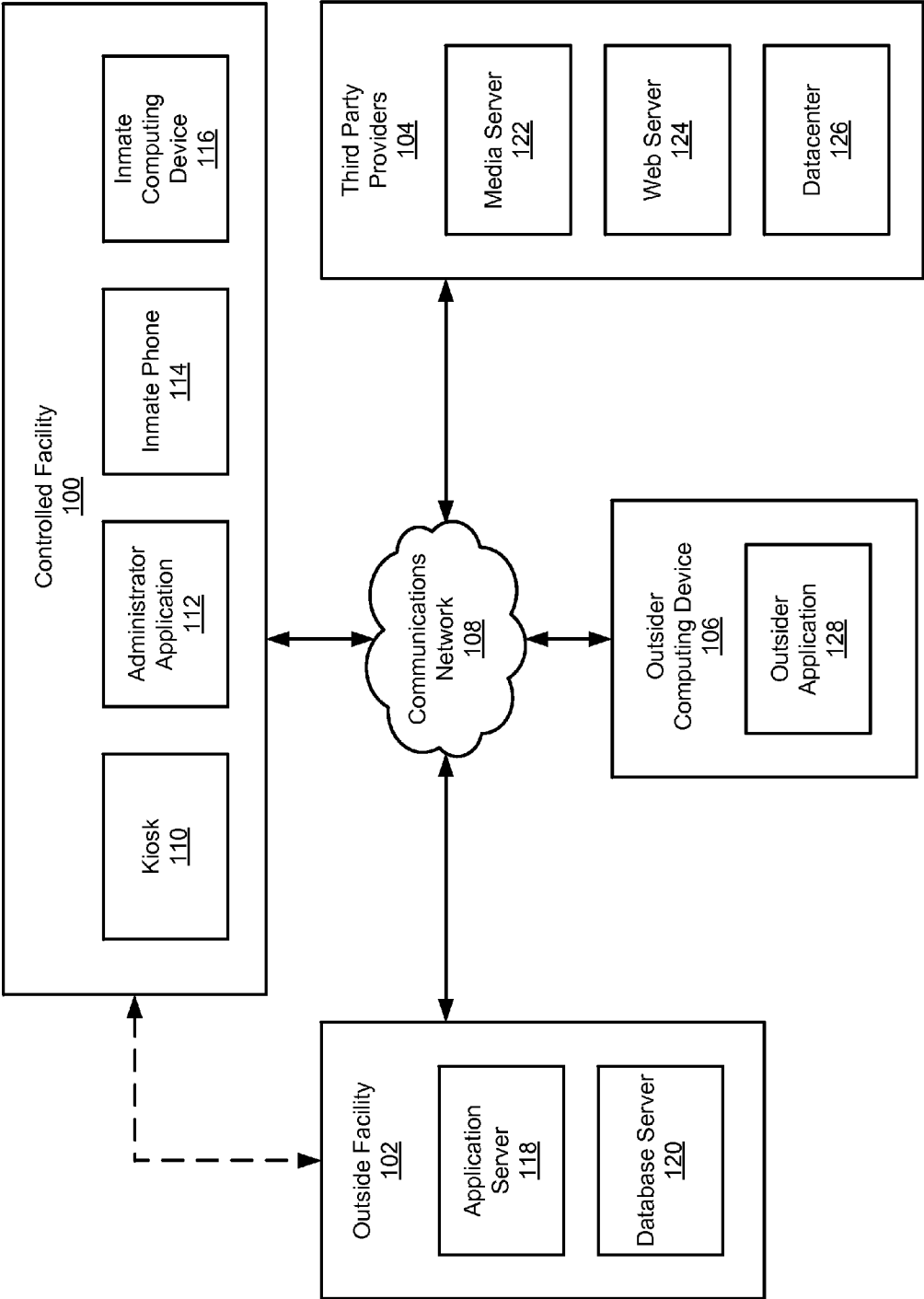


FIG. 1

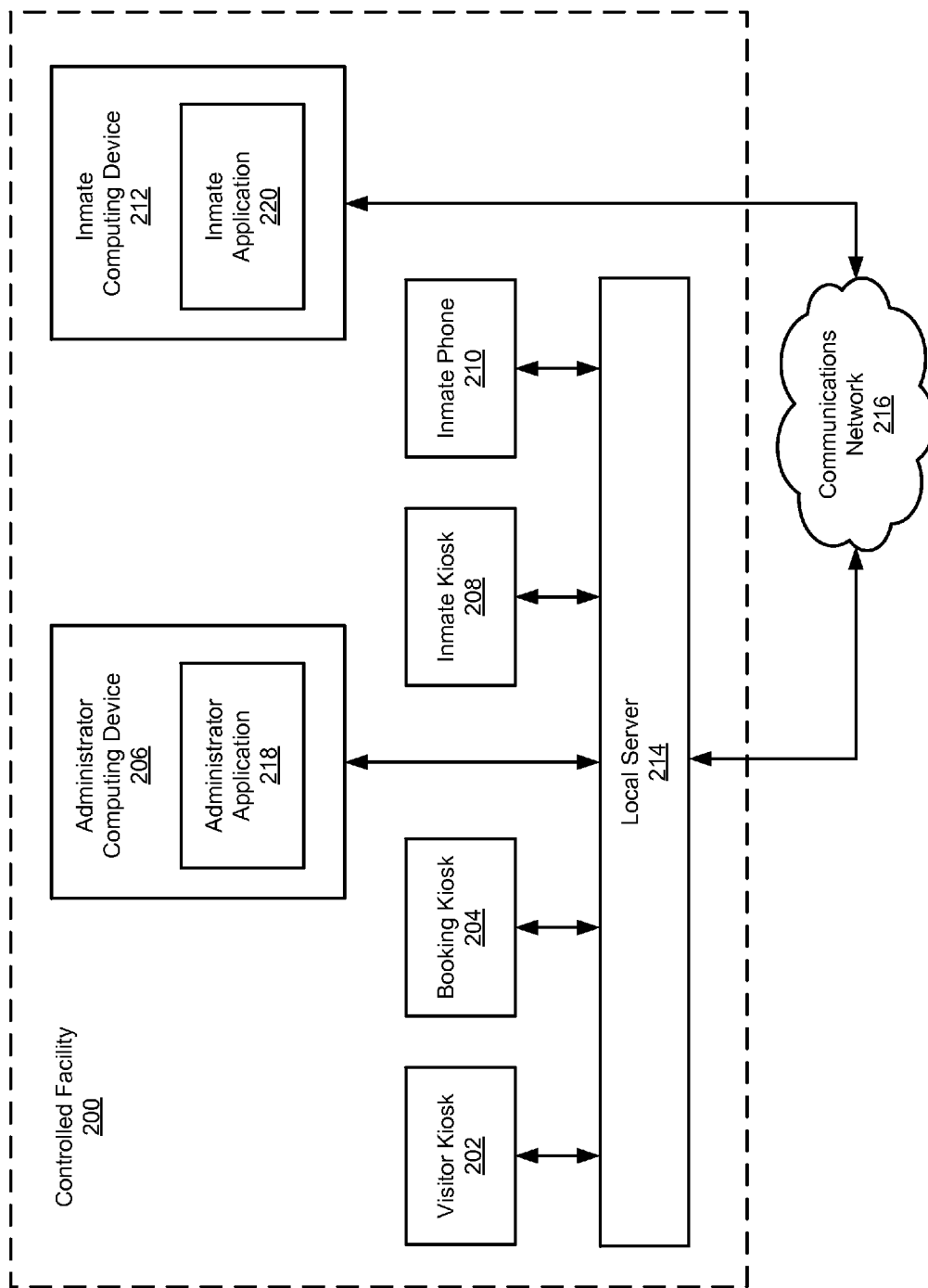


FIG. 2

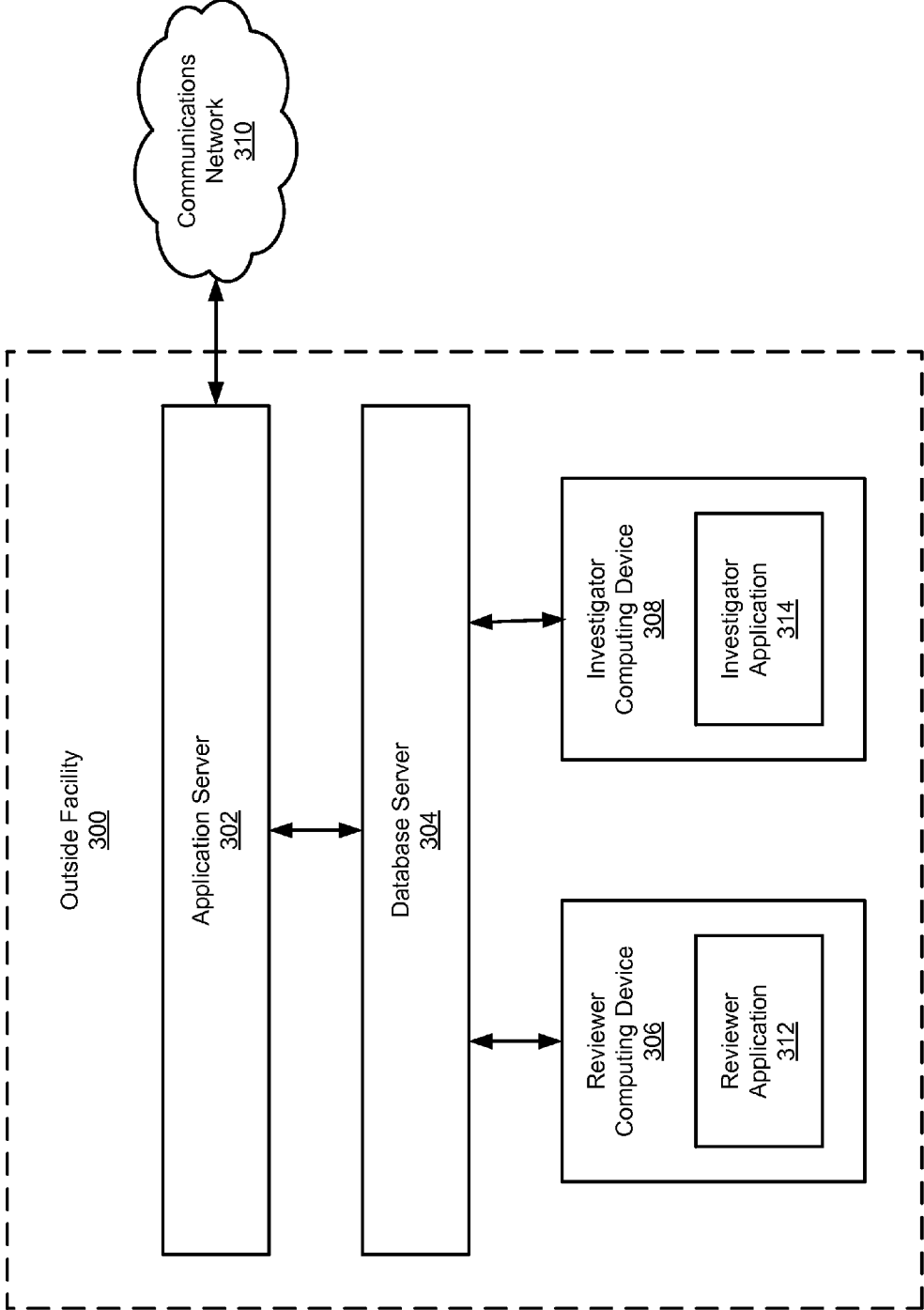


FIG. 3

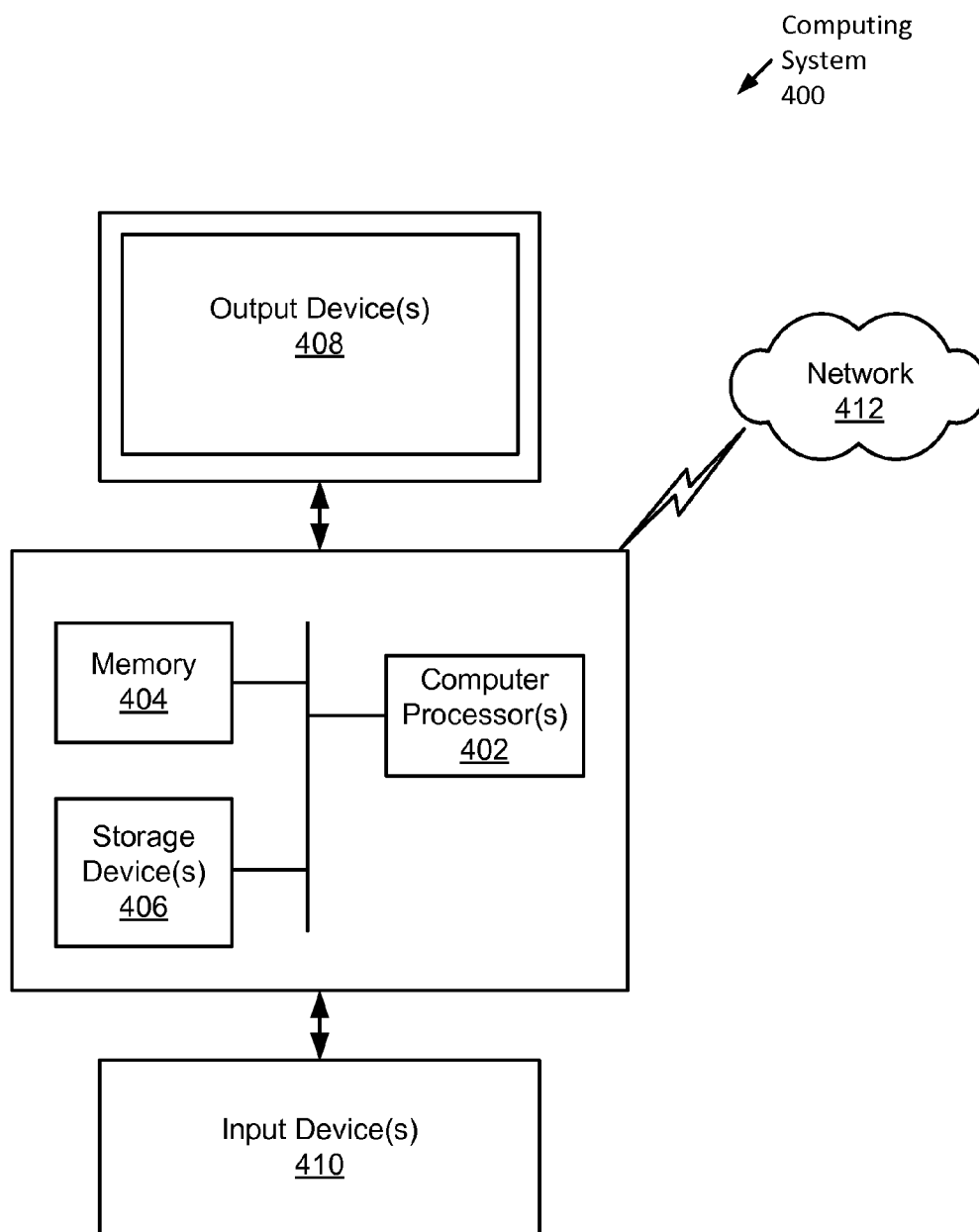


FIG. 4

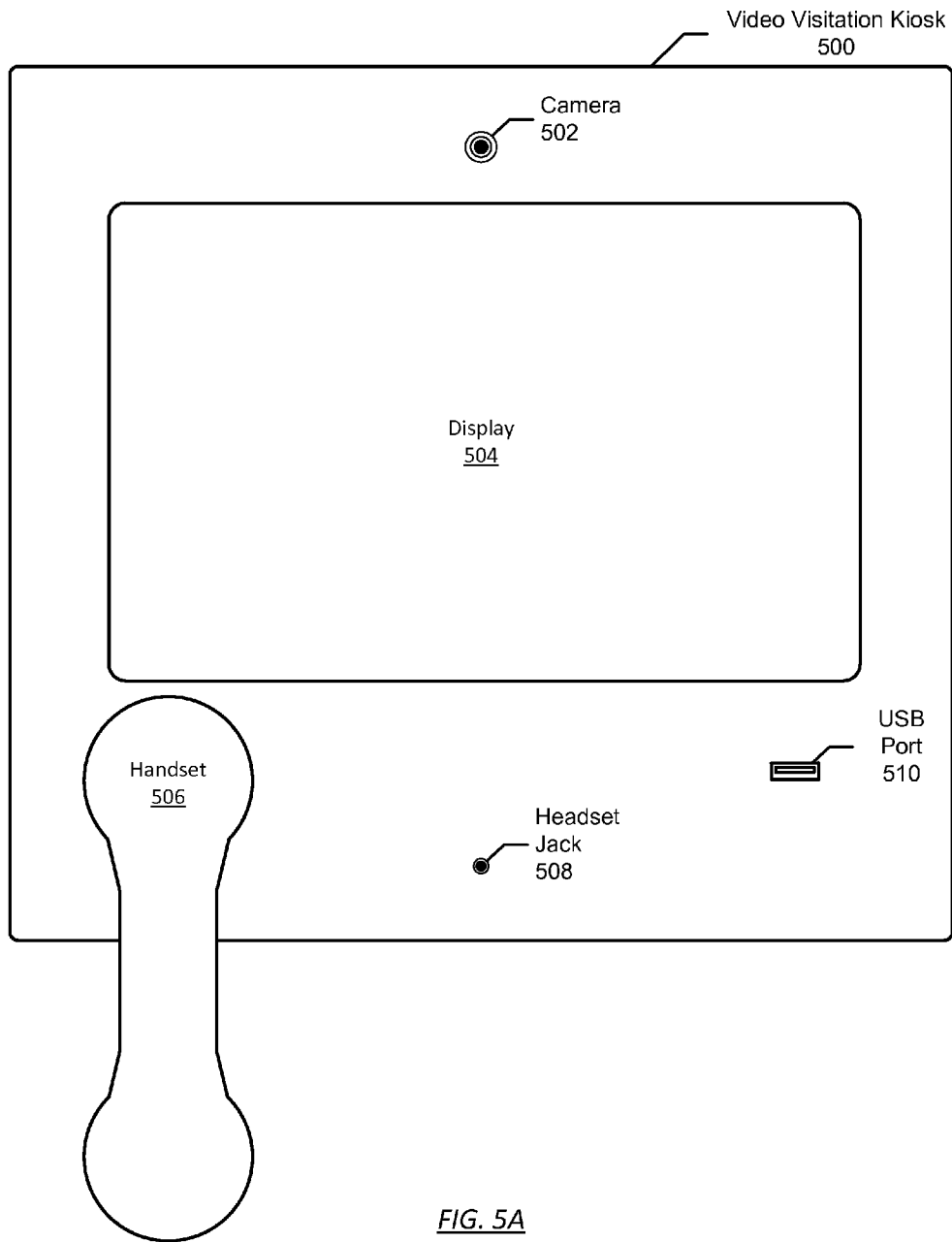


FIG. 5A

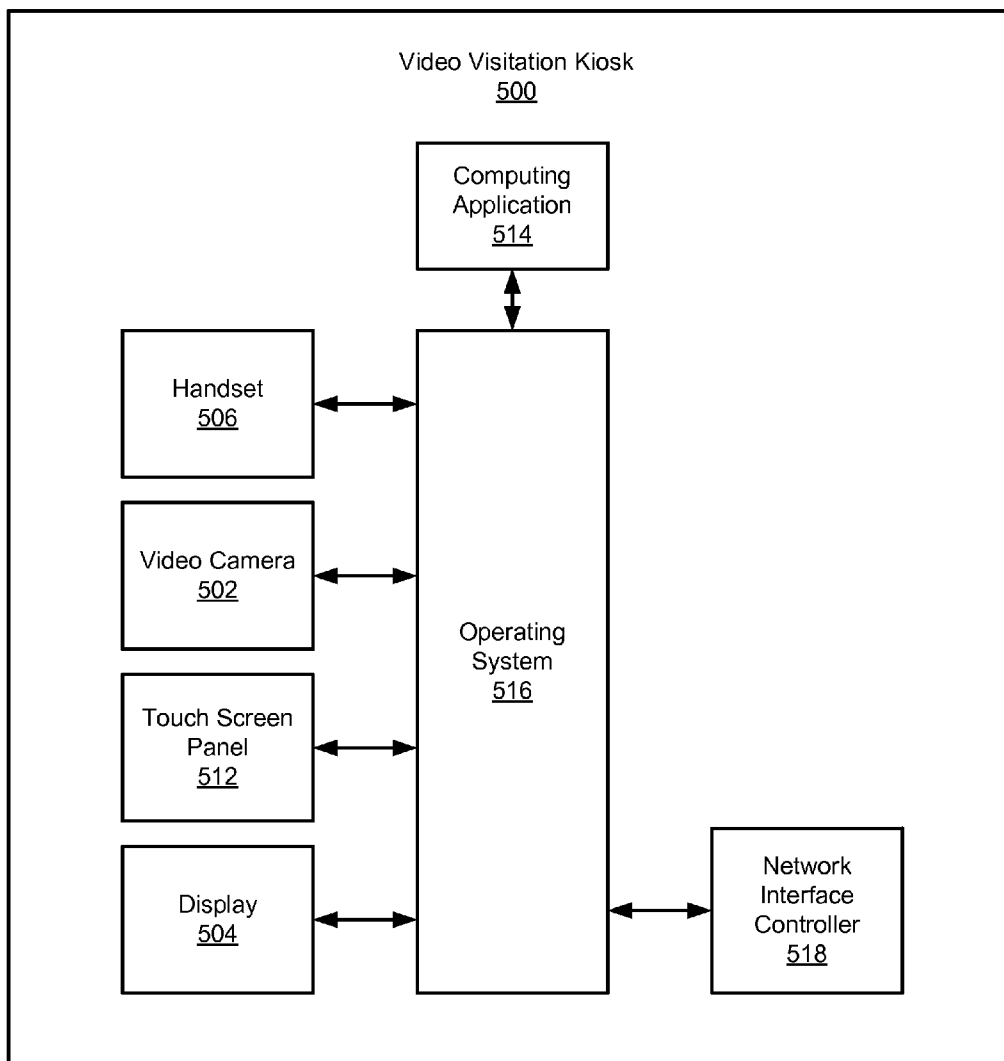


FIG. 5B

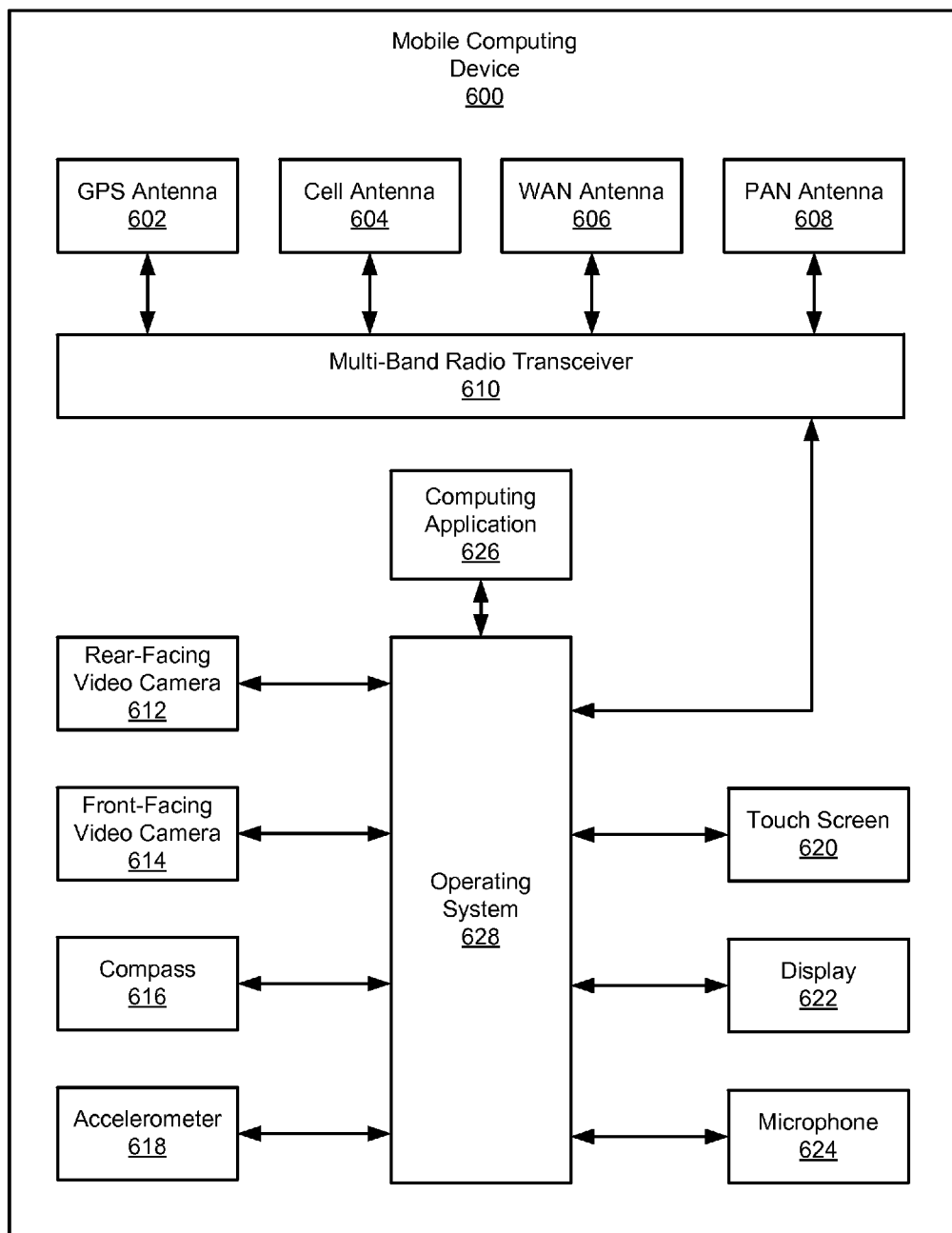


FIG. 6

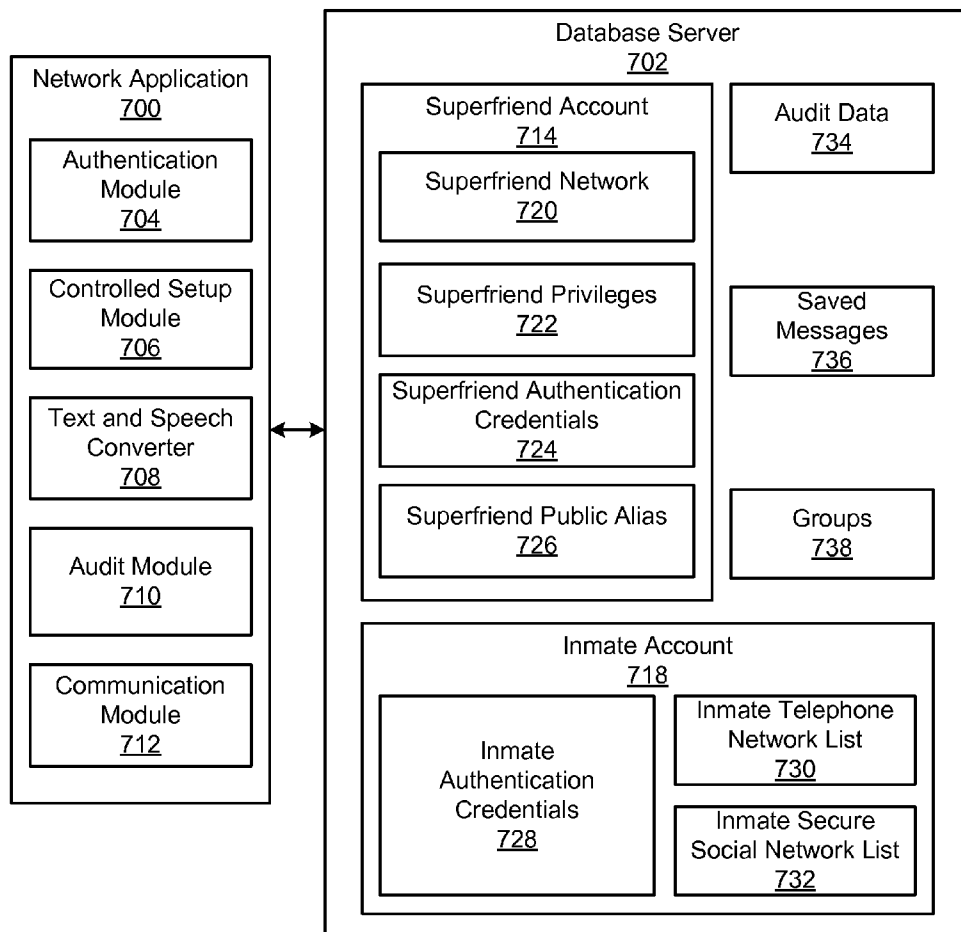


FIG. 7

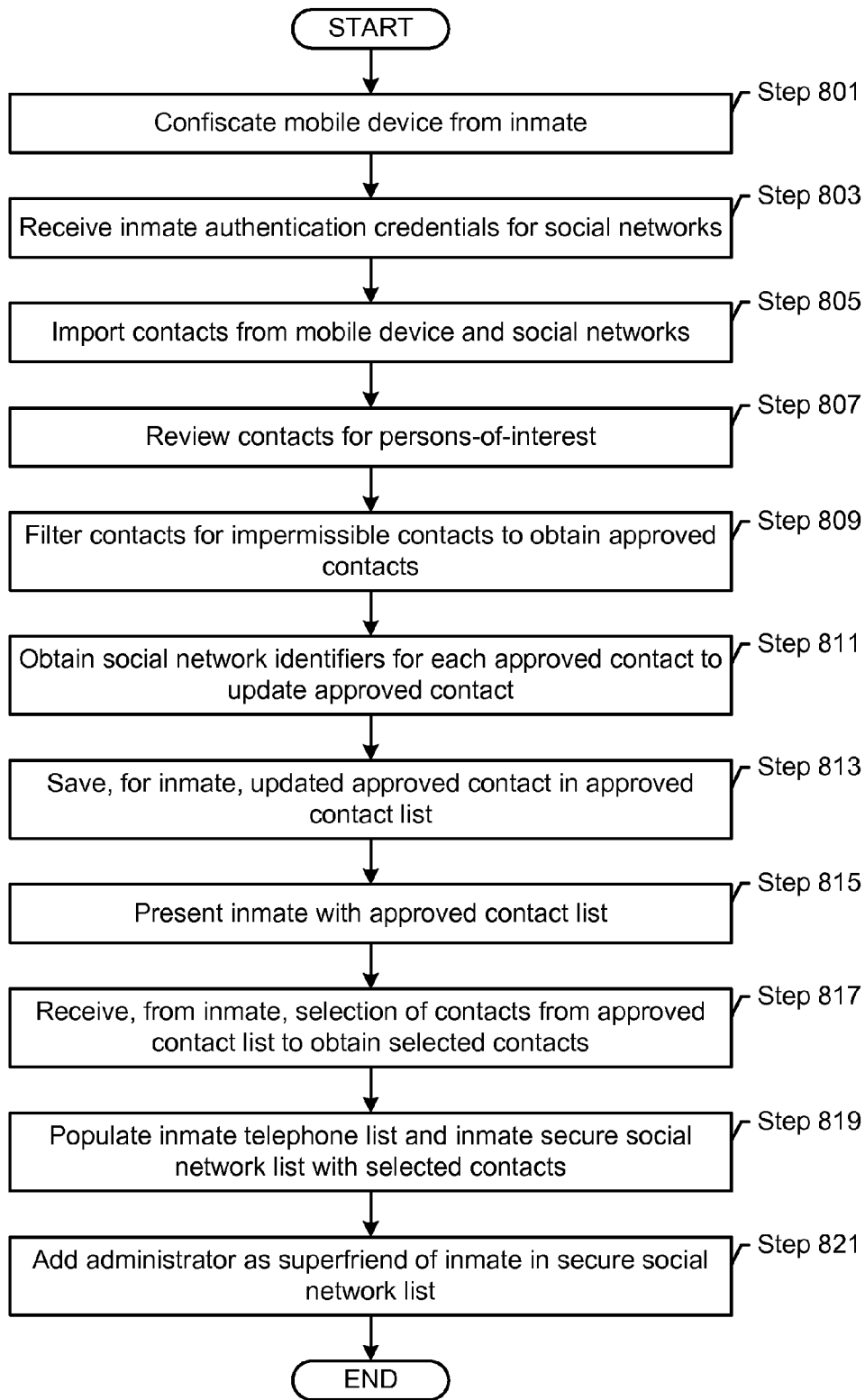


FIG. 8

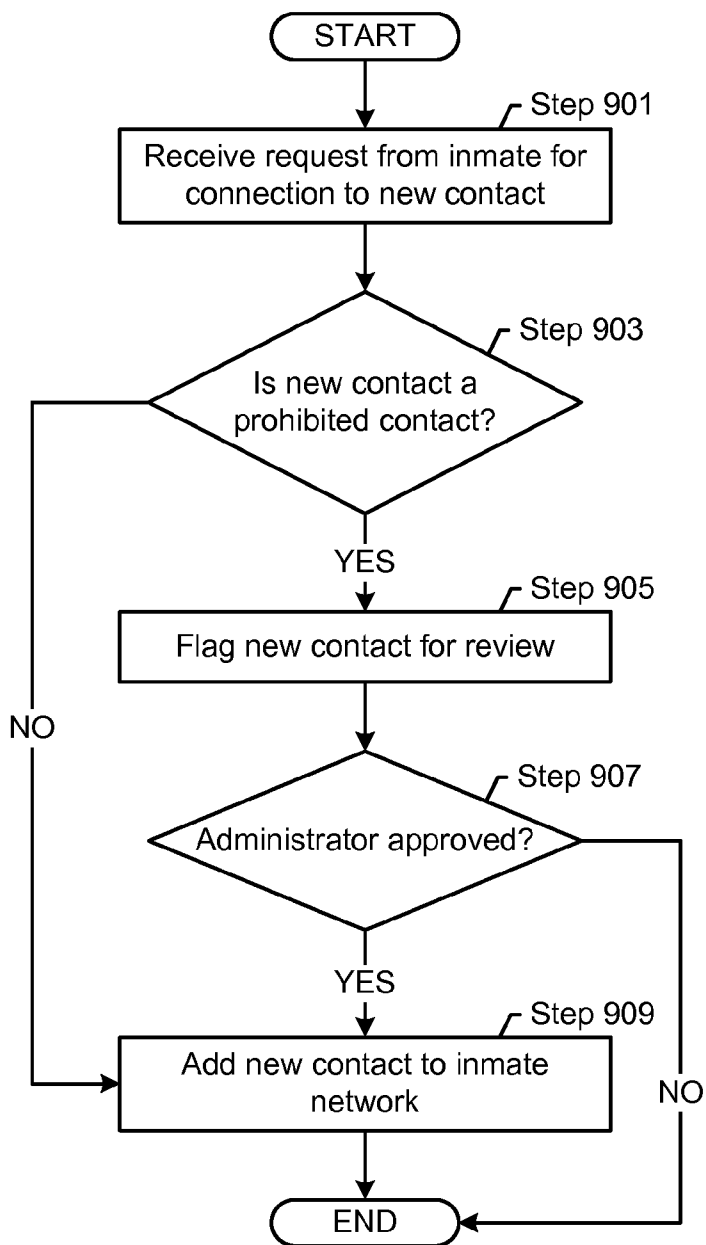


FIG. 9

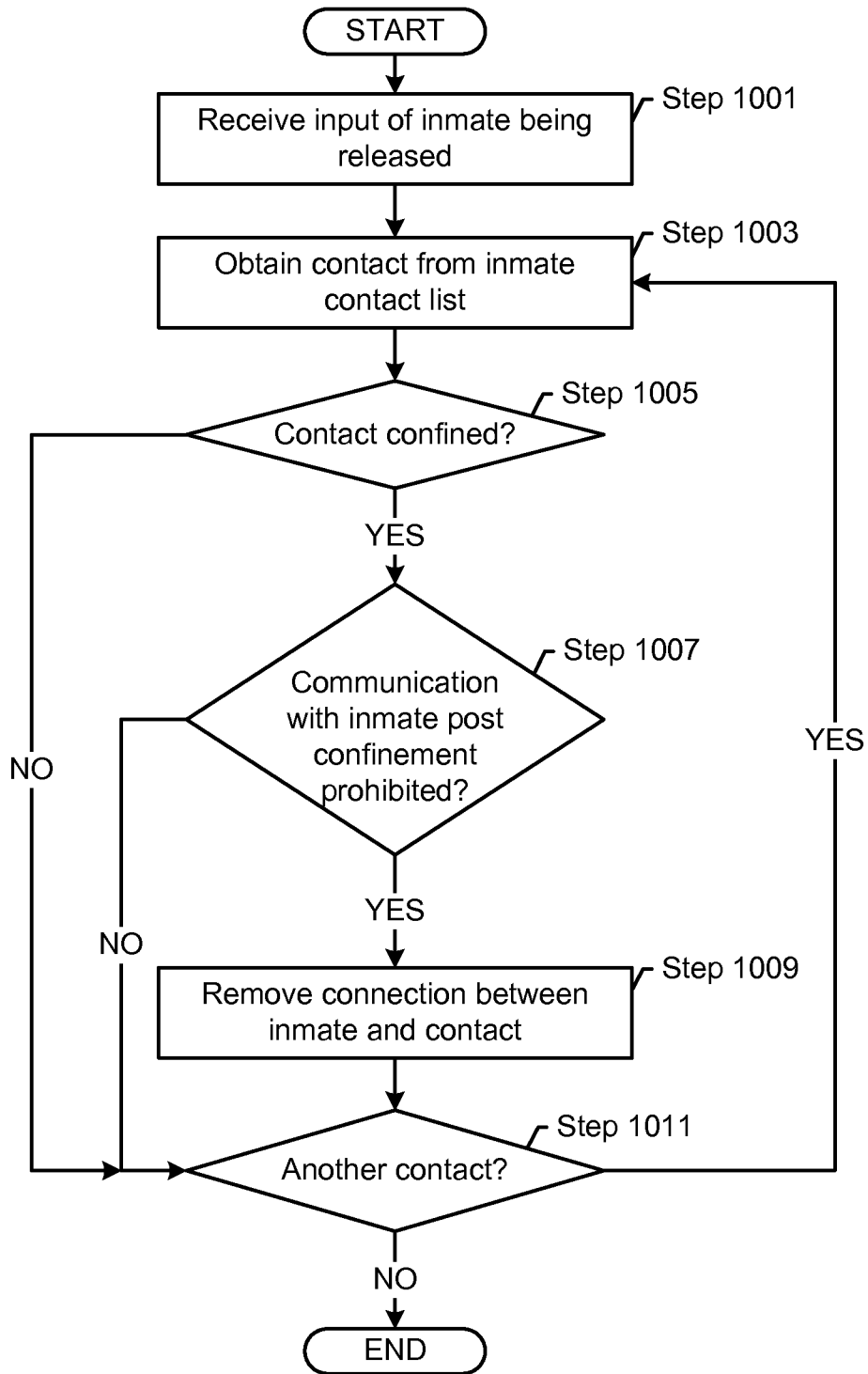


FIG. 10

INMATE NETWORK PRIMING
CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is related to U.S. patent application Ser. No. 13/438,940 filed on Apr. 4, 2012, entitled "Secure Social Network." U.S. patent application Ser. No. 13/438,940 is incorporated by reference in its entirety.

BACKGROUND

[0002] Controlled facilities, such as a jail, prison, secure detention environments, detention facility, secured hospital, or addiction treatment facility, house large populations of individuals in confinement, which presents unique administrative challenges. In such detention environments, detained individuals, such as prisoners, offenders, convicts, military personnel, patients, government cleared personnel, or other detainees, frequently desire to communicate with individuals outside the detention environment such as friends or family members.

SUMMARY

[0003] In general, in one aspect, embodiments relate to a method for network priming for an inmate of a controlled facility. The method includes receiving authentication credentials for the inmate to access a third party social network, importing social network contacts from the third party social network, filtering the social network contacts for prohibited contacts, presenting the inmate with the social network contacts, receiving, from the inmate, a selection of social network contacts to obtain selected social network contacts, and populating a secure social network list of the inmate with the selected social network contacts.

[0004] In general, in one aspect, embodiments relate to a system for network priming for an inmate of a controlled facility. The system includes a computer processor, a database server, and a network application that executes on the computer processor. The database server includes an inmate account including a secure social network list. The network application includes a controlled setup module. The controlled setup module is configured to receive authentication credentials for the inmate to access a third party social network, import social network contacts from the third party social network, filter the social network contacts for prohibited contacts, present the inmate with the social network contacts, receive, from the inmate, a selection of social network contacts obtain selected social network contacts, and populate a secure social network list in the inmate account with the plurality of selected social network contacts.

[0005] In general, in one aspect, embodiments relate to a non-transitory computer readable medium for network priming for an inmate of a controlled facility. The non-transitory computer readable medium includes computer readable program code for receiving authentication credentials for the inmate to access a third party social network, importing social network contacts from the third party social network, filtering the social network contacts for prohibited contacts, presenting the inmate with the social network contacts, receiving, from the inmate, a selection of social network contacts to obtain selected social network contacts, and populating a secure social network list of the inmate with the selected social network contacts.

[0006] In general, in one aspect, embodiments relate to a method for network priming for an inmate of a controlled facility. The method includes importing mobile device contacts from a mobile device used by the inmate, filtering the mobile device contacts for prohibited contacts, presenting the inmate with the mobile device contacts, receiving, from the inmate, a selection of mobile device contacts to obtain selected telephone contacts, and populating a telephone list of the inmate with the plurality of selected telephone contacts.

[0007] Other aspects of the invention will be apparent from the following description and the appended claims.

BRIEF DESCRIPTION OF DRAWINGS

[0008] FIGS. 1-7 show schematic diagrams of a system in one or more embodiments of the invention.

[0009] FIGS. 8-10 show flowcharts of a method in one or more embodiments of the invention.

DETAILED DESCRIPTION

[0010] Specific embodiments of the invention will now be described in detail with reference to the accompanying figures. Like elements in the various figures are denoted by like reference numerals for consistency.

[0011] In the following detailed description of embodiments of the invention, numerous specific details are set forth in order to provide a more thorough understanding of the invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these specific details. In other instances, well-known features have not been described in detail to avoid unnecessarily complicating the description.

[0012] In general, embodiments of the invention provide a method and system for network priming for an inmate of a controlled facility. Specifically, embodiments of the invention control which contacts an inmate can have in a secure social network. More specifically, social network contacts of the inmate are imported from a third party social network of the inmate. The social network contacts are filtered for prohibited contacts. In other words, contacts that the inmate does not have permission to communicate with are removed from the social network contacts. The remaining contacts are approved for communication. The inmate may be presented with remaining contacts, and select, from the remaining contacts, which contacts to add from the social network. Thus, those contacts are added to the inmate social network.

[0013] One or more embodiments may further add contacts from an inmate's mobile device. For example, if the inmate enters the controlled facility with a mobile phone, one or more embodiments add approved contacts in the mobile phone to the inmate's telephone network and/or social network.

[0014] Embodiments of the invention may include interactions with a secure social network. In one or more embodiments of the invention, a secure social network is a network application that facilitates and secures the exchange or transmission of information between two or more parties in which at least one of those parties is subject to special security or law enforcement restrictions or otherwise resides in, or is subject to the controls of a controlled facility. Exchanged or transmitted information may be member generated, such as a photo or a video message, or it may be member-curated, such as a news headline, a famous quote, or a sports score.

[0015] FIG. 1 shows a diagram of a system in accordance with one or more embodiments of the invention. As shown in FIG. 1, the system includes a controlled facility (100), an outside facility (102), third party providers (104), and an outsider computing device (106) each communicatively coupled to a communications network (108). The controlled facility (100) may include, but is not limited to, a kiosk (110), an administrator application (112), an inmate phone (114), and an inmate computing device (116). The outside facility (102) may include an application server (118) and a database server (120). The third party providers (104) may include a media server (122), a web server (124), and a datacenter (126). The outsider computing device (106) may include an outsider application (128).

[0016] In one or more embodiments of the invention, a controlled facility (100) is an access-restricted location. Examples of controlled facilities (e.g., controlled facility (100)) include, but are not limited to, detention environments (e.g., jails, prisons, etc.), immigration detention centers, military centers, government secure sites, law enforcement holding structures, secure business complexes, and psychiatric hospitals.

[0017] In one or more embodiments of the invention, an inmate is a person within a controlled facility (100) who is subject to one or more restrictions, primarily to his or her freedom or rights. Examples of inmates include, but are not limited to, prisoners, wards of the state, parolees, employees working in a secure business complex, temporary or long-term internees, patients, military personnel, uncharged suspects, and refugees. Inmate restrictions may be part of a court-imposed sentence on an inmate, while others may be specific to the controlled facility (100) in which the inmate resides. Restrictions may include limitations on an inmate's physical movement (i.e., physical restrictions) and limitations on the inmate's ability to communicate (i.e., communication restrictions). Communication restrictions include inmate use restrictions, inmate target restrictions, and device use restrictions.

[0018] In one or more embodiments of the invention, inmate use restrictions are limitations on an inmate's general ability to communicate with visitors and/or outsiders. Inmate use restrictions may include, for example, periods of time in which an inmate is not allowed to communicate with outsiders or visitors (e.g., between 10 PM and 8 AM, during an imposed one-week punitive period, etc.) and limitations based on lack of funds (e.g., insufficient commissary account balance to initiate a communication).

[0019] In one or more embodiments of the invention, inmate target restrictions are limitations on the target or source of a communication with the inmate. Inmate target restrictions may be specific outsiders or visitors with whom the inmate is not allowed to communicate (e.g., the victim of a crime perpetrated by the inmate, etc.). Inmate target restrictions may also include types of people with whom the inmate is not allowed contact (e.g., outsiders who are ex-cons, minors under the age of 18, etc.).

[0020] In one or more embodiments of the invention, device use restrictions are restrictions based on the condition or state of the communication device used by the inmate. Device use restrictions include, for example, limitations based on the location of the inmate's mobile device, limitations imposed based on a determination that the device has been tampered with, etc.

[0021] In one or more embodiments of the invention, an outsider is a person outside the controlled facility (100) who may be the source or target of a communication with an inmate. An outsider who enters the controlled facility (100) for the purpose of communicating with an inmate is referred to as a visitor.

[0022] In one or more embodiments of the invention, the kiosk (110) is a computing system with functionality to facilitate communication between an inmate and a visitor or outsider. Such communication facilitation may include creating a system identity data item or secure social networking account, adding or importing contact information for outsiders with whom the inmate wishes to communicate, uploading media (e.g., photos, videos, audio, and text) to, or viewing media from, a secure social network, sending or receiving messages or other media, acting as an endpoint for voice and video communication between an inmate and a visitor or outsider, scheduling a communication, and managing a commissary or communications account. Further detail about kiosks (e.g., kiosk (110)) is provided in FIG. 2, FIG. 5A, FIG. 5B, and FIG. 6.

[0023] In one or more embodiments of the invention, the administrator application (112) is a process or group of processes executing on a computing system with functionality to enable an administrator to create, remove, and/or enforce one or more restrictions on an inmate, outsider, or device. In one or more embodiments of the invention, an administrator is a person associated with the controlled facility charged with enforcing one or more restrictions. Examples of administrators include, but are not limited to, prison guards, orderlies, wardens, prison staff, jailers, information technology technicians, system administrators, and law enforcement agents. Using the administrator application, an administrator may retrieve or alter the identity data item and/or secure social network account of an inmate, visitor, or outsider. Further detail about the administrator application (112) is provided in FIG. 2.

[0024] In one or more embodiments of the invention, the inmate phone (114) is a device with functionality to send and receive audio communications between an inmate and an outsider or visitor. In one or more embodiments of the invention, the inmate phone (114) is a stationary (i.e., non-mobile) device. Further, a single inmate phone (114) may be used by more than one inmate. Further detail about the inmate phone (114) is provided in FIG. 2.

[0025] In one or more embodiments of the invention, the inmate computing device (116) is a computing device with functionality to enable an inmate to communicate with a visitor or outsider. Specifically, the inmate computing device (116) may be used to send or receive text messages and/or initiate or receive voice or video calls. In one or more embodiments of the invention, the inmate computing device (116) also enables an inmate to access a secure social network. Specifically, the inmate computing device (116) may be used to upload media to, or view media from, a secure social network account of the inmate or another secure social network member. In one or more embodiments of the invention, the inmate computing device (116) is a mobile computing device (e.g., a smartphone, a laptop, a tablet, etc.). Further detail about the inmate computing device (116) is provided in FIG. 2 and FIG. 6.

[0026] In one or more embodiments of the invention, the elements within the controlled facility (100) are communicatively coupled to the communications network (108). In one

or more embodiments of the invention, the communications network (108) is a collection of computing systems and other hardware interconnected by communication channels. The communications network (108) may include networks that are exclusively or primarily used for a single type of communication, such as a telephone network (e.g., Plain Old Telephone System (POTS)), and/or networks used for a wide array of communication types, such as the Internet through Voice over IP (VoIP). Communication channels used by the communications network (108) may include, for example, telephone lines, networking cables, wireless signals, radio waves, etc. Fees charged and payments received by the provider(s) of the communications network (108) may involve multiple parties, including a service provider of the outside facility (102), the management of the controlled facility (100), and provider(s) of the communications network (108). In one or more embodiments of the invention, fees may be split between multiple parties based on the terms of underlying agreements or contracts between the parties. Further, rebates, reimbursements, and/or refunds may be afforded to and paid to the management of the controlled facility (100) based on the terms of underlying agreements or contracts between the parties. For example, the management of the controlled facility (100) may receive a rebate from the service provider of the services provided to inmates based on such factors as the volume of use, the dollar amount, and/or the frequency of use.

[0027] In one or more embodiments of the invention, the outside facility (102) is a group of computing systems located outside of the controlled facility (100). Specifically, the outside facility (102) may house system elements with functionality to facilitate communication between inmates and outsiders, access communication data between inmates and outsiders, and enforce one or more restrictions imposed on inmates and inmate communications. In one or more embodiments of the invention, the outside facility (102) is connected directly to the controlled facility (100) bypassing a generally accessible communications network (communications network (108)). One or more of the components within the outside facility (102) may alternatively be located within the controlled facility (100) or within the third party providers (104).

[0028] In one or more embodiments of the invention, the application server (118) is a computing system with functionality to authenticate an inmate, outsider, administrator, reviewer, or investigator for access to system functionality (e.g., initiating voice or video calls, sending text messages, etc.) or data stored on the database server (120) (e.g., inmate identities, communications between inmates and outsiders, etc.). The application server may authenticate inmates, outsiders, administrators, reviewers, and/or investigators using passwords, biometric data, digital access codes, and/or physical access devices. Further detail about the application server (118) is provided in FIG. 3.

[0029] In one or more embodiments of the invention, the database server (120) is a computing system with functionality to store identities used to authenticate inmates, outsiders, administrators, reviewers, and/or investigators. Such identities may include verified data used to compare to verification data provided by the inmate, outsider, administrator, reviewer, or investigator to authenticate the inmate, outsider, administrator, reviewer, or investigator.

[0030] In one or more embodiments of the invention, the database server (120) also stores communication data about

communications between an inmate and an outsider or visitor. Such communication data may include, for example, a recording of a video call, the length of a voice call, the frequency of video calls, sent and received text messages, etc. The database server (120) may also store media submitted to a secure social network before, during, and/or after the media has been reviewed. Further detail about the database server (120) is provided in FIG. 3.

[0031] In one or more embodiments of the invention, the third party providers (104) are computing systems that provide network application and data storage services (i.e., cloud computing services). Third party providers (104) may include service providers used directly by inmates and outsiders, such as photo sharing services, general social networking sites, and digital music retailers. Third party providers (104) may include service providers employed by administrators and for use by inmates and outsiders, such as audio and video streaming applications, conferencing applications, and secure social network media storage. One or more of the components within the third party providers (104) may alternatively be located within the controlled facility (100) or the outside facility (102).

[0032] In one or more embodiments of the invention, the media server (122) is a computing system or group of computing system with functionality to provide network application services to facilitate communication between an inmate and an outsider, and to facilitate access to a secure social network. Such services include, but are not limited to, VoIP services, video conferencing services, and media streaming services.

[0033] In one or more embodiments of the invention, the web server (124) is a computing system or group of computing system with functionality to provide an interface to access and interact with webpages and other network application services. In one or more embodiments of the invention, the web server (124) is a type of media server (122).

[0034] In one or more embodiments of the invention, the datacenter (126) is a computing system or group of computing system with functionality to provide an interface to access and interact with data stored on one or more data servers (not shown). In one or more embodiments of the invention, the datacenter (126) is a type of media server (122).

[0035] In one or more embodiments of the invention, the outsider computing device (106) is a computing device with functionality to execute the outsider application (128). In one or more embodiments of the invention, the outsider computing device (106) is a mobile computing device (e.g., a smartphone, a laptop, a tablet, etc.). Further detail about the outsider computing device (106) is provided in FIG. 6.

[0036] In one or more embodiments of the invention, the outsider application (128) is a process or group of processes (in software, firmware, hardware, or combination thereof) with functionality to enable communication between an outsider and an inmate. Specifically, the outsider application (128) may be used to send or receive text messages and/or initiate or receive voice or video calls. In one or more embodiments of the invention, the outsider application (128) also enables an outsider to access a secure social network. Specifically, the outsider application (128) may be used to upload media to, or view media from, a secure social network account of the outsider, an inmate, other secure social network member.

[0037] FIG. 2 shows a controlled facility in accordance with one or more embodiments of the invention. As shown in

FIG. 2, the controlled facility (200) may include a visitor kiosk (202), a booking kiosk (204), an administrator computing device (206), an inmate kiosk (208), an inmate phone (210), an inmate computing device (212), and a local server (214). The inmate computing device (212) and the local server (214) are communicatively coupled to the communications network (216). The administrator computing device (206) includes an administrator application (218). The inmate computing device (212) includes an inmate application (220).

[0038] In one or more embodiments of the invention, the visitor kiosk (202) is a computing system with functionality to facilitate communication between an inmate and a visitor. Specifically, the visitor kiosk (202) may be a combination of computing hardware and software used by a visitor to make and receive voice and video calls to/from an inmate residing in the same controlled facility (200) or another controlled facility (not shown). The visitor kiosk (202) may also be used to schedule a voice or video call with an inmate for a future date. Further, the visitor kiosk (202) may also include the functionality to exchange media (e.g., photos, videos, and audio) with an inmate residing in the controlled facility (200). The visitor kiosk (202) may include functionality to generate such media, such as a camera, microphone, keyboard, and software to record or otherwise create media to send to an inmate. Such media may be subject to review before being delivered.

[0039] In one or more embodiments of the invention, a visitor wanting to use a visitor kiosk (202) may be required to participate in an authentication process to verify the identity of the visitor. The authentication process may include creating an identity data item and verified data for storage and later comparison. The verified data used for authentication may be a username and password combination and/or biometric information about the visitor.

[0040] In one or more embodiments of the invention, the visitor kiosk (202) includes functionality to access a secure social network. Specifically, the visitor kiosk (202) may be used by a visitor to create and manage a secure social network account. The visitor kiosk (202) may also be used by a visitor to upload digital media to the visitor's secure social network account or the account of another secure social network member. The visitor kiosk (202) may further be used to view digital media uploaded to the visitor's social network account or the account of another secure social network member.

[0041] In one or more embodiments of the invention, the visitor kiosk (202) includes functionality to manage a commissary account for one or more inmates. Specifically, a visitor may use a visitor kiosk (202) to add money to the commissary account of an inmate in the controlled facility (200), view a transaction history of the commissary account, transfer funds between commissary accounts, and/or remove funds from a commissary account. Further detail about the visitor kiosk (202) is provided in FIG. 5A and FIG. 5B.

[0042] In one or more embodiments of the invention, the booking kiosk (204) is a computing system with functionality to aid administrators in admitting an inmate into a controlled facility (e.g., controlled facility (200)). Specifically, the booking kiosk (204) may include functionality to create or update an inmate identity data item. Specifically, the booking kiosk (204) may be used to obtain verified data (e.g., passwords, biometric data, etc.) and save the verification data in one or more identity data items for the inmate. The verified data may then be used to authenticate the inmate (e.g., to access the communications network (216), etc.). In one or more embodi-

ments of the invention, the booking kiosk may also be used to associate one or more restrictions with the inmate via the inmate's identity data item.

[0043] In one or more embodiments of the invention, the booking kiosk (204) includes functionality to input contact information for visitors, outsiders, administrators, or other inmates with whom the inmate wants to communicate. Such contact information may then be associated with the inmate's identity data item, and may be used to initiate a voice or video call, or otherwise transmit media to visitors, outsiders, or other inmates. Further, in one or more embodiments of the invention, the contact information may be retrieved from an inmate's mobile computing device (e.g., cell phone, smart phone, etc.) or a local or remote data storage device (e.g., a flash drive, a webmail account, etc.). The contact information may be retrieved using a wired or wireless connection between the booking kiosk and the inmate's mobile computing device and/or the data storage device. The contact information may be subject to review before the inmate is permitted to contact the visitor, outsider, administrator, or other inmate.

[0044] In one or more embodiments of the invention, the booking kiosk (204) includes functionality to prepare a mobile computing device for use by the inmate within the controlled facility (200). Specifically, a controlled facility (200) may allow inmates the use of computing devices while in or subject to the controlled facility (200). However, use of such inmate computing devices may require that the computing device is instrumented with software restricting the use of the inmate computing device. The booking kiosk (204) may be used to instrument the inmate computing device as required. Further detail about the booking kiosk (204) is provided in FIG. 5A and FIG. 5B.

[0045] In one or more embodiments of the invention, the administrator computing device (206) is a computing system or group of computing systems with functionality to execute the administrator application (218). In one or more embodiments of the invention, the administrator application (218) is a process or group of process with functionality to provide access to communications between inmates at the controlled facility (200) and visitors, outsiders, administrators, and other inmates. The administrator application (218) may also be used to monitor current voice or video calls between an inmate and a visitor, outsider, administrator, or other inmate.

[0046] In one or more embodiments of the invention, the administrator application (218) is used to manage an identity data item associated with an inmate. Such management may include altering the restrictions (device use restrictions, inmate use restrictions, and inmate target restrictions) applicable to the inmate. In one or more embodiments of the invention, the administrator application (218) is used to access the secure social network account of an inmate, visitor, or outsider. In one or more embodiments of the invention, the administrator application (218) may provide heightened access (i.e., a level of access greater than that of the inmate, visitor, or outsider) to data stored in the secure social networking account.

[0047] In one or more embodiments of the invention, the inmate kiosk (208) is a computing system with functionality to facilitate communication between an inmate and a visitor or outsider. Specifically, the inmate kiosk (208) may be a combination of computing hardware and software used by an inmate to make and receive voice and video calls to/from a visitor, outsider, or another inmate residing in another con-

trolled facility (not shown). The inmate kiosk (208) may also be used to schedule a voice or video call with a visitor at a future date. Initiating or scheduling a voice or video call may include determining whether the currently attempted call or the scheduled call are adverse to one or more restrictions (e.g., inmate use restrictions, device use restrictions, and/or inmate target restrictions). Further, the inmate kiosk (208) may also include the functionality to exchange media (e.g., photos, videos, and audio) with a visitor or outsider. The inmate kiosk (208) may include functionality to generate such media, such as a camera, microphone, keyboard, and software to record or otherwise create media to send to a visitor or outsider. Such media may be subject to review before being delivered.

[0048] In one or more embodiments of the invention, an inmate wanting to use an inmate kiosk (208) may be required to participate in an authentication process to verify the identity of the inmate. The authentication process may include providing verification data for comparison to verified data previously obtained from the inmate and stored in the inmate identity data item. The verified data may be a username and password combination and/or biometric information about the inmate.

[0049] In one or more embodiments of the invention, the inmate kiosk (208) includes functionality to access a secure social network. Specifically, the inmate kiosk (208) may be used by an inmate to manage a secure social network account. The inmate kiosk (208) may include functionality to generate such media, such as a camera, microphone, keyboard, and software to record or otherwise create media to send to a visitor or outsider. The inmate kiosk (208) may also be used by an inmate to upload digital media to the inmate's secure social network account or the account of another secure social network member. The inmate kiosk (208) may further be used to view digital media uploaded to the inmate's social network account or the account of another secure social network member. Uploaded media may be subject to review before posting.

[0050] In one or more embodiments of the invention, the inmate kiosk (208) includes functionality to manage a commissary account for the inmate. Specifically, an inmate may use an inmate kiosk (208) to view a transaction history of the commissary account and/or to apply commissary funds for goods and services consumed or enjoyed by the inmate. Further detail about the inmate kiosk (208) is provided in FIG. 5A and FIG. 5B.

[0051] In one or more embodiments of the invention, the inmate phone (210) is a device with functionality to send and receive audio communications between an inmate and an outsider or visitor. The inmate phone (210) may be implemented as handset connected to a telephone line. In one or more embodiments of the invention, all or part of the voice call may be conducted over a VoIP connection. In one or more embodiments of the invention, a single inmate phone (210) is utilized by multiple inmates.

[0052] In one or more embodiments of the invention, initiating or receiving a voice call using the inmate phone (210) requires a form of authentication (e.g., providing a password, personal identification number, or voice verification). In one or more embodiments of the invention, voice calls made using the inmate phone (210) are monitored by one or more administrators using the administrator computing device (206), and are recorded and stored in a data storage system within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown). The inmate phone (210) may also be subject to device use restric-

tions limiting the ability to use the inmate phone (210) at certain times (e.g., between 9 PM and 8 AM) or under certain conditions (e.g., emergency lockdown).

[0053] In one or more embodiments of the invention, the identity of the visitor or outsider targeted by the inmate or attempting to contact the inmate using the inmate phone (210) is verified against inmate target restrictions imposed on the inmate. Such restrictions may be associated with the inmate's identity data item and may be stored locally within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown). The visitor or outsider identity may be verified by the local server (214) or by another server within the outside facility (not shown), or within a third party provider (not shown).

[0054] In one or more embodiments of the invention, the inmate computing device (212) is a computing system configured to execute the inmate application (202). In one or more embodiments of the invention, each inmate computing device (212) is utilized exclusively by a single inmate. In one or more embodiments of the invention, access to the inmate application requires a form of initial authentication. This initial authentication may use verification data stored locally on the inmate computing device (212) (e.g., a code or combination used to unlock the phone, locally stored biometric data, etc.).

[0055] In one or more embodiments of the invention, accessing a communications network (e.g., communications network (216)) using the inmate application (220) may require further network-based authentication. This further authentication may use verification data stored external to the inmate computing device (212) but locally within the controlled facility (200), or remotely within the outside facility (not shown) or within a third party provider (not shown).

[0056] In one or more embodiments of the invention, an authenticated inmate may use the inmate application to initiate or receive voice or video calls, initiate or receive text or media messages, schedule a voice or video call, manage a commissary account, or post media to a secure social network. In one or more embodiments of the invention, voice and video calls made using the inmate computing device (212) are monitored by one or more administrators using the administrator computing device (206), and are recorded and stored in a data storage system within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown).

[0057] In one or more embodiments of the invention, the identity of the visitor or outsider targeted by the inmate or attempting to contact the inmate using the inmate computing device (212) is verified against inmate target restrictions imposed on the inmate. Such restrictions may be associated with the inmate's identity data item and may be stored locally within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown). The visitor or outsider identity may be verified by the local server (214) or by another server within the outside facility (not shown), or within a third party provider (not shown).

[0058] In one or more embodiments of the invention, the inmate computing system (212) and/or the inmate application (220) may limit access to the communications network (216) based on one or more restrictions (inmate use restrictions, inmate target restrictions, and device use restrictions). Further, the inmate computing system (212) and/or the inmate application (220) may gather data from input devices of the inmate computing system (212) to determine whether one or

more restrictions apply. Such input devices may include, for example, a system clock, a global positioning system antenna, a wide area network antenna, etc.

[0059] In one or more embodiments of the invention, the local server (214) is a computer system or group of computers systems located within the controlled facility (200) that facilitate communication between inmates and visitors, outsiders, and/or other inmates. Specifically, the local server (214) may implement the software necessary to host voice and video calls between and among the visitor kiosk (202), the inmate kiosk (208), the inmate phone (210), and an outsider computing system (not shown). The local server (214) may also include functionality to enforce communication restrictions associated with the inmates using the inmate kiosk (208) or inmate phone (210). Alternatively, the local server (214) may merely provide access to other systems capable of hosting the communication software and data storage (e.g., located within an offsite facility or a third party provider). Further, in one or more embodiments of the invention, the local server (214) includes functionality to regulate inmate access to a secure social network.

[0060] FIG. 3 shows an outside facility in accordance with one or more embodiments of the invention. As shown in FIG. 3, the outside facility (300) may include an application server (302), a database server (304), a reviewer computing system (306), and an investigator computing system (308). The application server (302) is communicatively coupled to the communications network (310). The reviewer computing device (306) may include a reviewer application (312), and the investigator computing device (308) may include an investigator application (314).

[0061] In one or more embodiments of the invention, the application server (302) is a computing system or group of computing systems configured to authenticate inmates, visitors, outsiders, administrators, reviewers, and/or investigators. Specifically, the application server (302) includes functionality to receive a request to authenticate an inmate, visitor, outsider, administrator, reviewer, and/or an investigator, retrieve verified data associated with the request, and compare the verified data to verification data submitted in the authentication request. In one or more embodiments of the invention, the application server provides access to identity data items and other data stored in the database server (304).

[0062] In one or more embodiments of the invention, the database server (304) is a computing system or group of computing systems configured to store data about inmates, visitors, outsiders, administrators, reviewers, and/or investigators as well as communication data describing communications between and among inmates, visitors, outsiders, administrators, reviewers, and/or investigators. Data stored in the database server may include, but is not limited to, identity data items, verified data, approved communication media, communication media pending review

[0063] In one or more embodiments of the invention, the reviewer computing device (306) is a computing system configured to execute the reviewer application (312). In one or more embodiments of the invention, a reviewer is a person charged with viewing a media item submitted by an inmate, visitor, outsider or administrator, and determining one or more attributes of the media item. Based on the determined attributes of the media item, the reviewer may then approve the media item for transmission to its target inmate, visitor, or outsider. Alternatively, the reviewer may reject the media item, conditionally approve the media item, or redact parts of

the media item, thus preventing complete transmission to its target inmate, visitor, or outsider. In one or more embodiments of the invention, the reviewer application (312) includes functionality to view media items, associate one or more attributes to the media item, and/or mark the media items as approved or rejected.

[0064] In one or more embodiments of the invention, the investigator computing device (308) is a computing system configured to execute the investigator application (314). In one or more embodiments of the invention, an investigator is a person gathering information about an inmate, visitor, or outsider generally for the purposes of law enforcement. The investigator application (314) includes functionality to provide access to data stored on the database server (304) for investigative purposes.

[0065] FIG. 4 shows a general computing system in accordance with one or more embodiments of the invention. As shown in FIG. 4, the computing system (400) may include one or more computer processor(s) (402), associated memory (404) (e.g., random access memory (RAM), cache memory, flash memory, etc.), one or more storage device(s) (406) (e.g., a hard disk, an optical drive such as a compact disk (CD) drive or digital versatile disk (DVD) drive, a flash memory stick, etc.), and numerous other elements and functionalities. The computer processor(s) (402) may be an integrated circuit for processing instructions. For example, the computer processor(s) may be one or more cores, or micro-cores of a processor. The computing system (400) may also include one or more input device(s) (410), such as a touchscreen, keyboard, mouse, microphone, touchpad, electronic pen, camera, or any other type of input device. Further, the computing system (400) may include one or more output device(s) (408), such as a screen (e.g., a liquid crystal display (LCD), a plasma display, touchscreen, cathode ray tube (CRT) monitor, projector, or other display device), a printer, external storage, or any other output device. One or more of the output device(s) may be the same or different from the input device(s). The computing system (400) may be connected to a network (414) (e.g., a local area network (LAN), a wide area network (WAN) such as the Internet, mobile network, or any other type of network) via a network interface connection (not shown). The input and output device(s) may be locally or remotely (e.g., via the network (412)) connected to the computer processor(s) (402), memory (404), and storage device(s) (406). Many different types of computing systems exist, and the aforementioned input and output device(s) may take other forms.

[0066] Software instructions in the form of computer readable program code to perform embodiments of the invention may be stored, in whole or in part, temporarily or permanently, on a non-transitory computer readable medium such as a CD, DVD, storage device, a diskette, a tape, flash memory, physical memory, or any other computer readable storage medium. Specifically, the software instructions may correspond to computer readable program code that when executed by a processor(s), is configured to perform embodiments of the invention.

[0067] Further, one or more elements of the aforementioned computing system (400) may be located at a remote location and connected to the other elements over a network (414). Further, embodiments of the invention may be implemented on a distributed system having a plurality of nodes, where each portion of the invention may be located on a different node within the distributed system. In one or more

embodiments of the invention, the node corresponds to a distinct computing device. Alternatively, the node may correspond to a computer processor with associated physical memory. The node may alternatively correspond to a computer processor or micro-core of a computer processor with shared memory and/or resources.

[0068] FIG. 5A shows a video visitation kiosk in accordance with one or more embodiments of the invention. Specifically, the video visitation kiosk (500) is a type of computing device as described in FIG. 4. As shown in FIG. 5A, the video visitation kiosk (500) includes a camera (502), a display (504), a handset (506), a headset jack (508), and a universal serial bus (USB) port (510).

[0069] FIG. 5B shows the hardware and software elements of a video visitation kiosk in accordance with one or more embodiments of the invention. The hardware and software elements shown in FIG. 5B may be in addition to the elements described in FIG. 4. As shown in FIG. 5B, the video visitation kiosk (500) includes a handset (506), a video camera (502), a touch screen panel (512), a display (504), a computing application (514), an operating system (516), and a network interface controller (518).

[0070] FIG. 6 shows the hardware and software elements of a mobile computing device in accordance with one or more embodiments of the invention. Specifically, the mobile computing device (600) is a type of computing device as described in FIG. 4. The hardware and software elements shown in FIG. 6 may be in addition to the elements described in FIG. 4.

[0071] As shown in FIG. 6, the mobile computing device (600) may include a global positioning system (GPS) antenna (602), a cell antenna (604), a wide area network (WAN) antenna (606), and a personal area network (PAN) antenna (608), each connected to a multi-band radio transceiver (610). The mobile computing device (600) also may include a rear-facing video camera (612), a front-facing video camera (614), a compass (616), an accelerometer (618), a touch screen (620), a display (622), and a microphone (624). The mobile computing device (600) also may include a computing application (626) executing on an operating system (628).

[0072] FIG. 7 shows a schematic diagram of a system including a network application (700) and a database server (702). The network application (700) may execute or be a part of application server (118) in FIG. 1. Similarly, the database server may be database server (120) in FIG. 1. Alternative configurations may also be used. For example, either, both, or part of the network application (700) and database server (702) may be located in the controlled facility. The network application (700) and database server (702) are discussed below.

[0073] A network application (700) is a software application for connecting inmates and administrators to a network. For example, the network may be a telephone network (not shown) or a secure social network (not shown). The network application may include an authentication module (704), a controlled setup module (706), a text and speech converter (708), an audit module (710), and a communication module (712). Each of these components is discussed below.

[0074] An authentication module (704) includes functionality to authenticate individuals to the desired network. For example, the authentication module may include functionality to receive authentication credentials, and determine whether the authentication credentials match stored credentials for the individual. The authentication credentials may be user name, password, voiceprint authentication, face verifi-

cation information, identifying body marks and features information, retina verification information, palm or fingerprint verification information, or any other type of credential for authentication.

[0075] In one or more embodiments of the invention, the controlled setup module (706) includes functionality to create an account (e.g., inmate account (718), superfriend account (714)) for an individual. The controlled setup module (706) may further include functionality to populate the account with contacts, and update the account. Populating an inmate account (718) with contacts and updating the inmate account (718) are discussed with reference to FIGS. 8-10.

[0076] Continuing with FIG. 7, in one or more embodiments of the invention, the text and speech converter (708) includes functionality to convert textual input into audio output. The text and speech converter (708) may further include functionality to convert audio input to textual output. Further, the text and speech converter (708) may further include functionality to convert one audio input into a second audio input. For example, consider the scenario in which an administrator would like to transmit an anonymous message, such as deliver bad news. In such a scenario, the text and speech converter (708) may include functionality to replace an administrator's voice with a computerized audio. For example, the computerized audio may be a computer voice speaking the administrator's spoken words or manipulation of the sounds of the administrator's voice.

[0077] In one or more embodiments of the invention, the audit module (710) includes functionality to track communications from inmates. Specifically, the audit module (710) includes functionality to track, calculate, and store messages, timestamps defining when the message was transmitted, when the message was received, the length of time in which the message was being presented, a unique identifier of the communication device (e.g., inmate kiosk, inmate phone, inmate computing device) used to receive the message, any response to the message, and other tracking information about a message.

[0078] In one or more embodiments of the invention, the communication module (706) includes functionality to manage a communication on a network. For example, the communication module (706) may include functionality to identify an individual accessing the network, receive a connection request to connect to a contact, and connect the individual to the contact when the contact is in the individual's network list. The term, list, as used in this application refers to any data structure for storing a collection of contacts. The communication module (706) may further include functionality to connect the individual to all social network contacts via the secure social network. In one or more embodiments of the invention, the communication module (706) may facilitate oversight of an inmate's communication by transmitting all or a portion of the messages to an administrator or reviewer for approval.

[0079] The communication module (706) may further include functionality to track the length of time that an inmate is communicating on the selected network and/or a number of messages sent and/or received on the selected network. A payment module (not shown) may include functionality to obtain payment from the inmate or a contact of the inmate and disperse the payment. For example, dispersing the payment may include transmitting at least a portion of the payment to a controlled facility and/or transmitting a portion to a network management entity (e.g., telephone connection company,

internet connection company) and/or retaining at least a portion. The payment module may include functionality to debit an inmate's money account or otherwise bill the inmate based on the amount of time, number of messages, or other information.

[0080] Continuing with FIG. 7, the network application (700) is operatively connected to the database server (702). The database server (702) includes functionality to store information for the network application (700). For example, the database server (702) may store one or more superfriend accounts (714), an inmate account (718) for each inmate, audit data (734), saved messages (736), and groups (738). Each of the stored data is discussed below.

[0081] A superfriend account (714) is an account maintained for an administrator who is a superfriend of an inmate. A superfriend is a person, typically an administrator, contacts and communications from whom an inmate is not permitted to block, reject, or unfriend in accordance with one or more embodiments of the invention. For example, the superfriend may be a warden, guard, parole officer, counselor, doctor, investigator, or other individual. In one or more embodiments of the invention, a superfriend has superfriend privileges (722) over an inmate account (718) and has removal protection from the inmate account (718). In one or more embodiments of the invention, superfriend privileges may correspond to administrative privileges. Superfriend privileges (722) include being able to transmit any information to an inmate and having the transmission on the conspicuously placed or presented when the inmate accesses the network. Further, superfriend privileges (722) may include privilege to review all correspondence to and from the inmate. Additional superfriend privileges may exist without departing from the scope of the invention. In one or more embodiments of the invention, an inmate cannot limit the superfriend privileges.

[0082] Removal protection refers to an inability for an inmate to unfriend the superfriend. Specifically, without proper authority, which an inmate does not have, the superfriend cannot be disassociated from the inmate's network.

[0083] In one or more embodiments of the invention, the superfriend account (714) further includes a superfriend network list (720), superfriend authentication credentials (724), and at least one superfriend public alias. The superfriend network list (720) includes a list of contacts with whom the superfriend may communicate. A contact refers to an individual or group of individuals with whom a person is connected. For example, the contact may include a network identifier of an individual and connection information for connecting to the individual.

[0084] Superfriend authentication credentials (724) are authentication credentials used for authenticating the administrator. The superfriend authentication credentials (724) may include user name, password, voiceprint authentication, face verification information, identifying body marks and features information, retina verification information, palm or fingerprint verification information, or any other type of credential for authentication.

[0085] In one or more embodiments of the invention, a superfriend public alias (726) is an alternative identifier for the administrator that is presented as the sender and/or recipient of messages. For example, if the administrator is transmitting a message anonymously, the anonymous communication may be under the public alias. By way of another example, if the administrator is performing a communication

for a particular group (e.g., the entire controlled facility, a group of prisons, a counseling group), the administrator may use the public alias of a group name to send and receive messages.

[0086] Continuing with the database server (702), an inmate account is an account storing information about an inmate. For example, an inmate account may include inmate authentication credentials (728), an inmate telephone network list (730), and an inmate social network list (732). Additionally, although not shown in FIG. 7, the inmate account may also include administrative information, such as name, birthdate, inmate identifier, reason for the inmate to be in the controlled facility, historical confinement of the inmate, list of inmate's violations of regulations of the controlled facility, gang affiliations, account balance for payment of communications, and other information.

[0087] The inmate authentication credentials (728) correspond to authentication credentials for the inmate. For example, the authentication credentials may include user name, password, voiceprint authentication, face verification information, identifying body marks and features information, retina verification information, palm or fingerprint verification information, or any other type of credential for authentication.

[0088] The inmate telephone network list (730) corresponds to a list of contacts of the inmate for communication via the telephone network. The inmate secure social network list (732) corresponds to a list of contacts of the inmate for communication via a secure social network. In one or more embodiments of the invention, before being allowed to communicate with the contacts, the contacts must be approved. Further, although an inmate may communicate with contacts in the inmate telephone network list and the inmate secure social network list, the contacts may not be approved in accordance with one or more embodiments of the invention. Specifically, the inmate telephone network list and the inmate secure social network list may include unprocessed contacts, filtered contacts, and/or approved contacts.

[0089] An unprocessed contact is a contact that has not been vetted or checked to determine whether communication with the unprocessed contact is prohibited. A filtered contact is a contact that is not outright prohibited for communication. An approved contact is a contact that has been vetted and with whom the inmate may communicate. For example, unprocessed contacts may be filtered to remove contacts that are known gang members, are inmates, are wanted criminals, or have other attributes, which make communication with such contacts outright prohibited. In one or more embodiments of the invention, the filtering process may include comparing the contact with lists of prohibited people. In some embodiments, the remaining contacts after the filtering process are approved contacts. In alternative embodiments, filtered contacts may have to be vetted (e.g., go through an identification and/or approval process) to be approved contacts. The vetting may include performing background checks on the contact and confirming the identity of the contact. In one or more embodiments of the invention, rules of the controlled facility define whether filtered contacts must be vetted in order for the inmate to communicate with the approved contacts. Whether a contact is an unprocessed contact, filtered contact, or approved contact may be maintained as an attribute defined for the contact in the inmate account.

[0090] Although FIG. 7 shows the secure social network list (732) as separate and distinct from the telephone network

list (730), the secure social network list (732) may be the same as the telephone network list (730). Further, in one or more embodiments of the invention, the inmate may have a single contact list. Each contact in the single contact list may have a parameter indicating whether the inmate may communicate with the contact via telephone network, secure social network, or both. For example, the parameter may be a set bit and/or connection identifiers (e.g., telephone number, secure social network identifier) for the contact.

[0091] Continuing with the discussion regarding the database server (702), the audit data (734) includes information stored for auditing purposes. For example, for each message, the audit data may include timestamps defining when the message was transmitted, when the message was received, the length of time in which the message was being presented, a unique identifier of the communication device used to receive the message, any response to the message, and other tracking information about a message.

[0092] Saved messages (736) correspond to messages that are saved. For example, saved messages may include postings to the inmate secure social network, voicemail messages, one to one messages, multicast or broadcast messages, and other messages.

[0093] In one or more embodiments of the invention, groups relate a group identifier to account identifiers of individuals who are members of the group. For example, for a counseling group, the counseling group identifier is related to the counselor superfriend account identifier along with inmates who participate in the counseling session. By way of another example, for a controlled facility group, the controlled facility group identifier may be related to all inmates in the controlled facility. Thus, a communication sent to a group identifier will be broadcasted to all members of the group in one or more embodiments of the invention.

[0094] Although FIG. 7 shows a certain configuration of components, other configurations may be used without departing from the scope of the invention. For example, the superfriend account (714) may be located on an application. By way of another example, one or more modules of the network application (700) may be located in a different component of the system.

[0095] FIGS. 8-10 show flowcharts in one or more embodiments of the invention. While the various steps in these flowcharts are presented and described sequentially, some or all of the steps may be executed in different orders, may be combined or omitted, and some or all of the steps may be executed in parallel. Furthermore, the steps may be performed actively or passively. For example, some steps may be performed using polling or be interrupt driven in accordance with one or more embodiments of the invention. By way of an example, determination steps may not require a processor to process an instruction unless an interrupt is received to signify that condition exists in accordance with one or more embodiments of the invention. As another example, determination steps may be performed by performing a test, such as checking a data value to test whether the value is consistent with the tested condition in accordance with one or more embodiments of the invention.

[0096] FIG. 8 shows a flowchart for priming a network of an inmate in one or more embodiments of the invention. In Step 801, the mobile device of the inmate is confiscated in one or more embodiments of the invention. In one or more embodiments, when an inmate is confined, the inmate may be stripped of the inmate's possessions. For example, all com-

munication devices found on the inmate or in the inmate's belongings may be removed. The removal may be temporary, such as during a booking process, or semi-permanent, such as during the entire period of an inmate's confinement.

[0097] In Step 803, inmate authentication credentials for social networks are received in one or more embodiments of the invention. In one or more embodiments of the invention, the inmate provides his or her authentication credentials. Rather than providing authentication credentials to third party social network, the inmate may provide the credentials to an administrator. In other words, in one or more embodiments of the invention, the inmate is not allowed to access the inmate's third party social network once confinement of the inmate is initiated. Providing authentication credentials may be optional for the inmate. Specifically, the inmate may opt out of importing contacts from third party social networks. In such a scenario, the steps discussed below regarding importing contacts from the social network may be omitted.

[0098] In Step 805, contacts are imported from the inmate's mobile device and social networks in one or more embodiments of the invention. Specifically, third party social networks are accessed using the inmate's authentication credentials provided in Step 803. The contacts are extracted from the inmate's account on the third party's social network. Alternatively, contacts from the inmate's third party social network may be imported without input from the inmate. For example, a court order to the third party may require the third party to release a list of contacts of the inmate on the third party social network or the court order may require release of the authentication credentials to allow for automatic crawling and download.

[0099] Further, in one or more embodiments of the invention, contacts are downloaded from the inmate's mobile device. Importing contacts may be performed using extraction software. If the inmate has a passcode, the passcode may be overridden in order to extract the contacts.

[0100] In Step 807, the contacts are reviewed for persons of interest in one or more embodiments of the invention. For example, contacts may be reviewed to identify missing witnesses, individuals with warrants out for arrest, and other individuals. Reviewing contacts may be performed by a reviewer application comparing the contacts with one or more person of interest list. For example, the reviewer application may compare contacts against state and federal warrant lists to determine whether a contact has a warrant out for his or her arrest. By way of another example, the reviewer application may compare the contacts with a list of individuals connected to an inmate's confinement and flag the contacts that match. The reviewer application may transmit any matching contacts to a reviewer. For example, the reviewer may be an administrator. By way of an example, the reviewer may be an investigator that is managing the inmate's case.

[0101] In Step 809, contacts are filtered for prohibited contacts to obtain approved contacts in one or more embodiments of the invention. In one or more embodiments of the invention, filtering contacts includes determining which contacts with whom the inmate is outright not allowed to communicate with and saving the remainder of the contacts as filtered contacts. Depending on the rules of the controlled facility, vetting of the filtered contacts may be performed to obtain approved contacts. The vetting may be performed at this stage, when the inmate requests communication with the contact, or at another time. Alternatively, once the contacts are filtered, the remaining contacts may be deemed approved.

For example, the contacts may be filtered to remove other inmates, known gang members, and witnesses. The contacts may further be filtered to remove individuals confined in the same and/or different controlled facility. Filtering the contacts may include the setup module comparing the contacts with one or more lists of prohibited contacts. Such lists may include a list of known gang members, a list of jury members, a list of judges, a list of witnesses, and any other lists. After the contacts are filtered, the remaining contacts may be transmitted to a reviewer application for a reviewer to view the contacts. The reviewer may determine whether any of the remaining contacts are prohibited and remove any prohibited contacts. The resulting contacts from the filtering may be referred to as approved contacts. Alternatively, the resulting contacts may be subject to more vetting to be approved contacts.

[0102] In Step **811**, social network identifiers for each contact are obtained to update the contacts in one or more embodiments of the invention. Specifically, in one or more embodiments of the invention, one or more contacts that are obtained from an inmate's mobile device may not be associated with a third party social network in the inmate's mobile device. In such a scenario, the third party social networks are accessed with contact information, such as the name of the contact, to obtain the contact's social network identifier. Thus, not only is the inmate able to communicate with the contact via a telephone network, but also with the contact via the secure social network even when the inmate does not have a network identifier for the contact. If the contact is found in the third party social network, an updated contact is created.

[0103] In Step **813**, the updated contact is saved in the approved contact list for each updated contact in one or more embodiments of the invention. Specifically, the update to the contact is saved.

[0104] In Step **815**, the inmate is presented with a contact list in one or more embodiments of the invention. Presenting the inmate with the contact list may be performed during a booking process or afterwards, such as once the inmate is confined. For example, the inmate may be presented with telephone network contacts via the inmate phone or kiosk described above. In the example, the first time that the inmate uses the inmate phone or kiosk, the inmate may be presented with options for setting up an inmate account to access the social network. The inmate may be presented with a list of all contacts, unprocessed contacts, filtered contacts, or a combination thereof. In one or more embodiments of the invention, the filtering and vetting process may be performed before or after the inmate requests communication with the contact.

[0105] In Step **817**, a selection of contacts from the contact list is received from the inmate to obtain selected contacts in accordance with one or more embodiments of the invention. In one or more embodiments, the inmate selects the contacts with which the inmate would like to communicate while confined. By allowing the inmate to select contacts, the inmate can determine the contacts with which the inmate would like to communicate while confined. Further, embodiments prevent the inmate from accessing unapproved contacts.

[0106] In Step **819**, the inmate telephone list and the inmate secure social network list are populated with the selected contacts in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, once populated, the inmate is enabled to communicate with any contact in the inmate telephone list and the inmate secure

social network list. In one or more embodiments of the invention, the inmate may request communications with any contacts. The requested communication may require an approval process.

[0107] In Step **821**, an administrator is added as a super-friend of the inmate in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, the administrator is selected based on a relationship (or lack thereof) with the inmate. For example, the administrator may be a warden, an investigator, a guard, or another individual. By adding the administrator as super-friend, the administrator may review all messages from and to the inmate. Thus, the administrator may ensure that the messages comply with regulations. For example, the administrator may ensure that the inmate is not receiving crime reports, participating in a crime, communicating with gang members, plotting to receive or send contraband, or performing any other such acts. By way of another example, the administrator may gather evidence and other intelligence from messages to and from the inmate.

[0108] In one or more embodiments of the invention, when the inmate wants to use the telephone network, the inmate may access the inmate phone or kiosk. Using the inmate phone or kiosk, the inmate may authenticate him or herself to the telephone network. The inmate may be presented with the inmate's telephone network list. Alternatively, the inmate may select a speed dial number or graphical image for a particular contact in the inmate's telephone contact list. If the contact is in the inmate telephone network, the inmate is connected to the contact. The communication module and audit module may begin recording information, such as a contact identifier of the contact, a time and date of the communication, length of time for the communication, and a recording of the communication.

[0109] To access the inmate secure social network, the inmate may authenticate him or herself to the secure social network. The inmate may begin sending and/or receiving messages with the secure social network. The messages may be broadcasted to all of the inmate secure social network contacts, multi-casted to a subset of the inmate secure social network contacts, or uni-casted to a single secure social network contact. Each message or a subset thereof may be reviewed by the administrator before or after being transmitted.

[0110] In one or more embodiments of the invention, the inmate voluntarily or involuntarily provides, to the network application, his or her authentication credentials to an application providing an outside social network. The network application executing the secure social network may use the authentication credentials to connect to the outside social network. The network application may communicate with the outside social network using an Application Programming Interface (API) of the outside social network. Social data transmitted from the outside social network to the network application may be buffered and analyzed prior to being presented to the inmate in accordance with one or more embodiments of the invention.

[0111] For instance, the inmate might request access to specific photo libraries (by name) or all photo libraries and other content. The network application processes the request by downloading the requested content and storing the content in a review queue that is tagged and filtered by automated systems and/or by human reviewers. The resulting content that is tagged and filtered is provided to the inmate. Thus, the

inmate will eventually obtain access to none, some, or all of the requested content depending on the outcome of the review queue.

[0112] In one or more embodiments of the invention, the network application imports photos from the outside social network, regardless of whether the inmate is allowed to view them, may analyze the photos with facial and object recognition software. The network application may search for biometric matches between the faces in the imported photos and biometric data already known by the system. For example, the biometric data may be from individuals appearing in video visitations or otherwise recognized from other imported photos. In some cases, facial recognition is not used, such as in the case where the imported photos have already been tagged in the outside social network with identities. The network application may compare the identities from the photos with individuals known by the system. For example, individuals known to the system may include current and former inmates, and current and former contacts of the inmates made through telephone calls, video visitations, secure social networking, and other communications channels whose records are available to the system.

[0113] In one or more embodiments of the invention, social network contacts may be obtained as follows. The inmate may be presented with all contacts, but only a subset of the data, such as name, residence location, and profile photo. Some data, such as address, telephone number, email address, or social network identifier may be redacted. Based on the subset of data, the inmate then select which contacts that the inmate would like to communicate with from within the controlled facility. The selected contacts, along with the information withheld from the inmate, may be placed in a review queue analogous to the image review queue. In one or more embodiments of the invention, social network contacts associated with the inmate are then available to the system. By being available, the investigators, administrators, and software routines in the system may compare the imported contacts to lists of individuals with whom the inmate is prohibited from communicating. In one or more embodiments of the invention, any contacts matching, or appearing to match, the inmate's prohibited contact list are flagged for review. The investigator or administrator may make a determination of whether to allow or disallow communications with each requested contact.

[0114] One or more embodiments may perform social network crawling using the inmate's contacts. For example, the social network crawling may be performed to look for connections with other inmate users of the network application, connections with gang members or criminals, connections with controlled facility administrators, investigators, or other law enforcement officials, connections with people communicating with other inmates, and other connections. The connections may be direct or indirect connections (e.g., through a third party). Further, the number of connections between the inmate and the individual may correspond to the degree of the connection, which may be stored with the information. For example, the inmate may have a second degree connection with an investigator, where the second degree connection is through a family member of the inmate and a friend of the investigator.

[0115] In one or more embodiments of the invention, when the inmate connects to an outside social network through the network application, the inmate may be guided through an enrollment process. During the enrollment process, the

inmate may provide a new username if the inmate does not already have one to the outside social network. The network application may create a new account for the inmate on the outside social network.

[0116] In one or more embodiments of the invention, the network application may search databases and search engines using data provided by the inmate during enrolment. For example, if the inmate specifies his or her own account name, the system uses a search engine to determine whether the inmate specified username is used elsewhere. If other accounts with the same username are publicly accessible, or are accessible to other users of the same system, the system may log into these systems with an account of its own, perhaps as an automated proxy for a specific investigator at the facility, so as to access any data available. The available data, or in some cases, the account name alone, may be enough for investigators with sufficient cause to obtain a court order or subpoena to access additional information about these accounts and each account's list of connections. Thus, if an inmate specifies a username that the inmate has used in other online activities, investigators may obtain information about the other online activities.

[0117] One or more search engines may perform searching based on individuals and/or content matching information describing, or obtained from the inmate during his booking and/or enrollment. For example, if the inmate states his name as John Smith, age 51, residing in Long Beach, Calif., and among the first telephone calls he makes is to a number associated with a Susan Smith, age 49, also residing in Long Beach, Calif., the system may conclude that the two individuals are related, and perform additional searches based on this perceived first-degree connection. The search may be performed using a graph search or other search methods. Also, using only the inmate's claimed name, residence, and age, the system may perform a lookup using search engines such as MyLife.com, PeekYou.com, Pipl.com, ZoomInfo.com, and/or Spokeo.com, which all offer the ability to search for individuals based on scant submitted information.

[0118] Also, using any online account names associated with the inmate, that the inmate either provided or were derived from the above searches, additional online sites are searched for users with any of those same usernames, such as online dating sites. Additionally, the most commonly used dating sites are searched for profiles with attributes matching those attributes obtained from the system and that describe the inmate, including height, weight, age, hair color, eye color, and distinguishing features such as tattoos. The searches may be conducted not only for the specific values obtained or given, but for ranges above and below these values, to account for lies that dating site users may make.

[0119] FIG. 9 shows a flowchart for updating the inmate's network in one or more embodiments of the invention. Specifically, FIG. 9 shows a flowchart for when an inmate wants to add a contact. In Step 901, a request for connection to a new contact is received from the inmate in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, the inmate may provide contact information, such as name, connection identifier (e.g., telephone number, third party social network identifier), and other information for the new contact.

[0120] In Step 903, a determination is made whether the new contact is a prohibited contact. Determining whether the contact is a prohibited contact may be performed similar to the discussion above with respect to filtering contacts in Step

809 of FIG. 8. Additionally, determining whether the new contact is a prohibited contact may include confirming that the name of the contact matches the connection identifier. Specifically, confirming that the name matches the connection identifier ensures that the inmate is not attempting to access an unauthorized individual.

[0121] If the new contact is a prohibited contact, the new contact is flagged for review in Step 905 in one or more embodiments of the invention. Flagging the new contact for review may include sending a notification to the administrator. The notification may include contact information provided by the contact and the reason for flagging the contact (e.g., the basis for the contact being a prohibited contact). For example, a notification may be added to the superfriend account of the administrator. The administrator may be presented with the notification when the administrator logs into the administrator account or the administrator may receive an automated electronic communication, such as a text message. Alternatively, a non-superfriend, such as a reviewer may be notified of the new contact.

[0122] In Step 907, a determination is made whether an administrator approved the contact in one or more embodiments of the invention. Specifically, the administrator may select to override the prohibition of the contact. In such a scenario, the administrator may select that the contact is approved in the network application. If the administrator approves of the contact or if the new contact is not a prohibited contact, then the new contact is added to the inmate network in Step 909 in one or more embodiments of the invention. Once added, the inmate may begin communicating with the new contact.

[0123] FIG. 10 shows a flowchart for managing a release of the inmate in one or more embodiments of the invention. Specifically, in one or more embodiments, the release of an inmate may limit who the inmate may contact. For example, released inmates may be prohibited from contacting currently confined inmates. In Step 1001, input of an inmate being released is received in one or more embodiments of the invention. In one or more embodiments of the invention, the system may receive a notification that the particular inmate is being released.

[0124] In Step 1003, contact from the inmate contact list is obtained in one or more embodiments of the invention. In Step 1005, a determination is made whether the contact is confined in a controlled facility of some type in accordance with one or more embodiments of the invention. Specifically, if the contact is confined, then one or more regulations for communicating with the contact may apply. For example, the contact may be prohibited from communicating with the inmate and/or the inmate may be prohibited from communicating with the contact, such as by a condition of the inmate's release or other restriction set by the court.

[0125] In Step 1007, a determination is made whether communication with the inmate post-confinement is prohibited in accordance with one or more embodiments of the invention. To make the determination, the application rules defined by regulations defining with whom the inmate can communicate while released are executed. Released inmates may no longer be subject to the controlled facility. If communication with the contact by the inmate post-confinement is prohibited, then the connection between the inmate and the contact is removed in Step 1009 in accordance with one or more embodiments of the invention. Specifically, the contact is removed (e.g., deleted, blocked, hidden, etc.) from the inmate telephone

network list and secure social network list. Similarly, the inmate may be removed from the contact's telephone network list and secure social network list in accordance with one or more embodiments of the invention.

[0126] In Step 1011, a determination is made whether another unprocessed contact exists in one or more embodiments of the invention. Specifically, in one or more embodiments, each contact in the inmate network list is reviewed to determine whether the inmate may communicate with the contact post-confinement. Further, for any network list in which the inmate is a contact, the communication is analyzed to determine whether the communication with the inmate is prohibited. If prohibited, the inmate is deleted from the network list in accordance with one or more embodiments of the invention.

[0127] The following example is for explanatory purposes only and not intended to limit the scope of the invention. In the following example, consider the scenario in which Jeff, recently laid-off, unwisely decides to join Ruff Gang and illegally sell cocaine to obtain money. Because Jeff has had his cell phone on him at all times, he never bothers to remember how to connect to his contacts. One day, Jeff's life of crime caught up to him, and he is arrested and booked into a controlled facility. At the jail, Jeff's cell phone is confiscated from him as part of the booking process. Jeff has absolutely no idea whom he may contact.

[0128] Continuing with the example, Jeff is in luck. The controlled facility where he is booked has a network application that is able to obtain contacts from Jeff's cell phone. As part of the process, each contact in Jeff's cell phone is analyzed to determine whether Jeff is allowed to communicate with said contact. In other words, the contacts are filtered to remove prohibited contacts. Thus, contacts that are known members of Ruff Gang are removed. Further, known cocaine users who are contacts, and, therefore, may be witnesses to Jeff's illegal activities are removed. The remaining contacts include Jeff's family members, his attorney, and a few upstanding friends. Jeff decides that he does not want some of the contacts to know that he is incarcerated. So, Jeff selects a certain set of contacts to be in his network list and leaves the remaining contacts unselected. The warden and assistant warden may add themselves as superfriend of Jeff to review his communications.

[0129] Thus, although Jeff did not remember any of his contacts when he was booked into the controlled facility, he is still able to communicate with his contacts. Further, in accordance with certain embodiments of the invention, the contacts he has in his network list are confirmed to be those individuals with whom he may communicate without violating regulations or restrictions. Additionally, one or more embodiments allow for oversight of Jeff's messages to ensure that the messages do not violate regulations going forward.

[0130] While the invention has been described with respect to a limited number of embodiments, those skilled in the art, having benefit of this disclosure, will appreciate that other embodiments can be devised which do not depart from the scope of the invention as disclosed herein. Accordingly, the scope of the invention should be limited only by the attached claims.

What is claimed is:

1. A method for network priming for an inmate of a controlled facility, comprising:
 - receiving authentication credentials for the inmate to access a third party social network;

importing a plurality of social network contacts from the third party social network;
 filtering the plurality of social network contacts for prohibited contacts;
 presenting the inmate with the plurality of social network contacts;
 receiving, from the inmate, a selection of social network contacts from the plurality of social network contacts to obtain a plurality of selected social network contacts; and
 populating a secure social network list of the inmate with the plurality of selected social network contacts.

2. The method of claim **1**, further comprising:

importing a plurality of mobile device contacts from a mobile device used by the inmate;
 filtering the plurality of mobile device contacts for prohibited contacts;
 presenting the inmate with the plurality of mobile device contacts;
 receiving, from the inmate, a selection of mobile device contacts from the plurality of mobile device to obtain a plurality of selected telephone contacts; and
 populating a telephone list of the inmate with the plurality of selected telephone contacts.

3. The method of claim **2**, further comprising:

obtaining a social network identifier for at least one contact in the plurality of telephone contacts; and
 populating the plurality of social network contacts with the social network identifier for the at least one contact.

4. The method of claim **2**, further comprising:

reviewing the plurality of mobile device contacts for persons-of-interest; and
 notifying an administrator when a person-of-interest is found in the plurality of mobile device contacts.

5. The method of claim **2**, further comprising:

authenticating the inmate for telephone communication;
 receiving, in response to authenticating the inmate, a connection request to communicate with a telephone contact; and

connecting, via a telephone network, the inmate to the telephone contact when the telephone contact is in the telephone list of the inmate.

6. The method of claim **1**, further comprising:

adding an administrator to the secure social network list of the inmate; and
 providing the administrator with an administrative privilege and a removal protection from the secure social network list.

7. The method of claim **1**, further comprising:

receiving a request from an inmate for a connection to a new contact;

flagging, based on a determination that the new contact is a prohibited contact, the new contact to obtain a flagged contact; and

presenting the flagged contact to an administrator for approval.

8. The method of claim **1**, further comprising:

receiving a notification of a release of the inmate; and
 for each contact in the secure social network list of the inmate:

removing, based on the release, a connection between the inmate and the contact when communication with the contact post confinement is prohibited.

9. The method of claim **8**, wherein removing the connection comprising:

removing the contact from the secure social network contact list of the inmate; and

removing the inmate from a secure social network contact list of the contact.

10. The method of claim **1**, further comprising:

authenticating the inmate for secure social network communication; and

connecting, via a secure social network, the inmate to the secure social network list when the inmate is authenticated.

11. The method of claim **1**, further comprising:

obtaining outside social network authentication credentials for the inmate;

downloading, from an outside social network, content of the inmate using the outside social network authentication credentials;

analyzing the content to identify a plurality of individuals referenced in the content;

investigating the inmate using the plurality of individuals identified from the content;

filtering the content; and

presenting the filtered content to the inmate.

12. The method of claim **11**, further comprising performing social network crawling to identify a plurality of individuals indirectly connected to the inmate.

13. A system for network priming for an inmate of a controlled facility, comprising:

a computer processor;

a database server comprising an inmate account, wherein the inmate account comprises a secure social network list;

a network application executing on the computer processor and comprising:

a controlled setup module configured to:

receive authentication credentials for the inmate to access a third party social network;

import a plurality of social network contacts from the third party social network;

filter the plurality of social network contacts for prohibited contacts;

present the inmate with the plurality of social network contacts;

receive, from the inmate, a selection of social network contacts from the plurality of social network contacts to obtain a plurality of selected social network contacts; and

populate a secure social network list in the inmate account with the plurality of selected social network contacts.

14. The system of claim **13**, wherein the inmate account further comprises a telephone network list, and wherein the controlled setup module is further configured to:

import a plurality of mobile device contacts from a mobile device used by the inmate;

filter the plurality of mobile device contacts for prohibited contacts;

present the inmate with the plurality of mobile device contacts;

receive, from the inmate, a selection of mobile device contacts from the plurality of mobile device contacts to obtain a plurality of selected telephone contacts; and

- populate a telephone list of the inmate with the plurality of selected telephone contacts.
- 15.** The system of claim **14**, further comprising: a reviewer application configured to:
- review the plurality of mobile device contacts for persons-of-interest; and
 - notify an administrator when a person-of-interest is found in the plurality of mobile device contacts.
- 16.** The system of claim **14**, further comprising: an inmate phone for connecting to a telephone network, wherein the network application further comprises:
- an authentication module configured to authenticate the inmate for telephone communication; and
 - a communication module configured to:
 - receive, in response to authenticating the inmate, a connection request to communicate with a telephone contact; and
 - connect, using the inmate phone, the inmate to the telephone contact when the telephone contact is in the telephone list of the inmate.
- 17.** The system of claim **13**, wherein the database server further comprises a superfriend account for an administrator, and wherein the controlled setup module is further configured to:
- generate the superfriend account for the administrator; and
 - add an administrator to the secure social network list of the inmate, wherein the superfriend account comprises an administrative privilege and a removal protection in the secure social network list of the inmate.
- 18.** The system of claim **13**, further comprising: an inmate kiosk for connecting to a secure social network, wherein the network application further comprises:
- an authentication module configured to authenticate the inmate for secure social network communication; and
 - a communication module configured to:
 - connect, via the secure social network, the inmate to the secure social network list when the inmate is authenticated.
- 19.** A non-transitory computer readable medium for network priming for an inmate of a controlled facility, the non-transitory computer readable medium comprising computer readable program code for:
- receiving authentication credentials for the inmate to access a third party social network;
 - importing a plurality of social network contacts from the third party social network;
 - filtering the plurality of social network contacts for prohibited contacts;
 - presenting the inmate with the plurality of social network contacts;
 - receiving, from the inmate, a selection of social network contacts from the plurality of social network contacts to obtain a plurality of selected social network contacts; and
 - populating a secure social network list of the inmate with the plurality of selected social network contacts.
- 20.** The non-transitory computer readable medium of claim **19**, further comprising computer readable program code for: importing a plurality of mobile device contacts from a mobile device confiscated from the inmate; filtering the plurality of mobile device contacts for prohibited contacts; presenting the inmate with the plurality of mobile device contacts; receiving, from the inmate, a selection of mobile device contacts from the plurality of mobile device contacts to obtain a plurality of selected telephone contacts; and populating a telephone list of the inmate with the plurality of selected telephone contacts.
- 21.** The non-transitory computer readable medium of claim **20**, further comprising computer readable program code for: obtaining a social network identifier for at least one contact in the plurality of telephone contacts; and populating the plurality of social network contacts with the social network identifier for the at least one contact.
- 22.** The non-transitory computer readable medium of claim **17**, further comprising computer readable program code for: adding an administrator to the secure social network list of the inmate; and providing the administrator with an administrative privilege and a removal protection from the secure social network list.
- 23.** A method for network priming for an inmate of a controlled facility comprising:
- importing a plurality of mobile device contacts from a mobile device used by the inmate;
 - filtering the plurality of mobile device contacts for prohibited contacts;
 - presenting the inmate with the plurality of mobile device contacts;
 - receiving, from the inmate, a selection of mobile device contacts from the plurality of mobile device to obtain a plurality of selected telephone contacts; and
 - populating a telephone list of the inmate with the plurality of selected telephone contacts.

* * * * *



US 20140280631A1

(19) **United States**

(12) **Patent Application Publication**
Torgersrud

(10) **Pub. No.: US 2014/0280631 A1**

(43) **Pub. Date: Sep. 18, 2014**

(54) **MESSAGE TRANSMISSION SCHEME IN A CONTROLLED FACILITY**

(52) **U.S. Cl.**
CPC *H04L 51/14* (2013.01)
USPC *709/206*

(71) Applicant: **TELMATE LLC**, San Francisco, CA (US)

(57) **ABSTRACT**

(72) Inventor: **Richard Torgersrud**, San Francisco, CA (US)

A method for message transmission in a controlled facility includes receiving a request to transmit a message from a superfriend in a controlled facility. The superfriend includes an administrative privilege and a removal protection. The method further includes receiving, for the message from a superfriend network list of the superfriend, a selection contacts confined in the controlled facility, sending, via an electronic network, the message to each of the contacts in the controlled facility, and presenting the message to each of the contacts in the controlled facility. For each contact, the method further includes calculating audit information capturing the presenting of the message, and transmitting an acknowledgement of receipt of the message to the superfriend

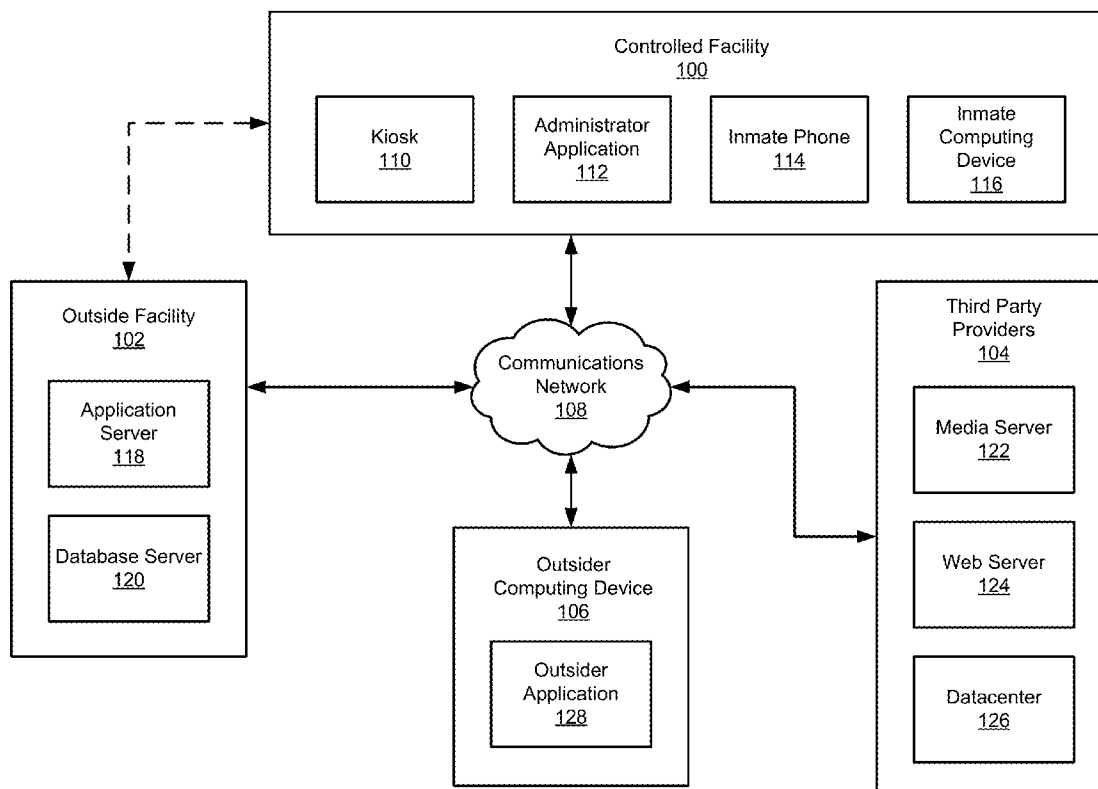
(73) Assignee: **TELMATE LLC**, San Francisco, CA (US)

(21) Appl. No.: **13/843,968**

(22) Filed: **Mar. 15, 2013**

Publication Classification

(51) **Int. Cl.**
H04L 12/58 (2006.01)



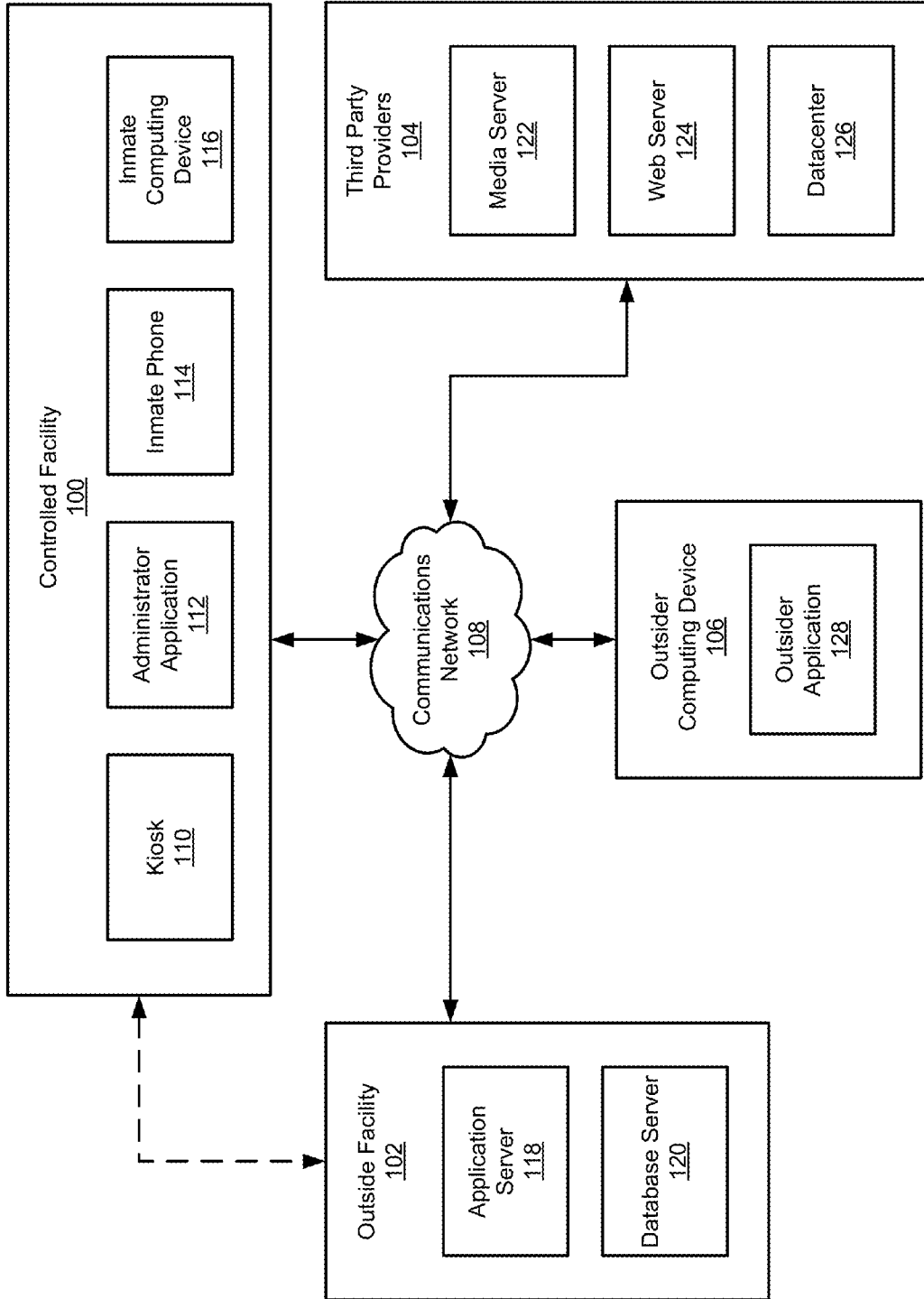


FIG. 1

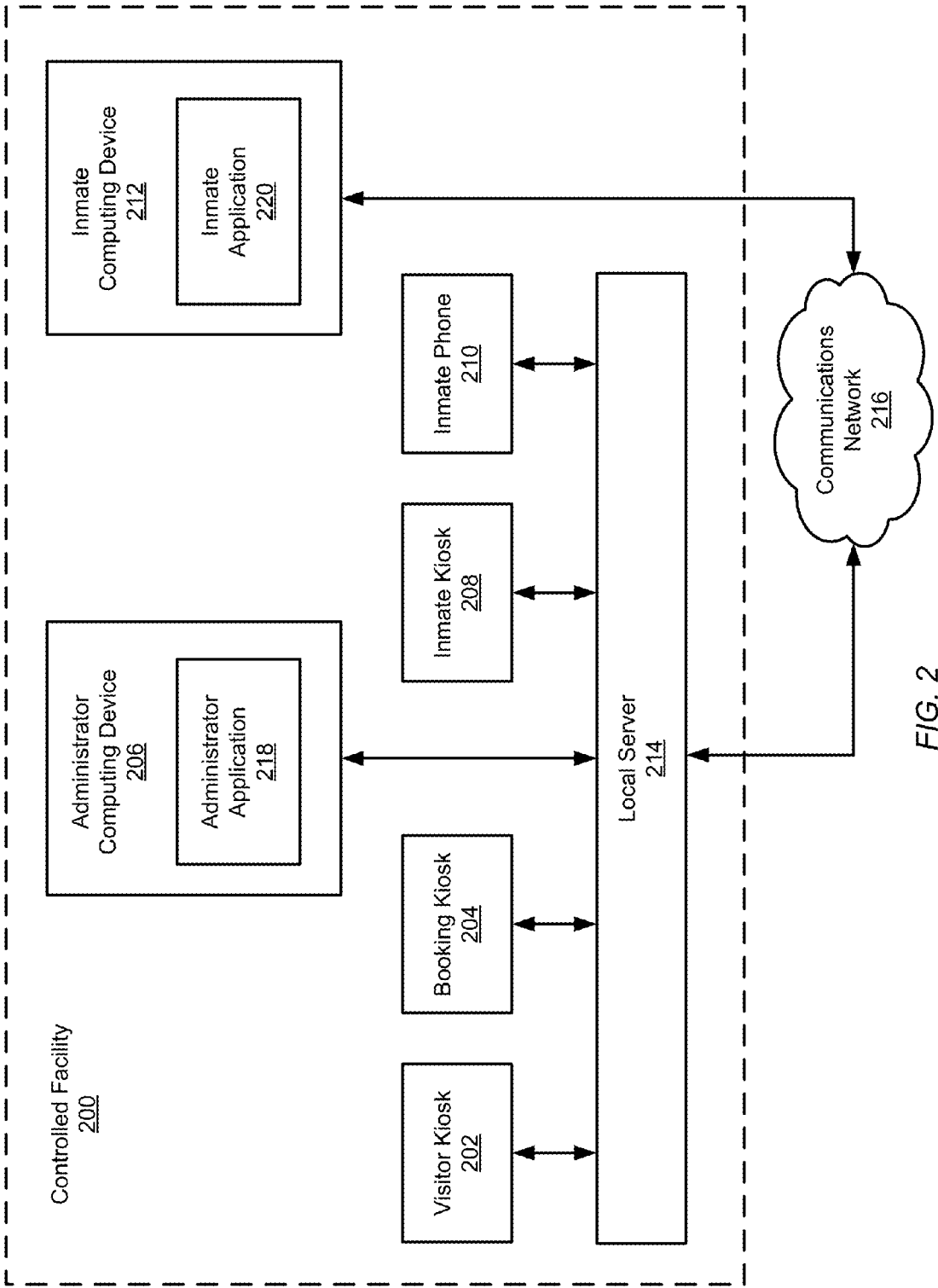


FIG. 2

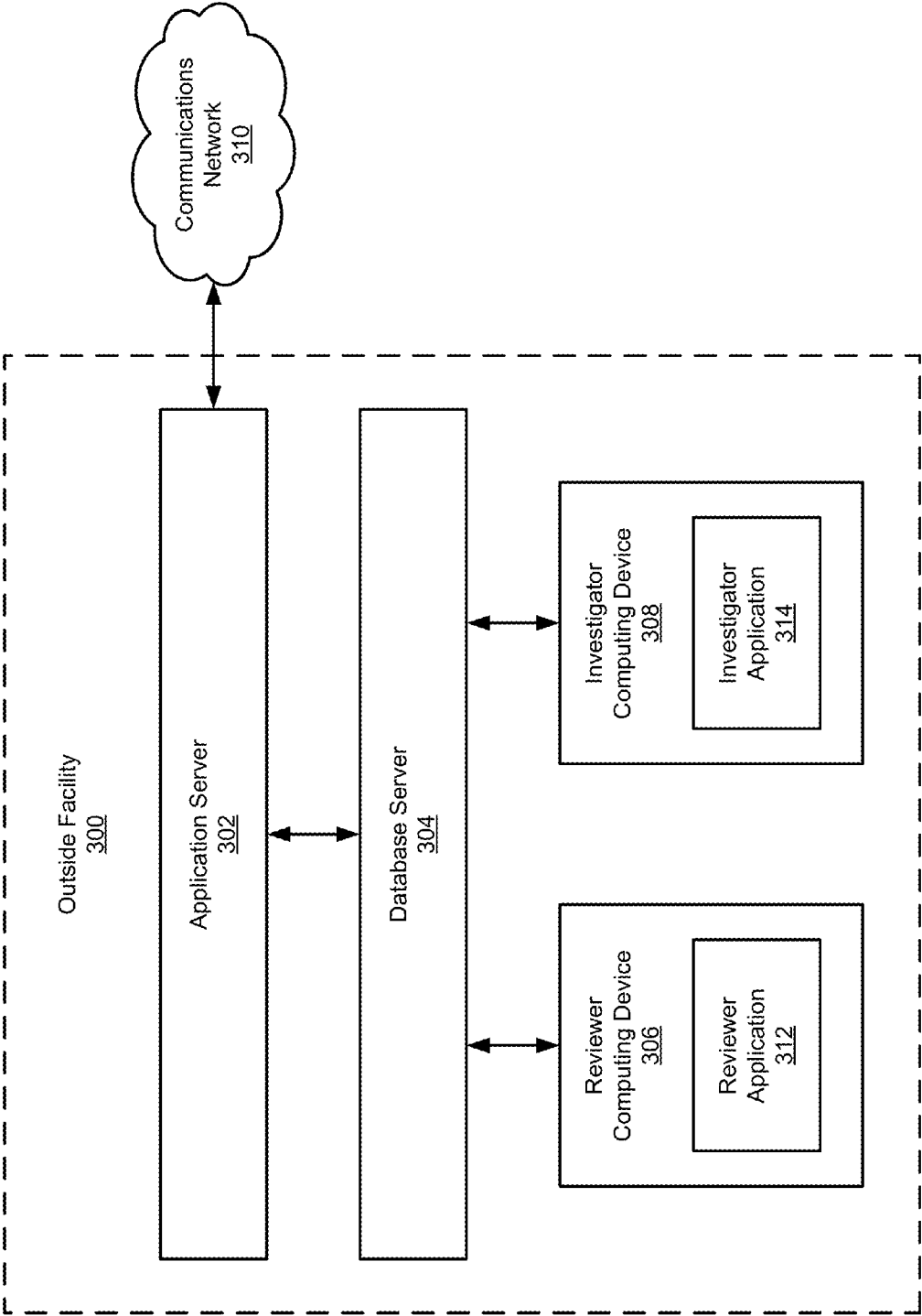


FIG. 3

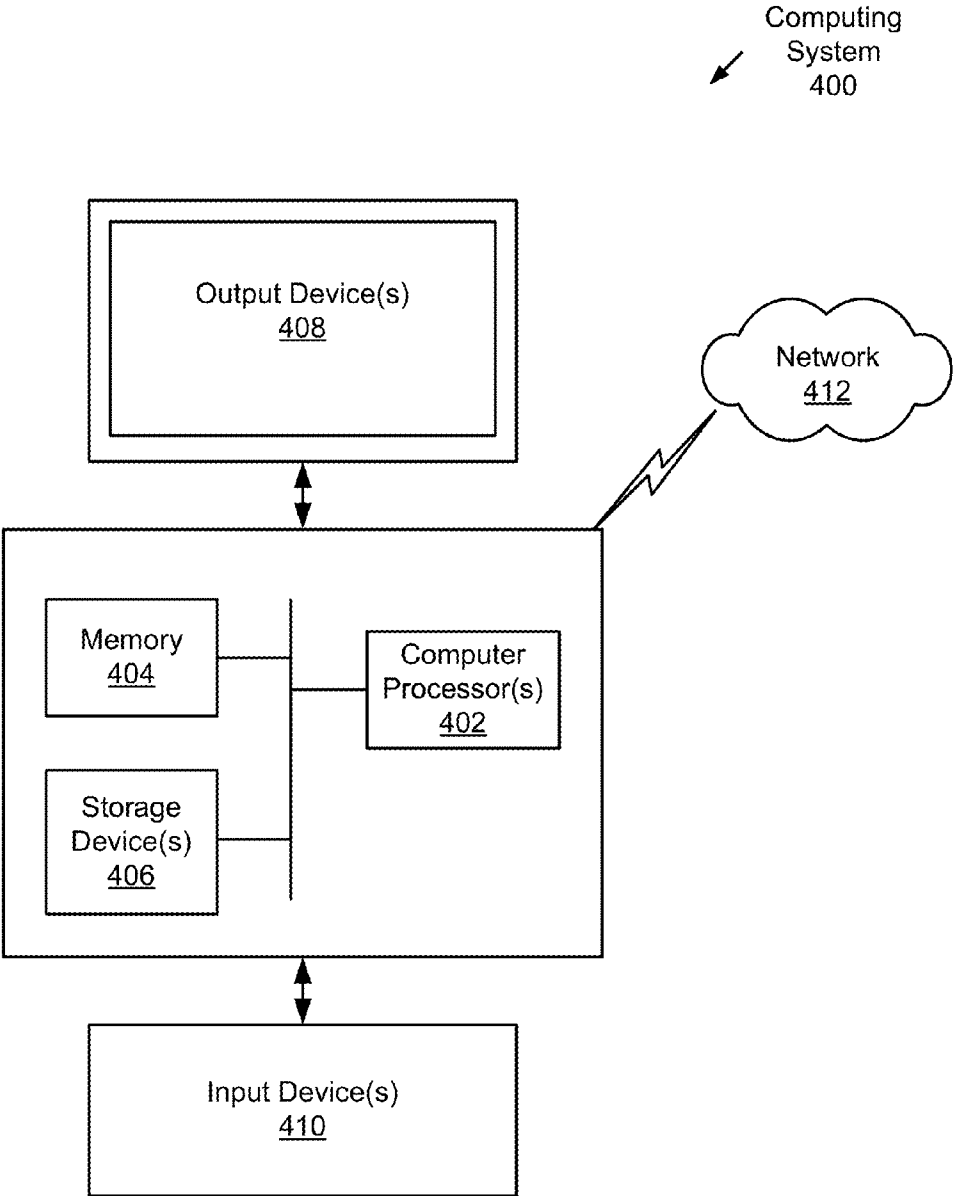


FIG. 4

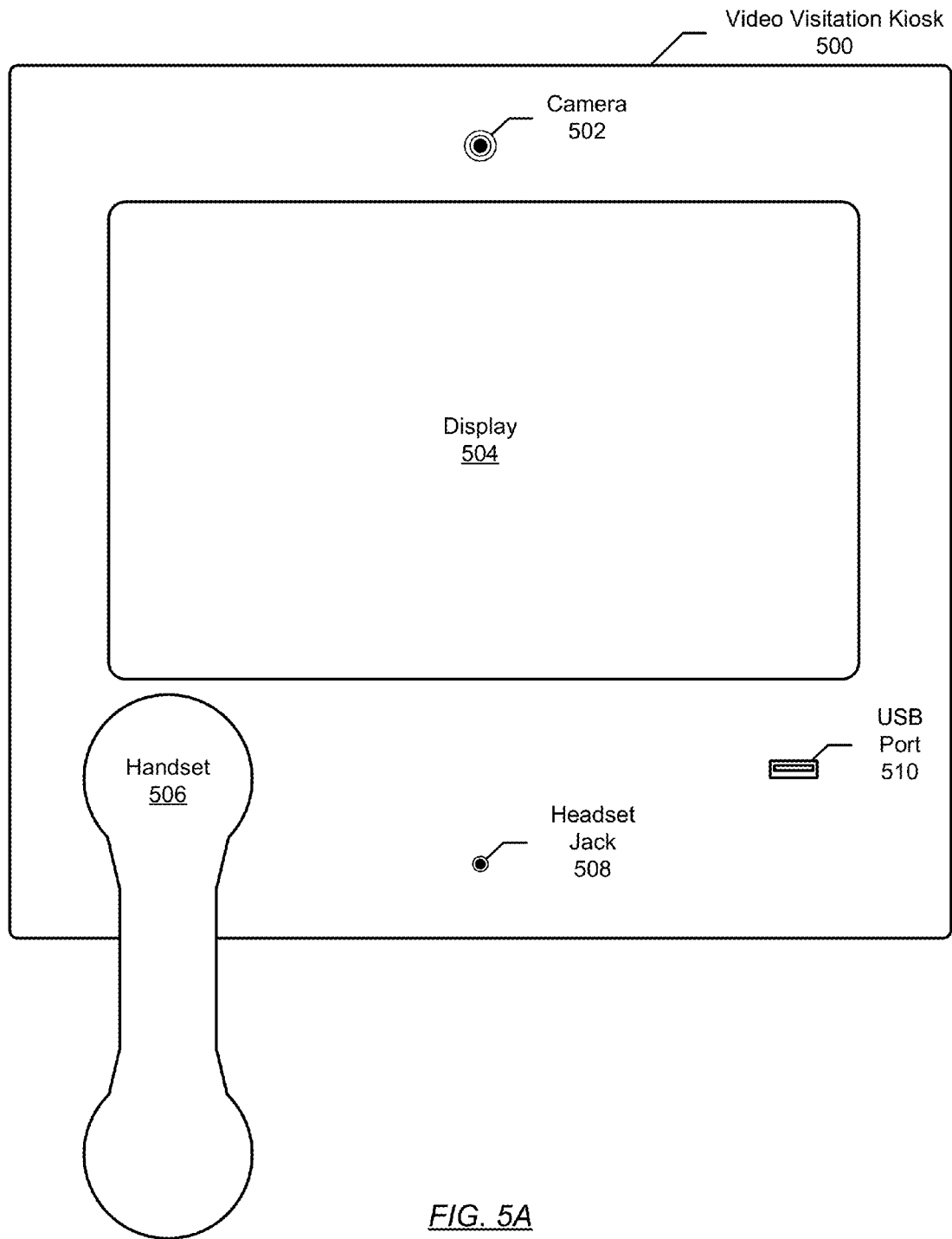


FIG. 5A

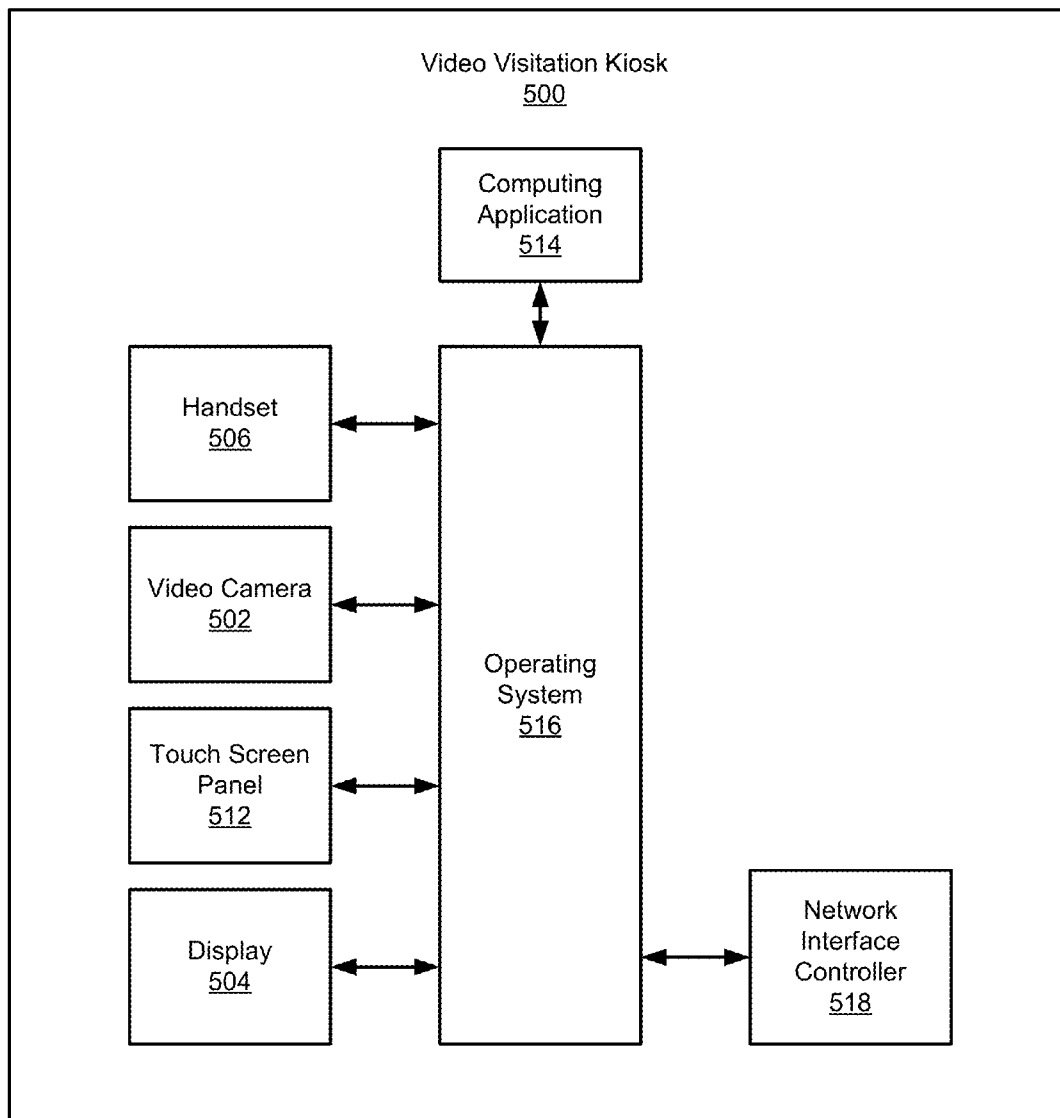


FIG. 5B

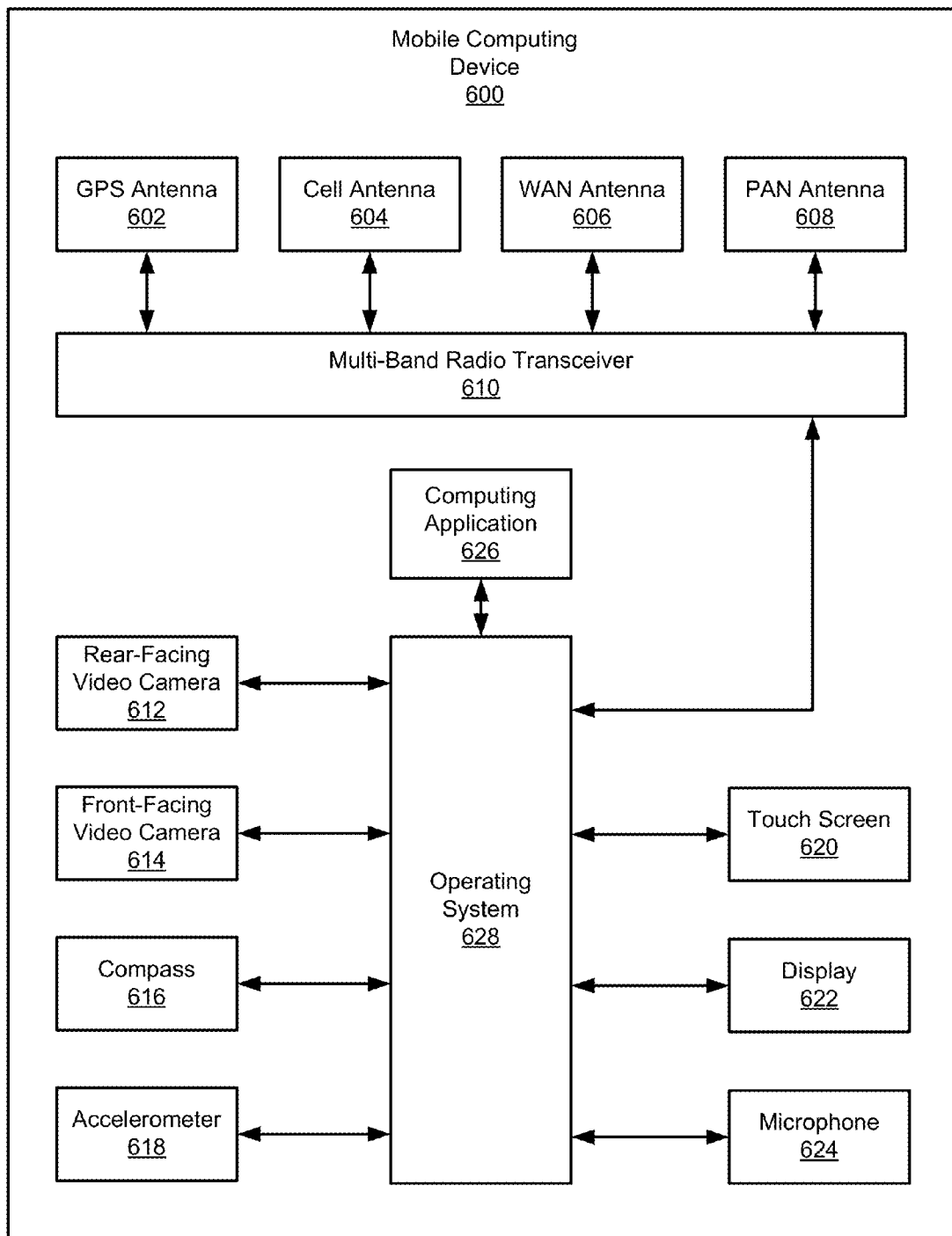


FIG. 6

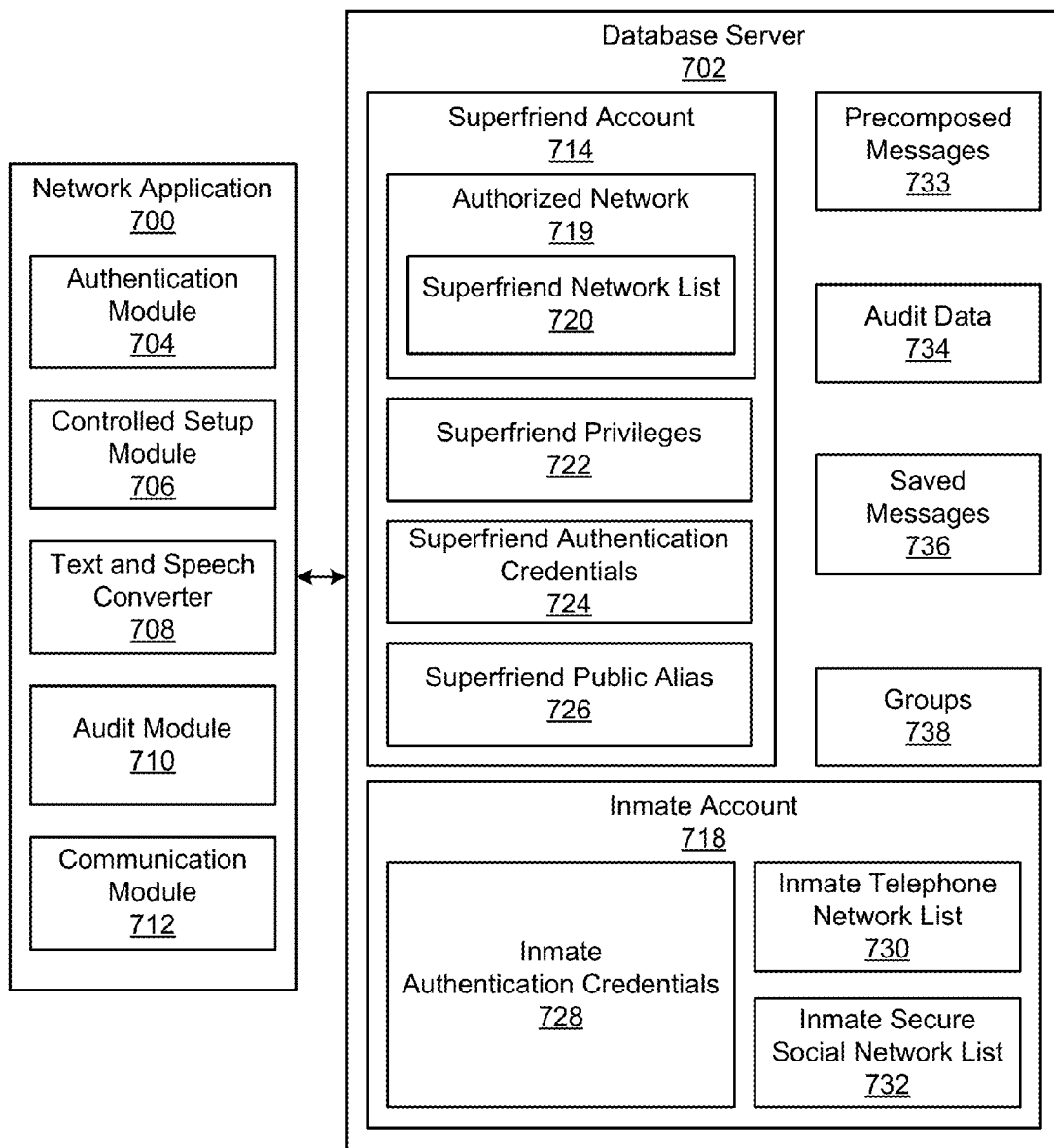


FIG. 7

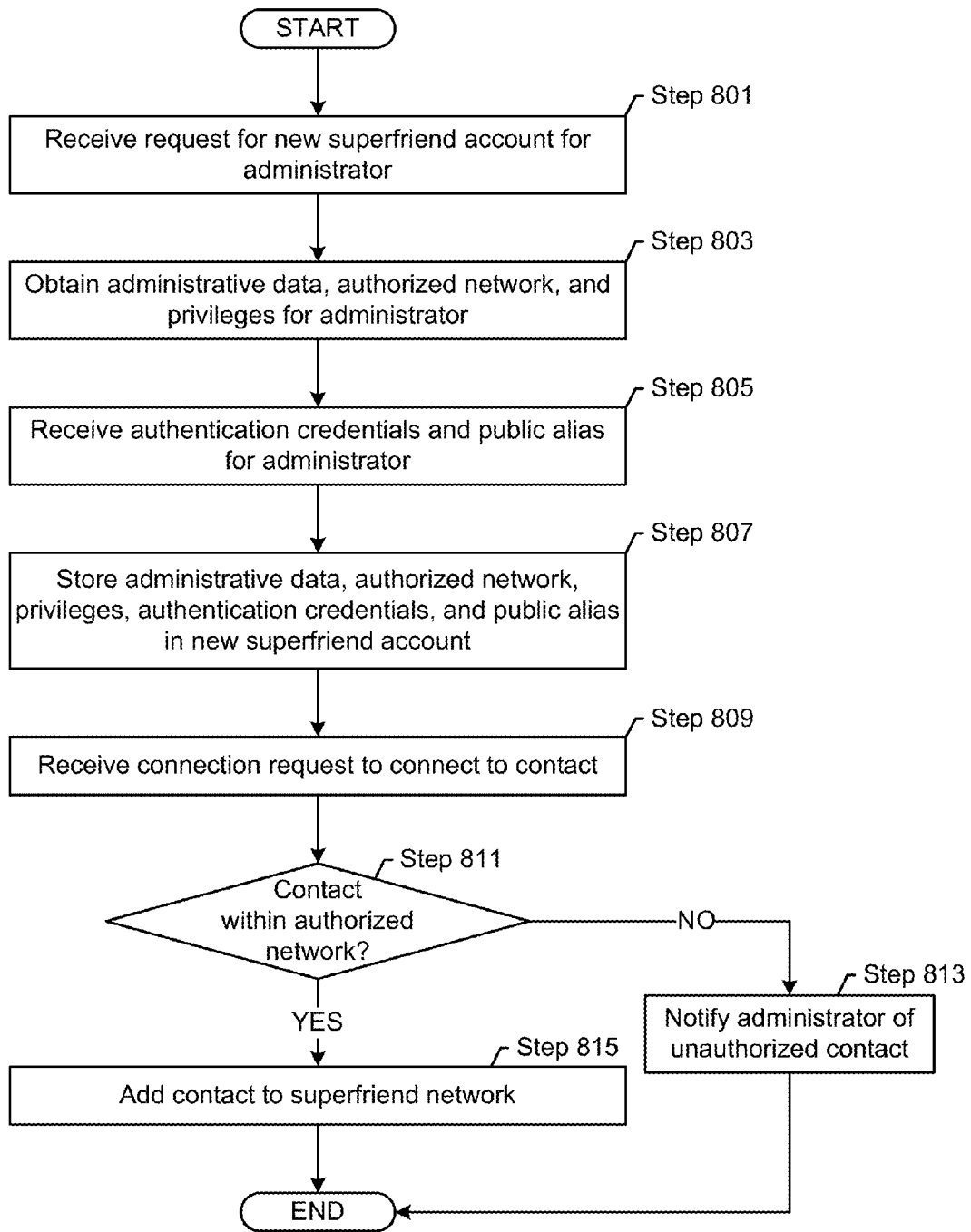


FIG. 8

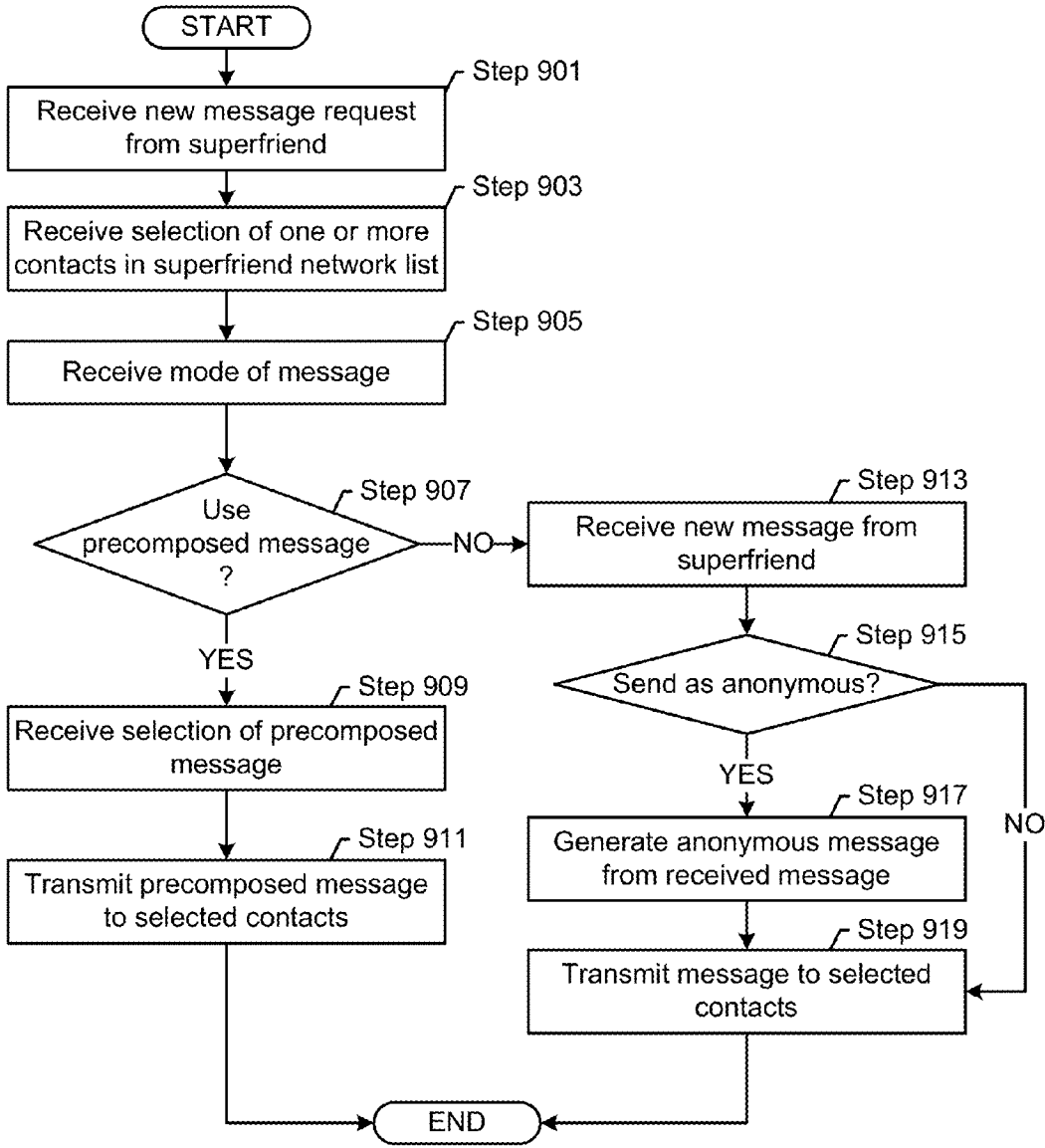


FIG. 9

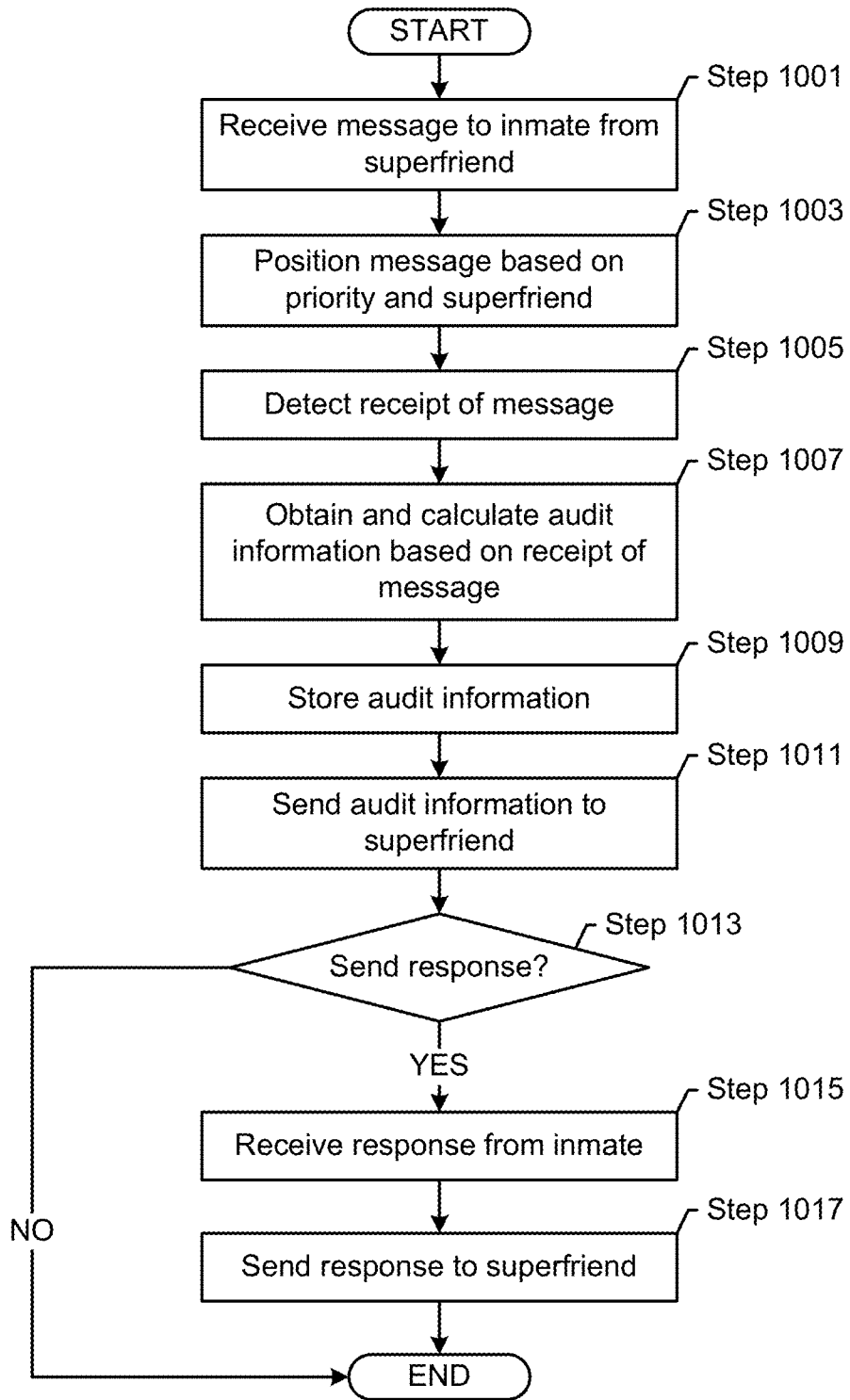


FIG. 10

1100 User Interface

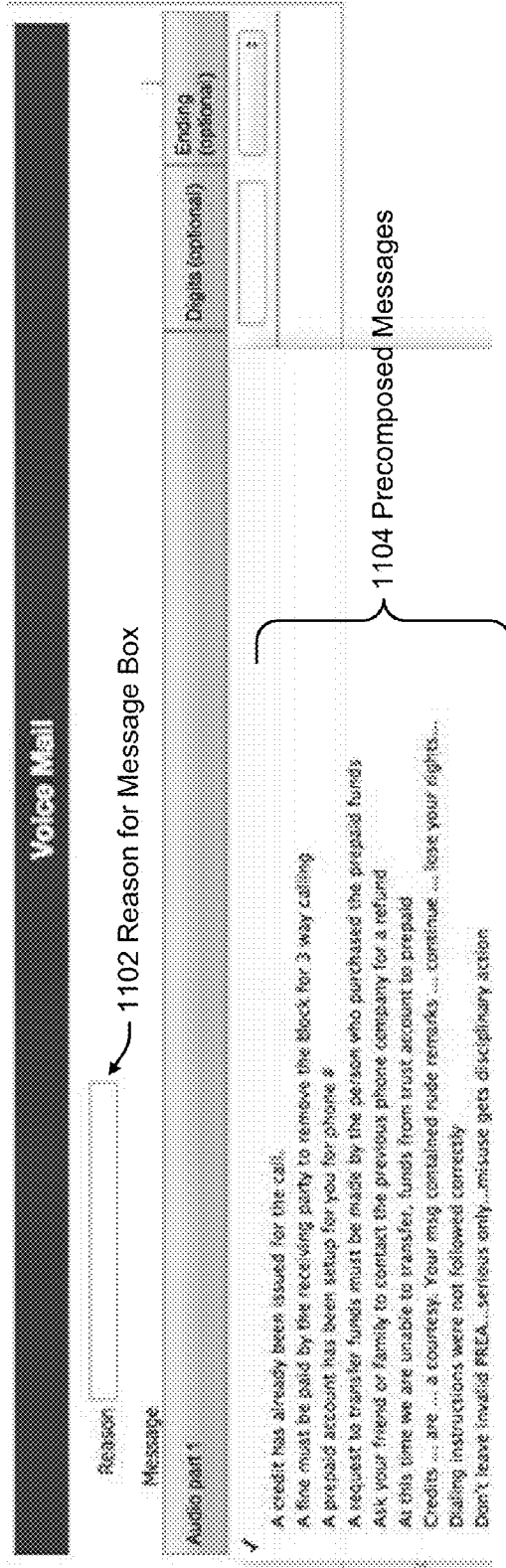


FIG. 11

MESSAGE TRANSMISSION SCHEME IN A CONTROLLED FACILITY

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is related to U.S. patent application Ser. No. 13/438,940 filed on Apr. 4, 2012, entitled "Secure Social Network." U.S. patent application Ser. No. 13/438,940 is incorporated by reference in its entirety.

BACKGROUND

[0002] Controlled facilities, such as a jail, prison, secure detention environments, detention facility, secured hospital, or addiction treatment facility, house large populations of individuals in confinement, which presents unique administrative challenges. In such detention environments, detained individuals, such as prisoners, offenders, convicts, military personnel, patients, government cleared personnel, or other detainees, frequently desire to communicate with individuals outside the detention environment such as friends or family members.

SUMMARY

[0003] In general, in one aspect, embodiments relate to a method for message transmission in a controlled facility. The method includes receiving a request to transmit a message from a superfriend in a controlled facility. The superfriend includes an administrative privilege and a removal protection. The method further includes receiving, for the message from a superfriend network list of the superfriend, a selection contacts confined in the controlled facility, sending, via an electronic network, the message to each of the contacts in the controlled facility, and presenting the message to each of the contacts in the controlled facility. For each contact, the method further includes calculating audit information capturing the presenting of the message, and transmitting an acknowledgement of receipt of the message to the superfriend.

[0004] In general, in one aspect, embodiments relate to a system for message transmission in a controlled facility. The system includes a computer processor, a database server, and a network application. The database server includes a superfriend account for a superfriend. The superfriend account stores a superfriend network list, where the superfriend includes an administrative privilege and a removal protection. The network application executes on the computer processor and includes a communication module and an audit module. The communication module is configured to receive a request to transmit a message from the superfriend in a controlled facility, receive, for the message from the superfriend network list of the superfriend, a selection of contacts confined in the controlled facility, send, via an electronic network, the message to each of the contacts in the controlled facility, and present the message to each of the contacts in the controlled facility. For each contact, the audit module is configured to calculate audit information capturing the presenting of the message, and transmit an acknowledgement of receipt of the message to the superfriend.

[0005] In general, in one aspect, embodiments relate to a non-transitory computer readable medium for message transmission in a controlled facility. The non-transitory computer readable medium includes computer readable program code for receiving a request to transmit a message from a super-

friend in a controlled facility. The superfriend includes an administrative privilege and a removal protection. The computer readable program code is further for receiving, for the message from a superfriend network list of the superfriend, a selection contacts confined in the controlled facility, sending, via an electronic network, the message to each of the contacts in the controlled facility, and presenting the message to each of the contacts in the controlled facility. For each contact, The computer readable program code is further for calculating audit information capturing the presenting of the message, and transmitting an acknowledgement of receipt of the message to the superfriend.

[0006] Other aspects of the invention will be apparent from the following description and the appended claims.

BRIEF DESCRIPTION OF DRAWINGS

[0007] FIGS. 1-7 show schematic diagrams of a system in one or more embodiments of the invention.

[0008] FIGS. 8-10 show flowcharts of a method in one or more embodiments of the invention.

[0009] FIG. 11 shows an example in one or more embodiments of the invention.

DETAILED DESCRIPTION

[0010] Specific embodiments of the invention will now be described in detail with reference to the accompanying figures. Like elements in the various figures are denoted by like reference numerals for consistency.

[0011] In the following detailed description of embodiments of the invention, numerous specific details are set forth in order to provide a more thorough understanding of the invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these specific details. In other instances, well-known features have not been described in detail to avoid unnecessarily complicating the description.

[0012] In general, embodiments of the invention provide a method and system for distributing messages in a controlled facility, and providing for the forced association of inmates with certain facility staff or communications system operator staff in a secure social network. Specifically, one or more embodiments transmit messages between a superfriend and inmates. A superfriend is a staff member of or other person affiliated with the controlled facility, or an employee of the communications system operator with an administrative privilege and removal protection. Removal protection prevents the individual from be removed from the contact. The superfriend sends a message to contacts in the controlled facility. The message is presented to the contact and audit information is calculated from the presentation of the message. Further, the administrator of the controlled facility is notified of the receipt of the message. The audit information may be transmitted to an investigator for investigative purposes.

[0013] Embodiments of the invention may include interactions with a secure social network. In one or more embodiments of the invention, a secure social network is a network application that facilitates and secures the exchange or transmission of information between two or more parties in which at least one of those parties is subject to special security or law enforcement restrictions or otherwise resides in, or is subject to the controls of a controlled facility. Exchanged or transmitted information may be member generated, such as a

photo or a video message, or it may be member-curated, such as a news headline, a famous quote, or a sports score.

[0014] FIG. 1 shows a diagram of a system in accordance with one or more embodiments of the invention. As shown in FIG. 1, the system includes a controlled facility (100), an outside facility (102), third party providers (104), and an outsider computing device (106) each communicatively coupled to a communications network (108). The controlled facility (100) may include, but is not limited to, a kiosk (110), an administrator application (112), an inmate phone (114), and an inmate computing device (116). The outside facility (102) may include an application server (118) and a database server (120). The third party providers (104) may include a media server (122), a web server (124), and a datacenter (126). The outsider computing device (106) may include an outsider application (128).

[0015] In one or more embodiments of the invention, a controlled facility (100) is an access-restricted location. Examples of controlled facilities (e.g., controlled facility (100)) include, but are not limited to, detention environments (e.g., jails, prisons, etc.), immigration detention centers, military centers, government secure sites, law enforcement holding structures, secure business complexes, and psychiatric hospitals.

[0016] In one or more embodiments of the invention, an inmate is a person within a controlled facility (100) who is subject to one or more restrictions, primarily to his or her freedom or rights. Examples of inmates include, but are not limited to, prisoners, wards of the state, parolees, employees working in a secure business complex, temporary or long-term internees, patients, military personnel, uncharged suspects, and refugees. Inmate restrictions may be part of a court-imposed sentence on an inmate, while others may be specific to the controlled facility (100) in which the inmate resides. Restrictions may include limitations on an inmate's physical movement (i.e., physical restrictions) and limitations on the inmate's ability to communicate (i.e., communication restrictions). Communication restrictions include inmate use restrictions, inmate target restrictions, and device use restrictions.

[0017] In one or more embodiments of the invention, inmate use restrictions are limitations on an inmate's general ability to communicate with visitors and/or outsiders. Inmate use restrictions may include, for example, periods of time in which an inmate is not allowed to communicate with outsiders or visitors (e.g., between 10 PM and 8 AM, during an imposed one-week punitive period, etc.) and limitations based on lack of funds (e.g., insufficient commissary account balance to initiate a communication).

[0018] In one or more embodiments of the invention, inmate target restrictions are limitations on the target or source of a communication with the inmate. Inmate target restrictions may be specific outsiders or visitors with whom the inmate is not allowed to communicate (e.g., the victim of a crime perpetrated by the inmate, etc.). Inmate target restrictions may also include types of people with whom the inmate is not allowed contact (e.g., outsiders who are ex-cons, minors under the age of 18, etc.).

[0019] In one or more embodiments of the invention, device use restrictions are restrictions based on the condition or state of the communication device used by the inmate. Device use restrictions include, for example, limitations

based on the location of the inmate's mobile device, limitations imposed based on a determination that the device has been tampered with, etc.

[0020] In one or more embodiments of the invention, an outsider is a person outside the controlled facility (100) who may be the source or target of a communication with an inmate. An outsider who enters the controlled facility (100) for the purpose of communicating with an inmate is referred to as a visitor.

[0021] In one or more embodiments of the invention, the kiosk (110) is a computing system with functionality to facilitate communication between an inmate and a visitor or outsider. Such communication facilitation may include creating a system identity data item or secure social networking account, adding or importing contact information for outsiders with whom the inmate wishes to communicate, uploading media (e.g., photos, videos, audio, and text) to, or viewing media from, a secure social network, sending or receiving messages or other media, acting as an endpoint for voice and video communication between an inmate and a visitor or outsider, scheduling a communication, and managing a commissary or communications account. Further detail about kiosks (e.g., kiosk (110)) is provided in FIG. 2, FIG. 5A, FIG. 5B, and FIG. 6.

[0022] In one or more embodiments of the invention, the administrator application (112) is a process or group of processes executing on a computing system with functionality to enable an administrator to create, remove, and/or enforce one or more restrictions on an inmate. In one or more embodiments of the invention, an administrator is a person associated with the controlled facility charged with enforcing one or more restrictions. Examples of administrators include, but are not limited to, prison guards, orderlies, wardens, prison staff, jailers, information technology technicians, system administrators, and law enforcement agents. In one or more embodiments of the invention, an administrator is a person associated with the software developer/operator, whose use of Superfriend privileges is for the purpose of communicating system events, notices, and/or promotions to the users of the system. Using the administrator application, an administrator may retrieve or alter the identity data item and/or secure social network account of an inmate, visitor, or outsider. Further detail about the administrator application (112) is provided in FIG. 2.

[0023] In one or more embodiments of the invention, the inmate phone (114) is a device with functionality to send and receive audio communications between an inmate and an outsider or visitor. In one or more embodiments of the invention, the inmate phone (114) is a stationary (i.e., non-mobile) device. Further, a single inmate phone (114) may be used by more than one inmate. Further detail about the inmate phone (114) is provided in FIG. 2.

[0024] In one or more embodiments of the invention, the inmate computing device (116) is a computing device with functionality to enable an inmate to communicate with a visitor or outsider. Specifically, the inmate computing device (116) may be used to send or receive text messages and/or initiate or receive voice or video calls. In one or more embodiments of the invention, the inmate computing device (116) also enables an inmate to access a secure social network. Specifically, the inmate computing device (116) may be used to upload media to, or view media from, a secure social network account of the inmate or another secure social network member. In one or more embodiments of the invention,

the inmate computing device (116) is a mobile computing device (e.g., a smartphone, a laptop, a tablet, etc.). Further detail about the inmate computing device (116) is provided in FIG. 2 and FIG. 6.

[0025] In one or more embodiments of the invention, the elements within the controlled facility (100) are communicatively coupled to the communications network (108). In one or more embodiments of the invention, the communications network (108) is a collection of computing systems and other hardware interconnected by communication channels. The communications network (108) may include networks that are exclusively or primarily used for a single type of communication, such as a telephone network (e.g., Public Switched Telephone Network (PSTN), Plain Old Telephone System (POTS)), and/or networks used for a wide array of communication types, such as the Internet through Voice over IP (VoIP). Communication channels used by the communications network (108) may include, for example, telephone lines, networking cables, wireless signals, radio waves, etc. Fees charged and payments received by the provider(s) of the communications network (108) may involve multiple parties, including a service provider of the outside facility (102), the management of the controlled facility (100), and provider(s) of the communications network (108). In one or more embodiments of the invention, fees may be split between multiple parties based on the terms of underlying agreements or contracts between the parties. Further, rebates, reimbursements, and/or refunds may be afforded to and paid to the management of the controlled facility (100) based on the terms of underlying agreements or contracts between the parties. For example, the management of the controlled facility (100) may receive a rebate from the service provider of the services provided to inmates based on such factors as the volume of use, the dollar amount, and/or the frequency of use.

[0026] In one or more embodiments of the invention, the outside facility (102) is a group of computing systems located outside of the controlled facility (100). Specifically, the outside facility (102) may house system elements with functionality to facilitate communication between inmates and outsiders, access communication data between inmates and outsiders, and enforce one or more restrictions imposed on inmates and inmate communications. In one or more embodiments of the invention, the outside facility (102) is connected directly to the controlled facility (100) bypassing a generally accessible communications network (communications network (108)). One or more of the components within the outside facility (102) may alternatively be located within the controlled facility (100) or within the third party providers (104).

[0027] In one or more embodiments of the invention, the application server (118) is a computing system with functionality to authenticate an inmate, outsider, administrator, reviewer, or investigator for access to system functionality (e.g., initiating voice or video calls, sending text messages, etc.) or data stored on the database server (120) (e.g., inmate identities, communications between inmates and outsiders, etc.). The application server may authenticate inmates, outsiders, administrators, reviewers, and/or investigators using passwords, biometric data, digital access codes, and/or physical access devices. Further detail about the application server (118) is provided in FIG. 3.

[0028] In one or more embodiments of the invention, the database server (120) is a computing system with functionality to store identities used to authenticate inmates, outsiders,

administrators, reviewers, and/or investigators. Such identities may include verified data used to compare to verification data provided by the inmate, outsider, administrator, reviewer, or investigator to authenticate the inmate, outsider, administrator, reviewer, or investigator.

[0029] In one or more embodiments of the invention, the database server (120) also stores communication data about communications between an inmate and an outsider or visitor. Such communication data may include, for example, a recording of a video call, the length of a voice call, the frequency of video calls, sent and received text messages, etc. The database server (120) may also store media submitted to a secure social network before, during, and/or after the media has been reviewed. Further detail about the database server (120) is provided in FIG. 3.

[0030] In one or more embodiments of the invention, the third party providers (104) are computing systems that provide network application and data storage services (i.e., cloud computing services). Third party providers (104) may include service providers used directly by inmates and outsiders, such as photo sharing services, general social networking sites, and digital music retailers. Third party providers (104) may include service providers employed by administrators and for use by inmates and outsiders, such as audio and video streaming applications, conferencing applications, and secure social network media storage. One or more of the components within the third party providers (104) may alternatively be located within the controlled facility (100) or the outside facility (102).

[0031] In one or more embodiments of the invention, the media server (122) is a computing system or group of computing system with functionality to provide network application services to facilitate communication between an inmate and an outsider, and to facilitate access to a secure social network. Such services include, but are not limited to, VoIP services, video conferencing services, and media streaming services.

[0032] In one or more embodiments of the invention, the web server (124) is a computing system or group of computing system with functionality to provide an interface to access and interact with webpages and other network application services. In one or more embodiments of the invention, the web server (124) is a type of media server (122).

[0033] In one or more embodiments of the invention, the datacenter (126) is a computing system or group of computing system with functionality to provide an interface to access and interact with data stored on one or more data servers (not shown). In one or more embodiments of the invention, the datacenter (126) is a type of media server (122).

[0034] In one or more embodiments of the invention, the outsider computing device (106) is a computing device with functionality to execute the outsider application (128). In one or more embodiments of the invention, the outsider computing device (106) is a mobile computing device (e.g., a smartphone, a laptop, a tablet, etc.). Further detail about the outsider computing device (106) is provided in FIG. 6.

[0035] In one or more embodiments of the invention, the outsider application (128) is a process or group of processes (in software, firmware, hardware, or combination thereof) with functionality to enable communication between an outsider and an inmate. Specifically, the outsider application (128) may be used to send or receive text messages and/or initiate or receive voice or video calls. In one or more embodiments of the invention, the outsider application (128) also

enables an outsider to access a secure social network. Specifically, the outsider application (128) may be used to upload media to, or view media from, a secure social network account of the outsider, an inmate, other secure social network member.

[0036] FIG. 2 shows a controlled facility in accordance with one or more embodiments of the invention. As shown in FIG. 2, the controlled facility (200) may include a visitor kiosk (202), a booking kiosk (204), an administrator computing device (206), an inmate kiosk (208), an inmate phone (210), an inmate computing device (212), and a local server (214). The inmate computing device (212) and the local server (214) are communicatively coupled to the communications network (216). The administrator computing device (206) includes an administrator application (218). The inmate computing device (212) includes an inmate application (220).

[0037] In one or more embodiments of the invention, the visitor kiosk (202) is a computing system with functionality to facilitate communication between an inmate and a visitor. Specifically, the visitor kiosk (202) may be a combination of computing hardware and software used by a visitor to make and receive voice and video calls to/from an inmate residing in the same controlled facility (200) or another controlled facility (not shown). The visitor kiosk (202) may also be used to schedule a voice or video call with an inmate for a future date. Further, the visitor kiosk (202) may also include the functionality to exchange media (e.g., photos, videos, and audio) with an inmate residing in the controlled facility (200). The visitor kiosk (202) may include functionality to generate such media, such as a camera, microphone, keyboard, and software to record or otherwise create media to send to an inmate. Such media may be subject to review before being delivered.

[0038] In one or more embodiments of the invention, a visitor wanting to use a visitor kiosk (202) may be required to participate in an authentication process to verify the identity of the visitor. The authentication process may include creating an identity data item and verified data for storage and later comparison. The verified data used for authentication may be a username and password combination and/or biometric information about the visitor.

[0039] In one or more embodiments of the invention, the visitor kiosk (202) includes functionality to access a secure social network. Specifically, the visitor kiosk (202) may be used by a visitor to create and manage a secure social network account. The visitor kiosk (202) may also be used by a visitor to upload digital media to the visitor's secure social network account or the account of another secure social network member. The visitor kiosk (202) may further be used to view digital media uploaded to the visitor's social network account or the account of another secure social network member.

[0040] In one or more embodiments of the invention, the visitor kiosk (202) includes functionality to manage a commissary account for one or more inmates. Specifically, a visitor may use a visitor kiosk (202) to add money to the commissary account of an inmate in the controlled facility (200), view a transaction history of the commissary account, transfer funds between commissary accounts, and/or remove funds from a commissary account. Further detail about the visitor kiosk (202) is provided in FIG. 5A and FIG. 5B.

[0041] In one or more embodiments of the invention, the booking kiosk (204) is a computing system with functionality to aid administrators in admitting an inmate into a controlled facility (e.g., controlled facility (200)). Specifically, the book-

ing kiosk (204) may include functionality to create or update an inmate identity data item. Specifically, the booking kiosk (204) may be used to obtain verified data (e.g., passwords, biometric data, etc.) and save the verification data in one or more identity data items for the inmate. The verified data may then be used to authenticate the inmate (e.g., to access the communications network (216), etc.). In one or more embodiments of the invention, the booking kiosk may also be used to associate one or more restrictions with the inmate via the inmate's identity data item.

[0042] In one or more embodiments of the invention, the booking kiosk (204) includes functionality to input contact information for visitors, outsiders, administrators, or other inmates with whom the inmate wants to communicate. Such contact information may then be associated with the inmate's identity data item, and may be used to initiate a voice or video call, or otherwise transmit media to visitors, outsiders, or other inmates. Further, In one or more embodiments of the invention, the contact information may be retrieved from an inmate's mobile computing device (e.g., cell phone, smart phone, etc.) or a local or remote data storage device (e.g., a flash drive, a webmail account, etc.). The contact information may be retrieved using a wired or wireless connection between the booking kiosk and the inmate's mobile computing device and/or the data storage device. The contact information may be subject to review before the inmate is permitted to contact the visitor, outsider, administrator, or other inmate.

[0043] In one or more embodiments of the invention, the booking kiosk (204) includes functionality to prepare a mobile computing device for use by the inmate within the controlled facility (200). Specifically, a controlled facility (200) may allow inmates the use of computing devices while in or subject to the controlled facility (200). However, use of such inmate computing devices may require that the computing device is instrumented with software restricting the use of the inmate computing device. The booking kiosk (204) may be used to instrument the inmate computing device as required. Further detail about the booking kiosk (204) is provided in FIG. 5A and FIG. 5B.

[0044] In one or more embodiments of the invention, the administrator computing device (206) is a computing system or group of computing systems with functionality to execute the administrator application (218). In one or more embodiments of the invention, the administrator application (218) is a process or group of process with functionality to provide access to communications between inmates at the controlled facility (200) and visitors, outsiders, administrators, and other inmates. The administrator application (218) may also be used to monitor current voice or video calls between an inmate and a visitor, outsider, administrator, or other inmate.

[0045] In one or more embodiments of the invention, the administrator application (218) is used to manage an identity data item associated with an inmate. Such management may include altering the restrictions (device use restrictions, inmate use restrictions, and inmate target restrictions) applicable to the inmate. In one or more embodiments of the invention, the administrator application (218) is used to access the secure social network account of an inmate, visitor, or outsider. In one or more embodiments of the invention, the administrator application (218) may provide heightened access (i.e., a level of access greater than that of the inmate, visitor, or outsider) to data stored in the secure social networking account.

[0046] In one or more embodiments of the invention, the inmate kiosk (208) is a computing system with functionality to facilitate communication between an inmate and a visitor or outsider. Specifically, the inmate kiosk (208) may be a combination of computing hardware and software used by an inmate to make and receive voice and video calls to/from a visitor, outsider, or another inmate residing in another controlled facility (not shown). The inmate kiosk (208) may also be used to schedule a voice or video call with a visitor at a future date. Initiating or scheduling a voice or video call may include determining whether the currently attempted call or the scheduled call are adverse to one or more restrictions (e.g., inmate use restrictions, device use restrictions, and/or inmate target restrictions). Further, the inmate kiosk (208) may also include the functionality to exchange media (e.g., photos, videos, and audio) with a visitor or outsider. The inmate kiosk (208) may include functionality to generate such media, such as a camera, microphone, keyboard, and software to record or otherwise create media to send to a visitor or outsider. Such media may be subject to review before being delivered.

[0047] In one or more embodiments of the invention, an inmate wanting to use an inmate kiosk (208) may be required to participate in an authentication process to verify the identity of the inmate. The authentication process may include providing verification data for comparison to verified data previously obtained from the inmate and stored in the inmate identity data item. The verified data may be a username and password combination and/or biometric information about the inmate.

[0048] In one or more embodiments of the invention, the inmate kiosk (208) includes functionality to access a secure social network. Specifically, the inmate kiosk (208) may be used by an inmate to manage a secure social network account. The inmate kiosk (208) may include functionality to generate such media, such as a camera, microphone, keyboard, and software to record or otherwise create media to send to a visitor or outsider. The inmate kiosk (208) may also be used by an inmate to upload digital media to the inmate's secure social network account or the account of another secure social network member. The inmate kiosk (208) may further be used to view digital media uploaded to the inmate's social network account or the account of another secure social network member. Uploaded media may be subject to review before posting.

[0049] In one or more embodiments of the invention, the inmate kiosk (208) includes functionality to manage a commissary account for the inmate. Specifically, an inmate may use an inmate kiosk (208) to view a transaction history of the commissary account and/or to apply commissary funds for goods and services consumed or enjoyed by the inmate. Further detail about the inmate kiosk (208) is provided in FIG. 5A and FIG. 5B.

[0050] In one or more embodiments of the invention, the inmate phone (210) is a device with functionality to send and receive audio communications between an inmate and an outsider or visitor. The inmate phone (210) may be implemented as handset connected to a telephone line. In one or more embodiments of the invention, all or part of the voice call may be conducted over a VoIP connection. In one or more embodiments of the invention, a single inmate phone (210) is utilized by multiple inmates.

[0051] In one or more embodiments of the invention, initiating or receiving a voice call using the inmate phone (210) requires a form of authentication (e.g., providing a password, personal identification number, or voice verification). In one

or more embodiments of the invention, voice calls made using the inmate phone (210) are monitored by one or more administrators using the administrator computing device (206), and are recorded and stored in a data storage system within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown). The inmate phone (210) may also be subject to device use restrictions limiting the ability to use the inmate phone (210) at certain times (e.g., between 9 PM and 8 AM) or under certain conditions (e.g., emergency lockdown).

[0052] In one or more embodiments of the invention, the identity of the visitor or outsider targeted by the inmate or attempting to contact the inmate using the inmate phone (210) is verified against inmate target restrictions imposed on the inmate. Such restrictions may be associated with the inmate's identity data item and may be stored locally within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown). The visitor or outsider identity may be verified by the local server (214) or by another server within the outside facility (not shown), or within a third party provider (not shown).

[0053] In one or more embodiments of the invention, the inmate computing device (212) is a computing system configured to execute the inmate application (202). In one or more embodiments of the invention, each inmate computing device (212) is utilized exclusively by a single inmate. In one or more embodiments of the invention, access to the inmate application requires a form of initial authentication. This initial authentication may use verification data stored locally on the inmate computing device (212) (e.g., a code or combination used to unlock the phone, locally stored biometric data, etc.).

[0054] In one or more embodiments of the invention, accessing a communications network (e.g., communications network (216)) using the inmate application (220) may require further network-based authentication. This further authentication may use verification data stored external to the inmate computing device (212) but locally within the controlled facility (200), or remotely within the outside facility (not shown) or within a third party provider (not shown).

[0055] In one or more embodiments of the invention, an authenticated inmate may use the inmate application to initiate or receive voice or video calls, initiate or receive text or media messages, schedule a voice or video call, manage a commissary account, or post media to a secure social network. In one or more embodiments of the invention, voice and video calls made using the inmate computing device (212) are monitored by one or more administrators using the administrator computing device (206), and are recorded and stored in a data storage system within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown).

[0056] In one or more embodiments of the invention, the identity of the visitor or outsider targeted by the inmate or attempting to contact the inmate using the inmate computing device (212) is verified against inmate target restrictions imposed on the inmate. Such restrictions may be associated with the inmate's identity data item and may be stored locally within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown). The visitor or outsider identity may be verified by the local server (214) or by another server within the outside facility (not shown), or within a third party provider (not shown).

[0057] In one or more embodiments of the invention, the inmate computing system (212) and/or the inmate application (220) may limit access to the communications network (216) based on one or more restrictions (inmate use restrictions, inmate target restrictions, and device use restrictions). Further, the inmate computing system (212) and/or the inmate application (220) may gather data from input devices of the inmate computing system (212) to determine whether one or more restrictions apply. Such input devices may include, for example, a system clock, a global positioning system antenna, a wide area network antenna, etc.

[0058] In one or more embodiments of the invention, the local server (214) is a computer system or group of computers systems located within the controlled facility (200) that facility communication between inmates and visitors, outsiders, and/or other inmates. Specifically, the local server (214) may implement the software necessary to host voice and video calls between and among the visitor kiosk (202), the inmate kiosk (208), the inmate phone (210), and an outsider computing system (not shown). The local server (214) may also include functionality to enforce communication restrictions associated with the inmates using the inmate kiosk (208) or inmate phone (210). Alternatively, the local server (214) may merely provide access to other systems capable of hosting the communication software and data storage (e.g., located within an offsite facility or a third party provider). Further, in one or more embodiments of the invention, the local server (214) includes functionality to regulate inmate access to a secure social network.

[0059] FIG. 3 shows an outside facility in accordance with one or more embodiments of the invention. As shown in FIG. 3, the outside facility (300) may include an application server (302), a database server (304), a reviewer computing system (306), and an investigator computing system (308). The application server (302) is communicatively coupled to the communications network (310). The reviewer computing device (306) may include a reviewer application (312), and the investigator computing device (308) may include an investigator application (314).

[0060] In one or more embodiments of the invention, the application server (302) is a computing system or group of computing systems configured to authenticate inmates, visitors, outsiders, administrators, reviewers, and/or investigators. Specifically, the application server (302) includes functionality to receive a request to authenticate an inmate, visitor, outsider, administrator, reviewer, and/or an investigator, retrieve verified data associated with the request, and compare the verified data to verification data submitted in the authentication request. In one or more embodiments of the invention, the application server provides access to identity data items and other data stored in the database server (304).

[0061] In one or more embodiments of the invention, the database server (304) is a computing system or group of computing systems configured to store data about inmates, visitors, outsiders, administrators, reviewers, and/or investigators as well as communication data describing communications between and among inmates, visitors, outsiders, administrators, reviewers, and/or investigators. Data stored in the database server may include, but is not limited to, identity data items, verified data, approved communication media, communication media pending review

[0062] In one or more embodiments of the invention, the reviewer computing device (306) is a computing system configured to execute the reviewer application (312). In one or

more embodiments of the invention, a reviewer is a person charged with viewing a media item submitted by an inmate, visitor, outsider or administrator, and determining one or more attributes of the media item. Based on the determined attributes of the media item, the reviewer may then approve the media item for transmission to its target inmate, visitor, or outsider. Alternatively, the reviewer may reject the media item, conditionally approve the media item, or redact parts of the media item, thus preventing complete transmission to its target inmate, visitor, or outsider. In one or more embodiments of the invention, the reviewer application (312) include functionality to view media items, associate one or more attributes to the media item, and/or mark the media items as approved or rejected.

[0063] In one or more embodiments of the invention, the investigator computing device (308) is a computing system configured to execute the investigator application (314). In one or more embodiments of the invention, an investigator is a person gathering information about an inmate, visitor, or outsider generally for the purposes of law enforcement. The investigator application (314) includes functionality to provide access to data stored on the database server (304) for investigative purposes.

[0064] FIG. 4 shows a general computing system in accordance with one or more embodiments of the invention. As shown in FIG. 4, the computing system (400) may include one or more computer processor(s) (402), associated memory (404) (e.g., random access memory (RAM), cache memory, flash memory, etc.), one or more storage device(s) (406) (e.g., a hard disk, an optical drive such as a compact disk (CD) drive or digital versatile disk (DVD) drive, a flash memory stick, etc.), and numerous other elements and functionalities. The computer processor(s) (402) may be an integrated circuit for processing instructions. For example, the computer processor (s) may be one or more cores, or micro-cores of a processor. The computing system (400) may also include one or more input device(s) (410), such as a touchscreen, keyboard, mouse, microphone, touchpad, electronic pen, camera, or any other type of input device. Further, the computing system (400) may include one or more output device(s) (408), such as a screen (e.g., a liquid crystal display (LCD), a plasma display, touchscreen, cathode ray tube (CRT) monitor, projector, or other display device), a printer, external storage, or any other output device. One or more of the output device(s) may be the same or different from the input device(s). The computing system (400) may be connected to a network (414) (e.g., a local area network (LAN), a wide area network (WAN) such as the Internet, mobile network, or any other type of network) via a network interface connection (not shown). The input and output device(s) may be locally or remotely (e.g., via the network (412)) connected to the computer processor(s) (402), memory (404), and storage device (s) (406). Many different types of computing systems exist, and the aforementioned input and output device(s) may take other forms.

[0065] Software instructions in the form of computer readable program code to perform embodiments of the invention may be stored, in whole or in part, temporarily or permanently, on a non-transitory computer readable medium such as a CD, DVD, storage device, a diskette, a tape, flash memory, physical memory, or any other computer readable storage medium. Specifically, the software instructions may

correspond to computer readable program code that when executed by a processor(s), is configured to perform embodiments of the invention.

[0066] Further, one or more elements of the aforementioned computing system (400) may be located at a remote location and connected to the other elements over a network (414). Further, embodiments of the invention may be implemented on a distributed system having a plurality of nodes, where each portion of the invention may be located on a different node within the distributed system. In one or more embodiments of the invention, the node corresponds to a distinct computing device. Alternatively, the node may correspond to a computer processor with associated physical memory. The node may alternatively correspond to a computer processor or micro-core of a computer processor with shared memory and/or resources.

[0067] FIG. 5A shows a video visitation kiosk in accordance with one or more embodiments of the invention. Specifically, the video visitation kiosk (500) is a type of computing device as described in FIG. 4. As shown in FIG. 5A, the video visitation kiosk (500) includes a camera (502), a display (504), a handset (506), a headset jack (508), and a universal serial bus (USB) port (510).

[0068] FIG. 5B shows the hardware and software elements of a video visitation kiosk in accordance with one or more embodiments of the invention. The hardware and software elements shown in FIG. 5B may be in addition to the elements described in FIG. 4. As shown in FIG. 5B, the video visitation kiosk (500) includes a handset (506), a video camera (502), a touch screen panel (512), a display (504), a computing application (514), an operating system (516), and a network interface controller (518).

[0069] FIG. 6 shows the hardware and software elements of a mobile computing device in accordance with one or more embodiments of the invention. Specifically, the mobile computing device (600) is a type of computing device as described in FIG. 4. The hardware and software elements shown in FIG. 6 may be in addition to the elements described in FIG. 4.

[0070] As shown in FIG. 6, the mobile computing device (600) may include a global positioning system (GPS) antenna (602), a cell antenna (604), a wide area network (WAN) antenna (606), and a personal area network (PAN) antenna (608), each connected to a multi-band radio transceiver (610). The mobile computing device (600) also may include a rear-facing video camera (612), a front-facing video camera (614), a compass (616), an accelerometer (618), a touch screen (620), a display (622), and a microphone (624). The mobile computing device (600) also may include a computing application (626) executing on an operating system (628).

[0071] FIG. 7 shows a schematic diagram of a system including a network application (700) and a database server (702). The network application (700) may execute or be a part of application server (118) in FIG. 1. Similarly, the database server may be database server (120) in FIG. 1. Alternative configurations may also be used. For example, either, both, or part of the network application (700) and database server (702) may be located in the controlled facility. The network application (700) and database server (702) are discussed below.

[0072] A network application (700) is a software application for connecting inmates and administrators to a network. For example, the network may be a telephone network (not shown) or a secure social network (not shown). The network application (700) may include an authentication module

(704), a controlled setup module (706), a text and speech converter (708), an audit module (710), and a communication module (712). Each of these components is discussed below.

[0073] An authentication module (704) includes functionality to authenticate individuals to the desired network. For example, the authentication module may include functionality to receive authentication credentials, and determine whether the authentication credentials match stored credentials for the individual. The authentication credentials may be user name, password, voiceprint authentication, face verification information, identifying body marks and features information, retina verification information, palm or fingerprint verification information, or any other type of credential for authentication.

[0074] In one or more embodiments of the invention, the controlled setup module (706) includes functionality to create an account (e.g., inmate account (718), superfriend account (714) for an individual. The controlled setup module (706) may further include functionality to populate the account with contacts, and update the account. Populating an inmate account (718) with contacts and updating the inmate account (718) are discussed with reference to FIGS. 8-10.

[0075] Continuing with FIG. 7, in one or more embodiments of the invention, the text and speech converter (708) includes functionality to convert textual input into audio output. The text and speech converter (708) may further include functionality to convert audio input to textual output. Further, the text and speech converter (708) may include functionality to convert one audio input into a second audio input. For example, consider the scenario in which an administrator would like to transmit an anonymous message, such as deliver bad news. In such a scenario, the text and speech converter (708) may include functionality to replace an administrator's voice with a computerized audio. For example, the computerized audio may be a computer voice speaking the administrator's spoken words or manipulation of the sounds of the administrator's voice.

[0076] In one or more embodiments of the invention, the audit module (710) includes functionality to track communications to and from inmates. Specifically, the audit module (710) includes functionality to track, calculate, and store messages, timestamps defining when the message was transmitted, when the message was received, whether the message was transmitted to audio format, the length of time in which the message was being presented, a unique identifier of the communication device (e.g., inmate kiosk, inmate phone, inmate computing device) used to receive the message, any response to the message, and other tracking information about a message.

[0077] The audit module (710) may further include functionality to receive a notification of an investigation of an inmate, search the datacenter server to obtain audit data (734) for the message, and transmit the audit data to an investigator application. For example, the inmate may deny having received a message regarding a court date or assert that the inmate did not read the message. In such an example, the audit module may receive a notification that an investigation is being performed into whether the inmate received the message. Continuing with the example, the audit module may include functionality to search the database server, obtain audit data for the message, and transmit the audit data to the investigator application. Thus, the investigator application may determine when the inmate received the message, how

long the message was being presented, whether the message was presented in audio format, and any other information.

[0078] In one or more embodiments of the invention, the communication module (706) includes functionality to manage a communication on a network. For example, the communication module (706) may include functionality to identify an individual accessing the network, receive a connection request to connect to a contact, and connect the individual to the contact when the contact is in the individual's network list. The term, list, as used in this application refers to any data structure for storing a collection of contacts. The communication module (706) may further include functionality to connect the individual to all social network contacts via the secure social network. In one or more embodiments of the invention, the communication module (706) may facilitate oversight of an inmate's communication by transmitting all or a portion of the messages to an administrator or reviewer for approval.

[0079] The communication module (706) may further include functionality to track the length of time that an inmate is communicating on the selected network and/or a number of messages sent and/or received on the selected network. A payment module (not shown) may include functionality to obtain payment from the inmate or a contact of the inmate and disperse the payment. For example, dispersing the payment may include transmitting at least a portion of the payment to a controlled facility and/or transmitting a portion to a network management entity (e.g., telephone connection company, internet connection company) and/or retaining at least a portion. The payment module may include functionality to debit an inmate's money account or otherwise bill the inmate based on the amount of time, number of messages, or other information.

[0080] Continuing with FIG. 7, the network application (700) is operatively connected to the database server (702). The database server (702) includes functionality to store information for the network application (700). For example, the database server (702) may store one or more superfriend accounts (714), an inmate account (718) for each inmate, precomposed messages (733), audit data (734), saved messages (736), and groups (738). Each of the stored data is discussed below.

[0081] A superfriend account (714) is an account maintained for an administrator or other individual who is a superfriend of an inmate. A superfriend is a person, typically and administrator, contacts and communications from whom an inmate is not permitted to block, reject, or unfriend in accordance with one or more embodiments of the invention. In one or more embodiments, a superfriend is an administrator in the inmate's network list that has authority over the inmate. For example, the superfriend may be a warden, guard, parole officer, counselor, doctor, investigator, or other individual. In some embodiments, a superfriend is an administrator employed by the communications system's developer/operator. For example, the superfriend may be a helpdesk support person, a marketing promotions person, or other individual. In one or more embodiments of the invention, a superfriend has superfriend privileges (722) over an inmate account (718) and has removal protection from the inmate account (718). In one or more embodiments of the invention, superfriend privileges may correspond to administrative privileges. In one or more embodiments of the invention, superfriend privileges (722) include being able to transmit any information to an inmate and having the transmission on the conspicuously

placed or presented when the inmate accesses the network. Further, superfriend privileges (722) may include privilege to review all correspondence to and from the inmate. Additional superfriend privileges may exist without departing from the scope of the invention. In one or more embodiments of the invention, an inmate cannot limit the superfriend privileges. In another embodiment, superfriend privileges may be granted to any of the above types of individuals' named accounts. Granting superfriend privileges may be performed in a case in which the type of individual is expected to maintain a personal relationship with an inmate, such as in the case of a doctor or counselor. Such individual may have no overt authority over the inmate, such that protecting said individual's identity is of less concern than, for example, a facility administrator capable of handing down punishment.

[0082] In one or more embodiments of the invention, superfriends are given superfriend privileges on a hierarchical basis according to the power of the domain scope of the individual with the superfriend account. For example, a superfriend of the system operator may be able to send messages to all inmates at all facilities using the service while a state director of a department of corrections (DOC) may be able to send messages to all inmates at any and all facilities in which the state director is responsible, even without the permission of the warden superfriend at each facility. Hierarchies may exist at a geographic level, such as state, then county, then facility, then wing of a facility, with a superfriend at each level of hierarchy being able to send messages to all inmates within that domain.

[0083] In one or more embodiments of the invention, a superfriend may choose to restrict the scope of the messages that the superfriend sends on a non-geographic basis. For example, a doctor may have a domain that includes all patients he has or is treating, or all of those inmates which are permitted to seek treatment from him. Normally, this doctor would send messages to all of his patients. However, he may choose to further restrict the delivery of messages on the basis of other attributes, such as, for example, sending a message to every inmate at his facility with a peanut food allergy, warning them that today's salad contains peanuts. By way of another example, the doctor may send a message to all inmates diagnosed with hepatitis C, informing them of a new medicine or treatment available.

[0084] The superfriend domain privileges or authorized network may be limited by the superfriend or the superfriend's superiors on the basis of gender, age, race, crime, medical condition, physical attributes, geographical locations, events they've done, inappropriate comments made in the social network, or any other foreseeable attribute or reason.

[0085] In one or more embodiments of the invention, superfriends may delegate their privileges to a subordinate. In the above example, the doctor may give his nurse the job of sending such messages, and grant this nurse superfriend privileges sufficient to carry out his instructions. In one or more embodiments of the invention, the delegated privileges do not exceed the superfriend's privileges.

[0086] In one or more embodiments of the invention, superfriends may choose to limit the scope of the superfriends authority for specified or all messages sent, but may not expand the scope of their authority outside of the superfriend's permitted domain.

[0087] In one or more embodiments of the invention, superfriends may have unilateral power to block inmates, without blocking the superfriend's ability to send message to blocked

inmates. For example, if a particular inmate sends abusive or threatening messages to a particular superfriend, the superfriend may block that inmate from sending any messages to that superfriend's account, yet that superfriend will still be able to send messages to that inmate.

[0088] In addition to receiving audit data defining which inmates have read the superfriend's messages, the superfriend may choose to embed a test of sorts within each message, to determine if the inmate actually read and comprehended the message, or merely allowed it to be displayed. Such test may take the form of a survey, for example.

[0089] Removal protection refers to an inability for an inmate to unfriend the superfriend. Specifically, without proper authority, which an inmate does not have, the superfriend cannot be disassociated from the inmate's network.

[0090] In one or more embodiments of the invention, the superfriend account (714) further includes an authorized network (719), superfriend authentication credentials (724), and at least one superfriend public alias.

[0091] The authorized network (719) includes a list of inmates with whom a superfriend has permission to have in the superfriend network list (720). In one or more embodiments of the invention, the authorized network (719) may be defined by a collection of is based on inmate attributes of the inmates. An inmate attribute is an attribute about the inmate with respect to being in the controlled facility. For example, the inmate attribute may be a controlled facility identifier, a reason for being in the controlled facility (e.g., crime the inmate committed, class of crimes that the inmate committed, drugs to which the inmate is addicted, and other reasons), history of the inmate in controlled facility, gang relations of the inmate, health issues of the inmate that need to be managed by the controlled facility, and/or other attributes of the inmate. By way of an example, the authorized network (719) may include all inmates in the controlled facility, all inmates in a collection of the controlled facility, inmates with particular health considerations, inmates who are in counseling, or based on other inmate attributes. In one or more embodiments of the invention, in addition to inmates, the authorized network may further include administrators.

[0092] The authorized network (719) includes a superfriend network list (720) in one or more embodiments of the invention. In one or more embodiments of the invention, the superfriend network list (720) may be a subset or the entire set of the authorized network (719). The superfriend network list (720) includes a list of contacts with whom the superfriend may communicate. Specifically, the superfriend network list (720) may be a collection of contacts with whom the superfriend is connected. A contact refers to an individual or group of individuals with whom a person is connected. For example, the contact may include a network identifier of an individual and connection information for connecting to the individual. In the case of a superfriend, the contact may include inmates and, optionally, administrators.

[0093] In one or more embodiments of the invention, superfriend authentication credentials (724) are authentication credentials used for authenticating the administrator. The superfriend authentication credentials (724) may include user name, password, voiceprint authentication, face verification information, identifying body marks and features information, retina verification information, palm or fingerprint verification information, or any other type of credential for authentication.

[0094] In one or more embodiments of the invention, a superfriend public alias (726) is an alternative identifier for the administrator that is presented as the sender and/or recipient of messages. For example, if the administrator is transmitting a message anonymously, the anonymous communication may be under the public alias. By way of another example, if the administrator is performing a communication for a particular group (e.g., the entire controlled facility, a group of prisons, a counseling group), the administrator may use the public alias of a group name to send and receive messages.

[0095] Continuing with the database server (702), an inmate account is an account storing information about an inmate. For example, an inmate account may include inmate authentication credentials (728), an inmate telephone network list (730), and an inmate social network list (732). Additionally, although not shown in FIG. 7, the inmate account may also include administrative information, such as name, birthdate, inmate identifier, reason for the inmate to be in the controlled facility, historical confinement of the inmate, list of inmate's violations of regulations of the controlled facility, gang affiliations, account balance for payment of communications, and other information.

[0096] The inmate authentication credentials (728) correspond to authentication credentials for the inmate. For example, the authentication credentials may include user name, password, voiceprint authentication, face verification information, identifying body marks and features information, retina verification information, palm or fingerprint verification information, or any other type of credential for authentication.

[0097] The inmate telephone network list (730) corresponds to a list of contacts of the inmate for communication via the telephone network. The inmate secure social network list (732) corresponds to a list of contacts of the inmate for communication via a secure social network. In one or more embodiments of the invention, before being allowed to communicate with the contacts, the contacts must be approved. Further, although an inmate may communicate with contacts in the inmate telephone network list and the inmate secure social network list, the contacts may not be approved in accordance with one or more embodiments of the invention. Specifically, the inmate telephone network list and the inmate secure social network list may include unprocessed contacts, filtered contacts, and/or approved contacts.

[0098] An unprocessed contact is a contact that has not been vetted or checked to determine whether communication with the unprocessed contact is prohibited. A filtered contact is a contact that is not outright prohibited for communication. An approved contact is a contact that has been vetted and with whom the inmate may communicate. For example, unprocessed contacts may be filtered to remove contacts that are known gang members, are inmates, are wanted criminals, or have other attributes, which make communication with such contacts outright prohibited. In one or more embodiments of the invention, the filtering process may include comparing the contact with lists of prohibited people. In some embodiments, the remaining contacts after the filtering processed are approved contacts. In alternative embodiments, filtered contacts may have to be vetted (e.g., go through an identification and/or approval process) to be approved contacts. The vetting may include performing background checks on the contact and confirming the identity of the contact. In one or more embodiments of the invention, rules of the controlled facility

define whether filtered contacts must be vetted in order for the inmate to communicate with the approved contacts. Whether a contact is an unprocessed contact, filtered contact, or approved contact may be maintained as an attribute defined for the contact in the inmate account.

[0099] Although FIG. 7 shows the secure social network list (732) as separate and distinct from the telephone network list (730), the secure social network list (732) may be the same as the telephone network list (730). Further, in one or more embodiments of the invention, the inmate may have a single contact list. Each contact in the single contact list may have a parameter indicating whether the inmate may communicate with the contact via telephone network, secure social network, or both. For example, the parameter may be a set bit and/or connection identifiers (e.g., telephone number, secure social network identifier) for the contact.

[0100] Continuing with the discussion regarding the database server (702), the precomposed messages (733) correspond to a set of predefined messages from which a sender may select. For example, precomposed messages may be a message about which schedule the inmate is on for the week, the status of an inmate's debit account, notification of violation of a rule or regulation, or other standard message that may be sent to an inmate.

[0101] In one or more embodiments of the invention, audit data (734) includes information stored for auditing purposes. For example, for each message, the audit data may include timestamps defining when the message was transmitted, whether the message was transmitted in audio format, when the message was received, the length of time in which the message was being presented, a unique identifier of the communication device used to receive the message, any response to the message, and other tracking information about a message.

[0102] Saved messages (736) correspond to messages that are saved. For example, saved messages may include postings to the inmate secure social network, voicemail messages, one to one messages, multicast or broadcast messages, and other messages.

[0103] In one or more embodiments of the invention, groups (738) relate a group identifier to account identifiers of individuals who are members of the group. For example, for a counseling group, the counseling group identifier is related to the counselor superfriend account identifier along with inmates who participate in the counseling session. By way of another example, for a controlled facility group, the controlled facility group identifier may be related to all inmates in the controlled facility. Thus, a communication sent to a group identifier will be broadcasted to all members of the group in one or more embodiments of the invention.

[0104] Although FIG. 7 shows a certain configuration of components, other configurations may be used without departing from the scope of the invention. For example, the superfriend account (714) may be located on an application. By way of another example, one or more modules of the network application (700) may be located in a different component of the system.

[0105] FIGS. 8-10 show flowcharts in one or more embodiments of the invention. While the various steps in these flowcharts are presented and described sequentially, some or all of the steps may be executed in different orders, may be combined or omitted, and some or all of the steps may be executed in parallel. Furthermore, the steps may be performed actively or passively. For example, some steps may be performed

using polling or be interrupt driven in accordance with one or more embodiments of the invention. By way of an example, determination steps may not require a processor to process an instruction unless an interrupt is received to signify that condition exists in accordance with one or more embodiments of the invention. As another example, determination steps may be performed by performing a test, such as checking a data value to test whether the value is consistent with the tested condition in accordance with one or more embodiments of the invention.

[0106] FIG. 8 shows a flowchart for initializing a superfriend account in one or more embodiments of the invention. In Step 801, a request for a new superfriend account for an administrator is received in one or more embodiments of the invention. For example, the administrator may be a new administrator to the controlled facility.

[0107] In Step 803, administrative data, authorized network, and privileges for the administrator are obtained in accordance with one or more embodiments of the invention. Specifically, the administrator, an information technology specialist, and/or other individual may submit the administrator's name, employee identifier, address, phone number, birth date, and other such data to the setup module of the network application. Further, the administrator, an information technology specialist, and/or other individual may submit information defining the administrator's authorized network. The administrator's authorized network may be defined based on the role of the administrator with respect to the controlled facility. For example, a warden may have an authorized network of the entire facility while a physician in the controlled facility may only have an authorized network over all inmates diagnosed with a mental illness. In one or more embodiments of the invention, privileges may be set based on the needs of the administrator in the controlled facility.

[0108] In Step 805, authentication credentials and a public alias are received for the administrator in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, the administrator submits the authentication credentials and select a public alias. The selected public alias may be defined based on the employment position of the administrator. For example, a doctor may have an alias of Clinic. A food service manager known as Bob to the inmates may have an alias of Chef Bob. Further, if the administrator is responsible for transmitting bad news occasionally, the administrator may have an alias that does not have anything to do with the administrator specifically. For example, the administrator may have the alias of Controlled Facility.

[0109] In Step 807, administrative data, authorized network, privileges, authentication credentials, and public alias are stored in a new superfriend account in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, the new superfriend account is created and the data received is stored.

[0110] In Step 809, a connection request is received to connect to a contact in accordance with one or more embodiments of the invention. The connection request may be received when creating the superfriend account, when creating an inmate account, and/or on an as desired basis. For example, the administrator, an information technology specialist, and/or other individual may initially select contacts to add based on an employment position of the administrator. By way of a more concrete example, if the administrator is a

doctor of the controlled facility, all inmates that have medical issues may be added to the administrator network list. Further, in one or more embodiments of the invention, when a new inmate is confined in the controlled facility, a connection request may be received to add the new inmate. In one or more embodiments of the invention, the inmates have no control over which administrators are connected to them. Specifically, an inmate does not have any authority to accept or reject a connection with a superfriend or remove a superfriend.

[0111] In Step 811, a determination is made whether the contact is in the authorized network in accordance with one or more embodiments of the invention. Specifically, a determination is made whether the contact is approved. If the contact is not in the authorized network, the administrator is notified of the unauthorized contact in Step 813 in accordance with one or more embodiments of the invention. Specifically, the administrator is notified that the administrator cannot connect to the unauthorized contact. Notification that the administrator is attempting to connect to an unapproved contact may be sent to a supervisor of the administrator for evaluation. The supervisor may allow or deny of the connection. Further, denial information may be stored to track the contacts to whom the administrator is attempting to connect. The denial information may be used for investigative purposes to investigate whether the administrator is performing or attempting to perform improper communication with inmates.

[0112] In Step 815, if the contact is part of the authorized network, the contact is added to the superfriend network in accordance with one or more embodiments of the invention. Specifically, the contact is added to the superfriend network list. In one or more embodiments of the invention, once added, the administrator may send messages to the contact.

[0113] Although not shown in FIG. 8, rather than performing Steps 809-815, all contacts in the superfriend's authorized network may be automatically added to the superfriend network list. In such a scenario, one or more of Steps 809-815 may be omitted without departing from the scope of the invention.

[0114] FIG. 9 shows a flowchart for a superfriend to send a message to one or more contacts in accordance with one or more embodiments of the invention. In Step 901, a new message request is received from the superfriend in one or more embodiments of the invention. The new message request may be received via a computer interface or via a telephone interface. Prior to or as a part of receiving the new message request, the administrator may authenticate him or herself to the network application. The authentication attempt and whether the authentication was successful may be stored for tracking purposes. Further, the administrator may select to compose a new message.

[0115] In Step 903, a selection of one or more contacts in the superfriend network is received. For example, the superfriend may request to send the message to all contacts, a particular group of contacts, to a subset of contacts, etc. In one or more embodiments of the invention, the superfriend may select the subset using inmate attributes.

[0116] In Step 905, the mode of the message is received in accordance with one or more embodiments of the invention. In one or more embodiments, the administrator selects the mode by which the contacts will receive the message. The administrator may select the mode on a per contact basis. For example, if the administrator knows that a particular inmate cannot read, the administrator may select that the particular inmate receive the message in audio format (e.g., via tele-

phone or played on the inmate kiosk or computing device) while the remaining inmates receive a textual format of the message.

[0117] In Step 907, a determination may be made whether to use a precomposed message in accordance with one or more embodiments of the invention. For example, the communication module of the network application may present an option to use a precomposed message. For example, the superfriend may decide to use the precomposed message when the message is a standard message or when the superfriend would like to be completely anonymous when transmitting the message.

[0118] If a determination is made to use a precomposed message, then a selection of the precomposed message is received in Step 909. For example, the communication module may present the administrator with a series of optional precomposed messages. The presentation may be via a graphical user interface of an administrator computer system or kiosk or via an auditory list accessed via telephone. From the list of options, the administrator may select the desired precomposed message.

[0119] In Step 911, the precomposed message is transmitted to selected contacts in accordance with one or more embodiments of the invention. The precomposed message is transmitted in accordance with the selected mode for sending to each contact. For example, for contacts that are to receive messages via inmate telephone, precomposed message is added to the contacts inbox. Further, the contacts are notified that a new message exists. For example, a guard may notify an inmate that the inmate has a new message. Alternatively, the inmate may periodically check for new messages. By way of another example, for contacts that receive messages via the inmate kiosk or inmate computing device, when an inmate authenticates him or herself to the inmate computing device, the inmate may be notified of the new message. Although not shown in FIG. 9, a precomposed message may be sent anonymously by using an anonymous public alias of the superfriend.

[0120] Returning to Step 907 of FIG. 9, if a determination is made not to use the precomposed message, then a new message is received from the superfriend in Step 913 in accordance with one or more embodiments of the invention. For example, the superfriend may dictate the message for speech to text conversion, the superfriend may speak the message, the superfriend may type the message, or perform any other action for transmitting the new message.

[0121] In Step 915, a determination is made whether to send the message anonymously. For example, the superfriend may select an option to send message as anonymous. The superfriend may select such an option in order to avoid bodily retribution from the inmates.

[0122] If a determination is made to send the message anonymously, then in Step 917, an anonymous message is generated from the received new message in accordance with one or more embodiments of the invention. Various techniques may be used to generate the anonymous message. For example, generating the anonymous message may include performing a first conversion of the superfriend's voice auditory message to a text message and then performing a second conversion of the text message to an auditory format read by a generic computer voice. By way of another example, direct voice alteration of the superfriend's voice in an auditory message may be performed. Additionally or alternatively, an

alias of the superfriend may be used as the sender of the message to transform the message to an anonymous message.

[0123] In Step 919, the message is transmitted to selected contacts. Transmitting the message may be performed similar to transmitting the precomposed message.

[0124] FIG. 10 shows a flowchart for an inmate to receive a message in accordance with one or more embodiments of the invention. In Step 1001, a message to an inmate is received from a superfriend. For example, the inmate's inbox may receive a new message. Although not shown in FIG. 1, the inmate may authenticate him or herself to the telephone network, the inmate kiosk, or the inmate computing device. The authentication assures that any messages from superfriends are actually being received by the inmate.

[0125] In Step 1003, the message is positioned based on priority and the superfriend in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, for any message from a superfriend, the message is conspicuously placed. For example, if the inmate is accessing the message via an inmate telephone, then any message from one or more superfriends are played prior to any message from any other contact. Further, the inmate may be prohibited from making a telephone call until after such messages are played to the inmate. By way of another example, if the inmate is accessing the message via an inmate kiosk or inmate computer system, any messages from superfriends are conspicuously placed. In the example, the message(s) may be placed on a separate window that is displayed prior to any window displaying other messages from non-superfriends. Alternatively or additionally, the messages may be placed in the same window as other messages, but prior to other messages. Further, the inmate may be prohibited from sending messages or viewing other messages until after all and entire messages from superfriends are presented to the inmate.

[0126] In one or more embodiments of the invention, messages from superfriends may be ordered according to priority. For example, messages that relate to an inmate's court date may be set and displayed prior to a message that corresponds to an inmate survey. By way of another example, messages involving a violation of a rule or regulation of the controlled facility may be placed at a higher priority than a message from a guidance counselor.

[0127] In Step 1005, receipt of the message is detected in one or more embodiments of the invention. Specifically, when the message is presented, the system detects that the inmate has received the message.

[0128] In one or more embodiments of the invention, the inmate may control the mode in which the message is transmitted. For example, for textual messages, the inmate may select to have an audio version of the message played for the message. For audio messages, the inmate may select to have a textual version of the message displayed for the inmate. The speech and text converter may perform the desired conversion in accordance with one or more embodiments of the invention.

[0129] In Step 1007, audit information is obtained and calculated based on the receipt of the message. In one or more embodiments of the invention, obtaining and calculating the audit information may include obtaining a starting timestamp indicating when the presentation of the message started, obtaining an ending timestamp indicating when presentation of the message ended, and calculating a difference to obtain a length of time in which the message was presented. Addition-

ally, a unique identifier of the device (e.g., inmate computing device, inmate kiosk, inmate telephone) used to receive the message may be obtained. Additional audit information may include information about the superfriend sending the message, and the mode (e.g., audio, textual) used to present the message.

[0130] In Step 1009, the audit information is stored in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, the audit information may be stored in a secured datacenter system. The message, as well as any other message or response transmitted to and from the inmate, may be stored with the audit information. Multiple copies of the audit information may be stored on different physical devices to ensure the audit information is maintained.

[0131] By maintaining audit information and messages, embodiments provide a mechanism for tracking messages for investigative purposes. For example, if an inmate denies having received a message, such as a court date, the datacenter may be accessed to obtain audit information corresponding to the message of the court date. Specifically, a query may be performed on the datacenter to search and recover all messages to the inmate regarding a court date. The corresponding audit information for each message returned in the query may be obtained. The corresponding audit information and the message may be transmitted to an investigator to prove that the inmate did receive the message or did not receive the message.

[0132] By way of another example, the use of the audit information and message may be used to show that the inmate is in the process of committing perjury to the court or committing a crime while in the controlled facility. For example, the messages to and from inmates may be periodically reviewed and analyzed to determine whether the message includes information about a crime or inconsistent statements made in court. If a message is found, the message may be sent to an investigator with audit information proving that the inmate did in fact receive or transmit the message.

[0133] In Step 1011, the audit information is transmitted to the superfriend in accordance with one or more embodiments of the invention. By transmitting the audit information to the superfriend, the superfriend is assured that the message was received.

[0134] In Step 1013, a determination is made whether to send a response. For example, the inmate may desire to send a response message to the superfriend. If a determination is made to send the response, the response from the inmate may be received in Step 1015. For example, the response may be received via the same device used to present the message. The received response may be parsed and analyzed for vulgar or aggressive words. If vulgar or aggressive words are used, the response may be sent to a reviewer. In Step 1017, the response is sent to the superfriend in accordance with one or more embodiments of the invention. Sending the response to the superfriend may be performed in a same or similar manner to transmitting the message to the inmate.

[0135] The following example is for explanatory purposes only and not intended to limit the scope of the invention. FIG. 11 shows an example user interface (1100) for a superfriend to transmit precomposed messages to one or more inmates. As shown in FIG. 11, a superfriend may indicate in box (1102), the reason for the message. The reason may be used for auditing purposes, as a subject line, to define priority, for another reason, or combination thereof. Further, the super-

friend may select from a set of precomposed messages (1104). For example, if the inmate is having difficulty using the inmate telephone, the precomposed message (1104) may be that fine must be paid or that a request to transfer funds must be made in order to allow use of the phone. As shown in the example, the precomposed message (1104) may be transmitted to an inmate's voicemail inbox. Thus, the inmate may receive a notice from a guard that he or she has a new message and check his or her voicemail via the inmate telephone to receive the new message.

[0136] By way of another example, a warden of the controlled facility may authenticate himself using a "Warden" superfriend account that may allow him to communicate with and access the wall posts of anyone in his facility. The warden may post a message to each pod (i.e., separate collection of inmates) announcing that pod's meal schedules for the week and what will be served for the detainees in that pod, along with a survey that will be used to help determine foods that will be served the following week. Next, the warden may send a message to all inmates who are HIV positive, notifying them that medication distribution has been delayed by fifteen minutes. Further, the warden may respond to an inmate who has asked him a specific question. Last, the warden may send a pre-recorded welcome and rules video to all inmates booked within the last twenty-four hours. In the example, audit information for each of the messages may be stored. Thus, inmates who are HIV positive cannot deny that they have received the message. Further, in one or more embodiments of the invention, as a superfriend the warden's messages are conspicuously presented to the inmates. Priority amongst the messages may be set, such that the survey is given lowest priority and the HIV message is given the highest priority.

[0137] While the invention has been described with respect to a limited number of embodiments, those skilled in the art, having benefit of this disclosure, will appreciate that other embodiments can be devised which do not depart from the scope of the invention as disclosed herein. Accordingly, the scope of the invention should be limited only by the attached claims.

What is claimed is:

1. A method for message transmission in a controlled facility, comprising:
 - receiving a request to transmit a message from a superfriend in a controlled facility, wherein the superfriend has an administrative privilege and a removal protection;
 - receiving, for the message from a superfriend network list of the superfriend, a selection of a plurality of contacts confined in the controlled facility;
 - sending, via an electronic network, the message to each of the plurality of contacts in the controlled facility;
 - presenting the message to each of the plurality of contacts in the controlled facility; and
 - for each contact of the plurality of contacts:
 - calculating audit information capturing the presenting of the message; and
 - transmitting an acknowledgement of receipt of the message to the superfriend.
2. The method of claim 1, further comprising:
 - receiving a notice of an investigation of an inmate of the controlled facility; and
 - transmitting the audit information captured for the inmate to an investigator for the investigation of the inmate.
3. The method of claim 1, wherein receiving the request to transmit the message is anonymous and comprises:

generating an anonymous message from a new message, wherein the anonymous message is sent to each of the plurality of contacts.

4. The method of claim 3, wherein generating the anonymous message comprises:
 - performing a speech to text conversion on the new message to obtain a textual message; and
 - performing a text to speech conversion on the textual message to obtain a computer voice message, wherein the computer voice message is an anonymous message.
5. The method of claim 3, wherein generating the anonymous message comprises:
 - obtain a public alias of the superfriend; and
 - sending the message using the public alias of the superfriend.
6. The method of claim 1, wherein the selection of the plurality of contacts is received by presenting the superfriend with a plurality of groups and receiving a selection of a group from the plurality of groups, wherein the group comprises the plurality of contacts.
7. The method of claim 1, further comprising:
 - generating the plurality of groups based on inmate attributes of a plurality of inmates.
8. A system for message transmission in a controlled facility, comprising:
 - a computer processor;
 - a database server comprising a superfriend account for a superfriend, wherein the superfriend account stores a superfriend network list, wherein the superfriend comprises an administrative privilege and a removal protection; and
 - a network application executing on the computer processor and comprising:
 - a communication module configured to:
 - receive a request to transmit a message from the superfriend in a controlled facility,
 - receive, for the message from the superfriend network list of the superfriend, a selection of a plurality of contacts confined in the controlled facility,
 - send, via an electronic network, the message to each of the plurality of contacts in the controlled facility, and
 - present the message to each of the plurality of contacts in the controlled facility, and
 - an audit module configured to:
 - for each contact of the plurality of contacts:
 - calculate audit information capturing the presenting of the message; and
 - transmit an acknowledgement of receipt of the message to the superfriend.
9. The system of claim 8,
 - wherein the audit module is further configured to:
 - receive a notice of an investigation of an inmate of the controlled facility, and
 - transmit the audit information to an investigator application, and
 - wherein the system further comprises an investigator application configured to present the audit information captured for the inmate to an investigator for the investigation of the inmate.
10. The system of claim 8,
 - wherein receiving the request to transmit the message is anonymous and comprises generating an anonymous message from a new message, and

wherein the anonymous message is sent to each of the plurality of contacts.

11. The system of claim **10**, wherein the network application further comprises a text and speech converter configured to:
perform a speech to text conversion on the new message to obtain a textual message, and
perform a text to speech conversion on the textual message to obtain a computer voice message, wherein the computer voice message is an anonymous message, and

wherein generating the anonymous message comprises sending the message to the text to speech converter.

12. The system of claim **10**, wherein the superfriend account further stores a public alias of the superfriend, and wherein generating the anonymous message comprises:

obtain the public alias of the superfriend from the superfriend account; and
sending the message using the public alias of the superfriend.

13. The system of claim **10**, wherein the database server comprises a plurality of groups generated based on inmate attributes of a plurality of inmates, and wherein selection of the plurality of contacts is received by presenting the superfriend with the plurality of groups and receiving a selection of a group from the plurality of groups, wherein the group comprises the plurality of contacts.

14. A non-transitory computer readable medium for message transmission in a controlled facility, the non-transitory computer readable medium comprising computer readable program code for:

receiving a request to transmit a message from a superfriend in a controlled facility, wherein the superfriend comprises an administrative privilege and a removal protection;
receiving, for the message from a superfriend network list of the superfriend, a selection of a plurality of contacts confined in the controlled facility;
sending, via an electronic network, the message to each of the plurality of contacts in the controlled facility;
presenting the message to each of the plurality of contacts in the controlled facility; and

for each contact of the plurality of contacts:
calculating audit information capturing the presenting of the message; and
transmitting an acknowledgement of receipt of the message to the superfriend.

15. The non-transitory computer readable medium of claim **14**, further comprising computer readable program code for: receiving a notice of an investigation of an inmate of the controlled facility; and
transmitting the audit information captured for the inmate to an investigator for the investigation of the inmate.

16. The non-transitory computer readable medium of claim **14**, wherein receiving the request to transmit the message is anonymous and comprises generating an anonymous message from a new message, and
wherein the anonymous message is sent to each of the plurality of contacts.

17. The non-transitory computer readable medium of claim **16**, wherein generating the anonymous message comprises: performing a speech to text conversion on the new message to obtain a textual message; and
performing a text to speech conversion on the textual message to obtain a computer voice message, wherein the computer voice message is an anonymous message.

18. The non-transitory computer readable medium of claim **16**, wherein generating the anonymous message comprises: obtain a public alias of the superfriend; and
sending the message using the public alias of the superfriend.

19. The non-transitory computer readable medium of claim **14**, wherein the selection of the plurality of contacts is received by presenting the superfriend with a plurality of groups and receiving a selection of a group from the plurality of groups, wherein the group comprises the plurality of contacts.

20. The non-transitory computer readable medium of claim **14**, further comprising computer readable program code for: generating the plurality of groups based on inmate attributes of a plurality of inmates.

* * * * *



(19) **United States**

(12) **Patent Application Publication**
Bloms et al.

(10) **Pub. No.: US 2014/0218466 A1**

(43) **Pub. Date: Aug. 7, 2014**

(54) **AUDIO-VIDEO REMOTE VISITATION
TELECOMMUNICATIONS TECHNOLOGY**

(52) **U.S. Cl.**
CPC **H04N 7/152** (2013.01); **H04L 65/4038**
(2013.01)

(71) Applicant: **TW Vending, Inc.**, Hudson, WI (US)

USPC **348/14.09**

(72) Inventors: **Eric Bloms**, River Falls, WI (US); **Todd Westby**, Woodbury, MN (US); **Ben Halberg**, River Falls, WI (US); **Sam Bengston**, River Falls, WI (US)

(57) **ABSTRACT**

A telecommunications system for use in a secure facility such as a jail, prison or the like. The systems, devices and methods disclosed provide telecommunications, email, other messaging, financial services, vending, and commissary or canteen services for inmates of a secure facility with respect to family, friends and others. The system also includes a system for video visitation via audio-visual communication. The system includes a phone server adapted to be communicatively connected to an external service provider; a monitoring station communicatively connected to the phone server, an account manager server communicatively connected to the phone server, and at least one telecommunications device disposed at the secure facility for use by the inmate and which is communicatively connected to the phone server. A method of telecommunicating, including video visitation, via the system is also disclosed.

(21) Appl. No.: **14/136,886**

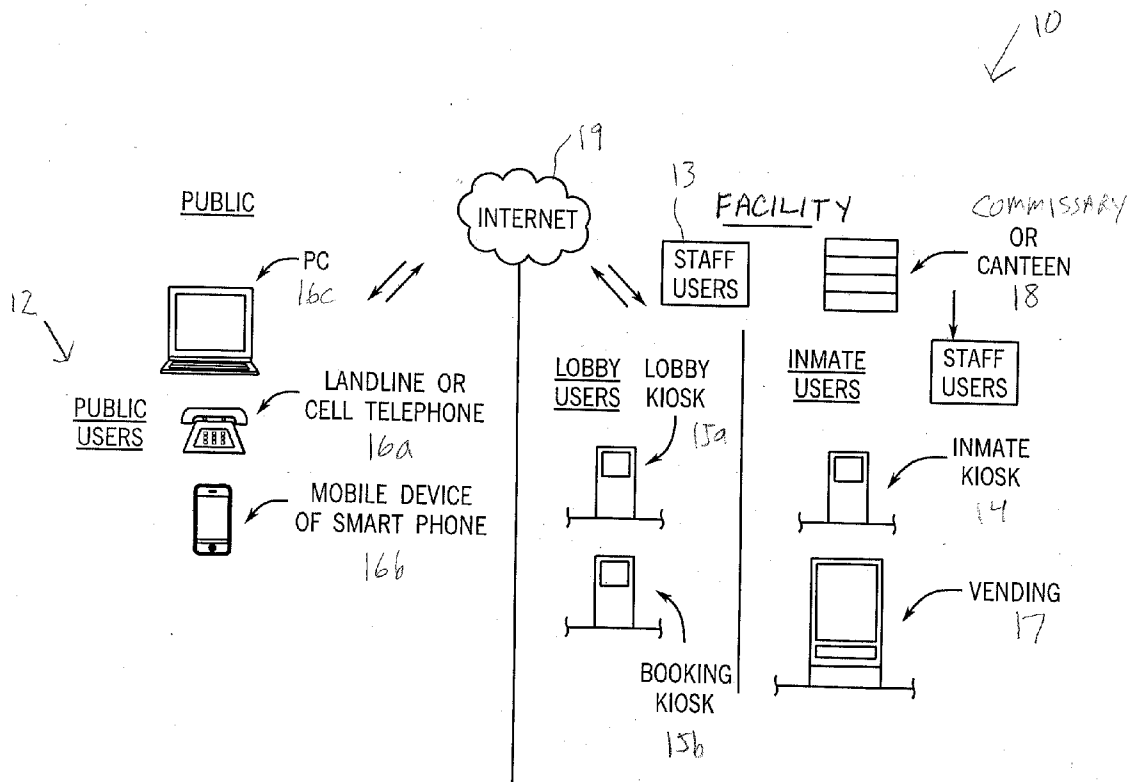
(22) Filed: **Dec. 20, 2013**

Related U.S. Application Data

(60) Provisional application No. 61/848,148, filed on Dec. 21, 2012.

Publication Classification

(51) **Int. Cl.**
H04N 7/15 (2006.01)
H04L 29/06 (2006.01)



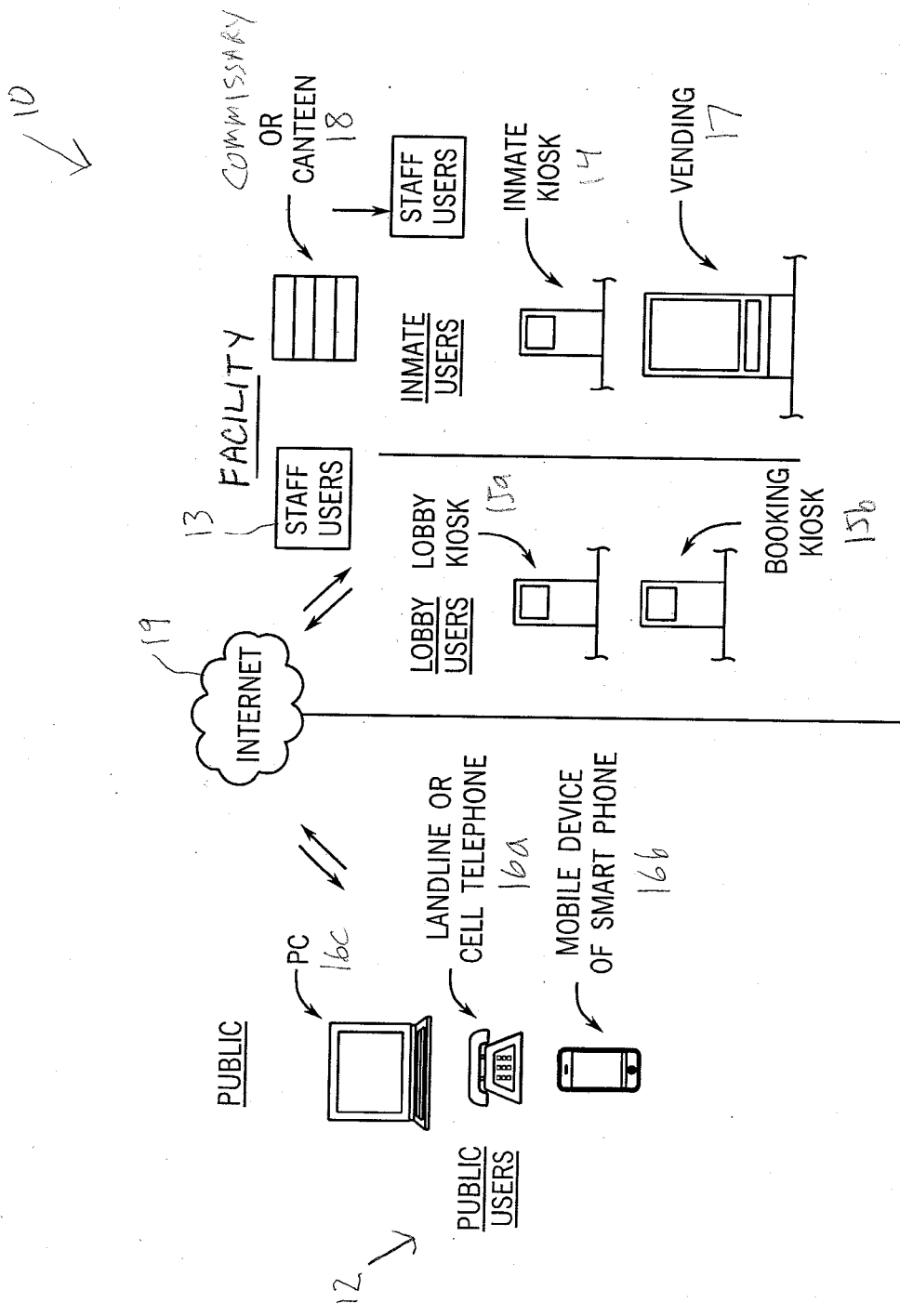


FIG. 1

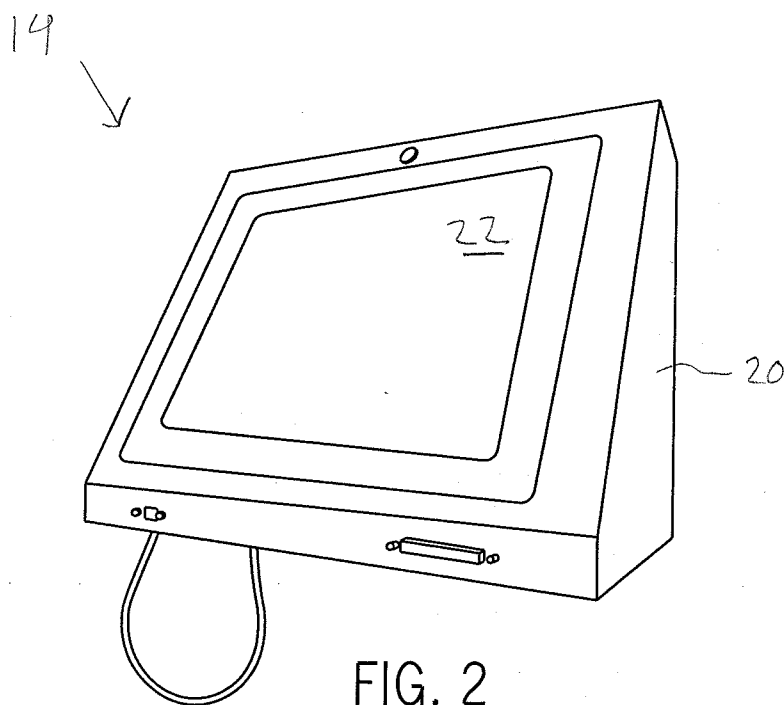


FIG. 2

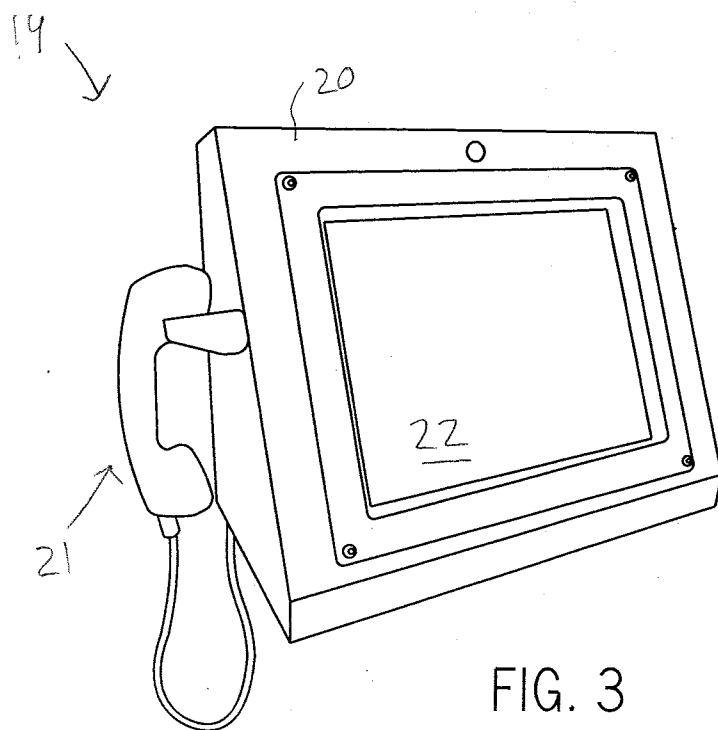


FIG. 3

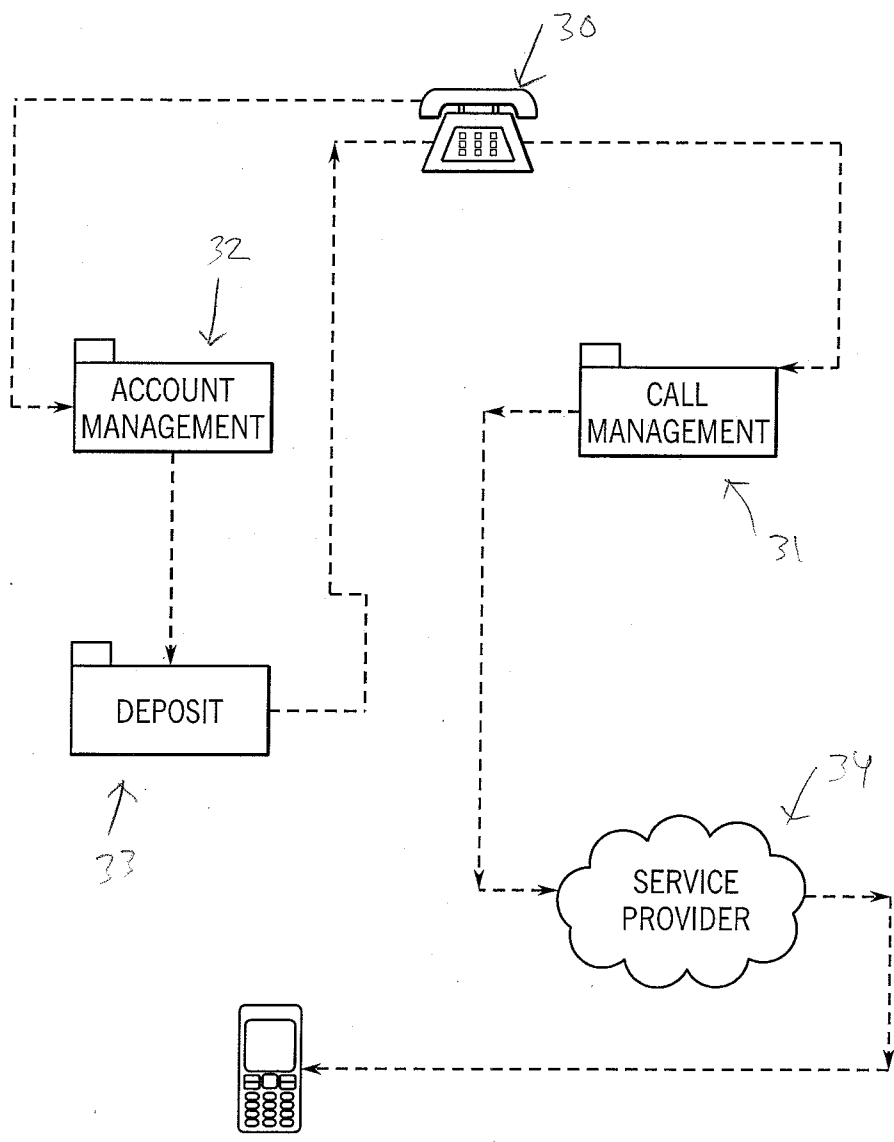


FIG. 4

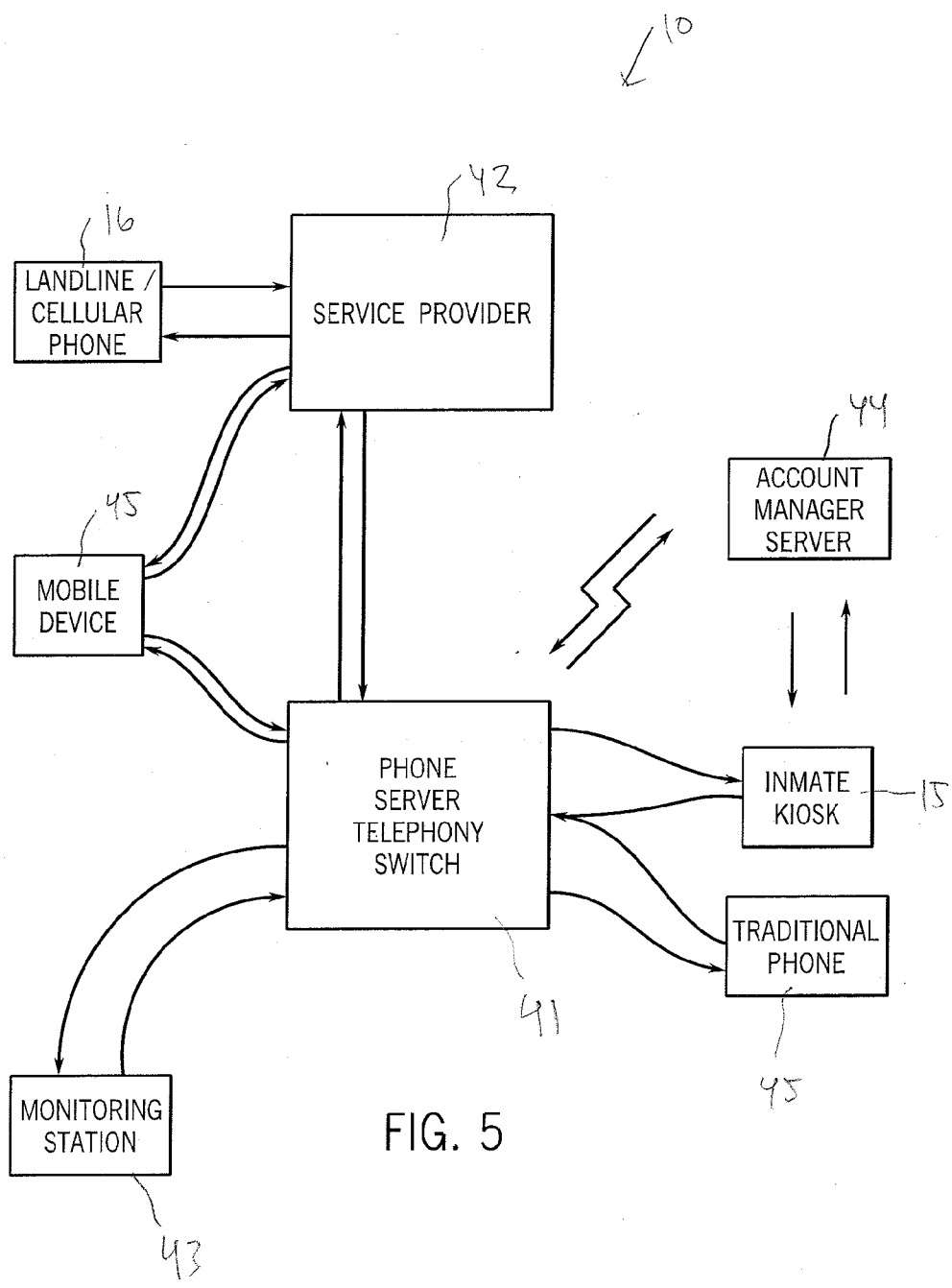


FIG. 5

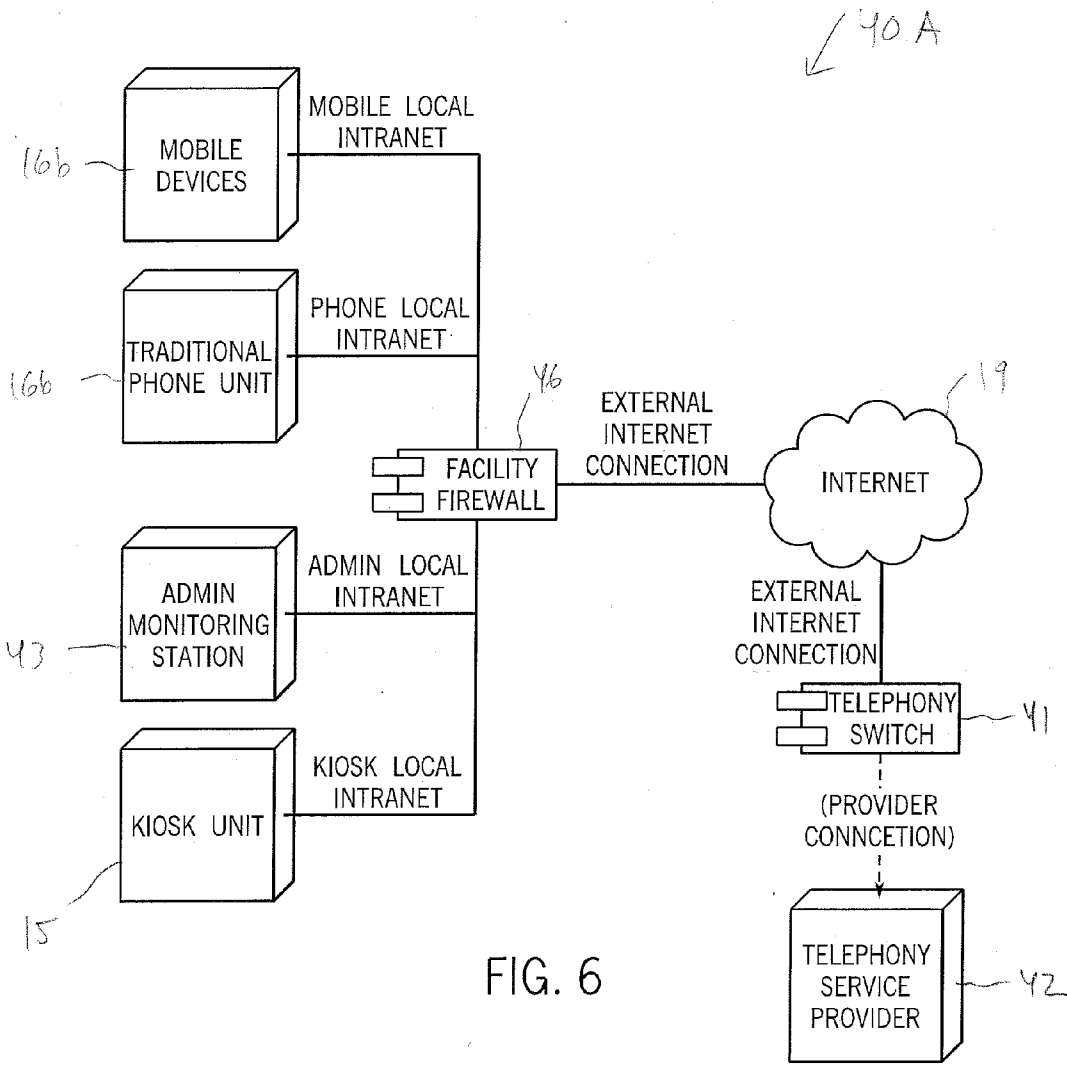


FIG. 6

40B
↓

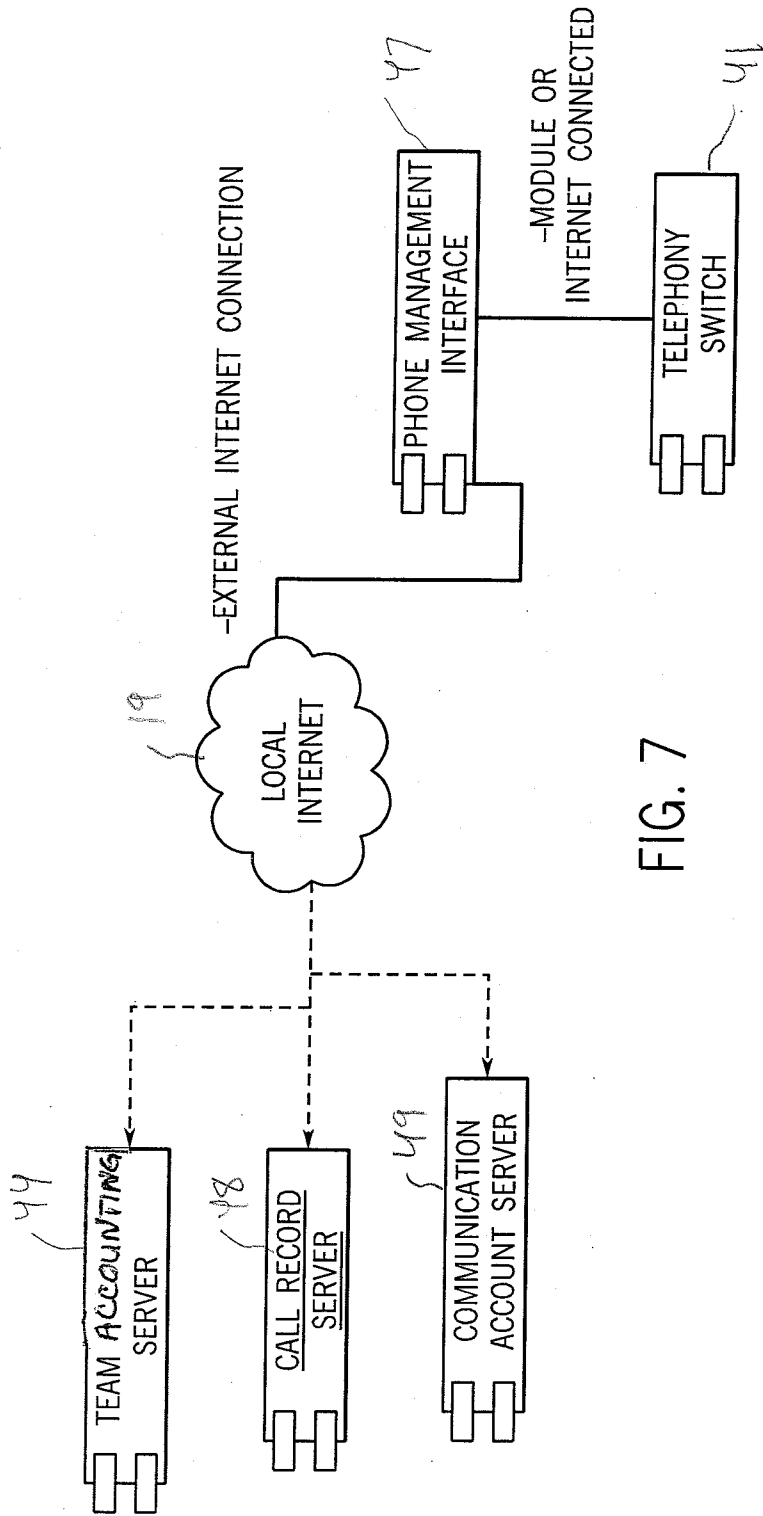


FIG. 7

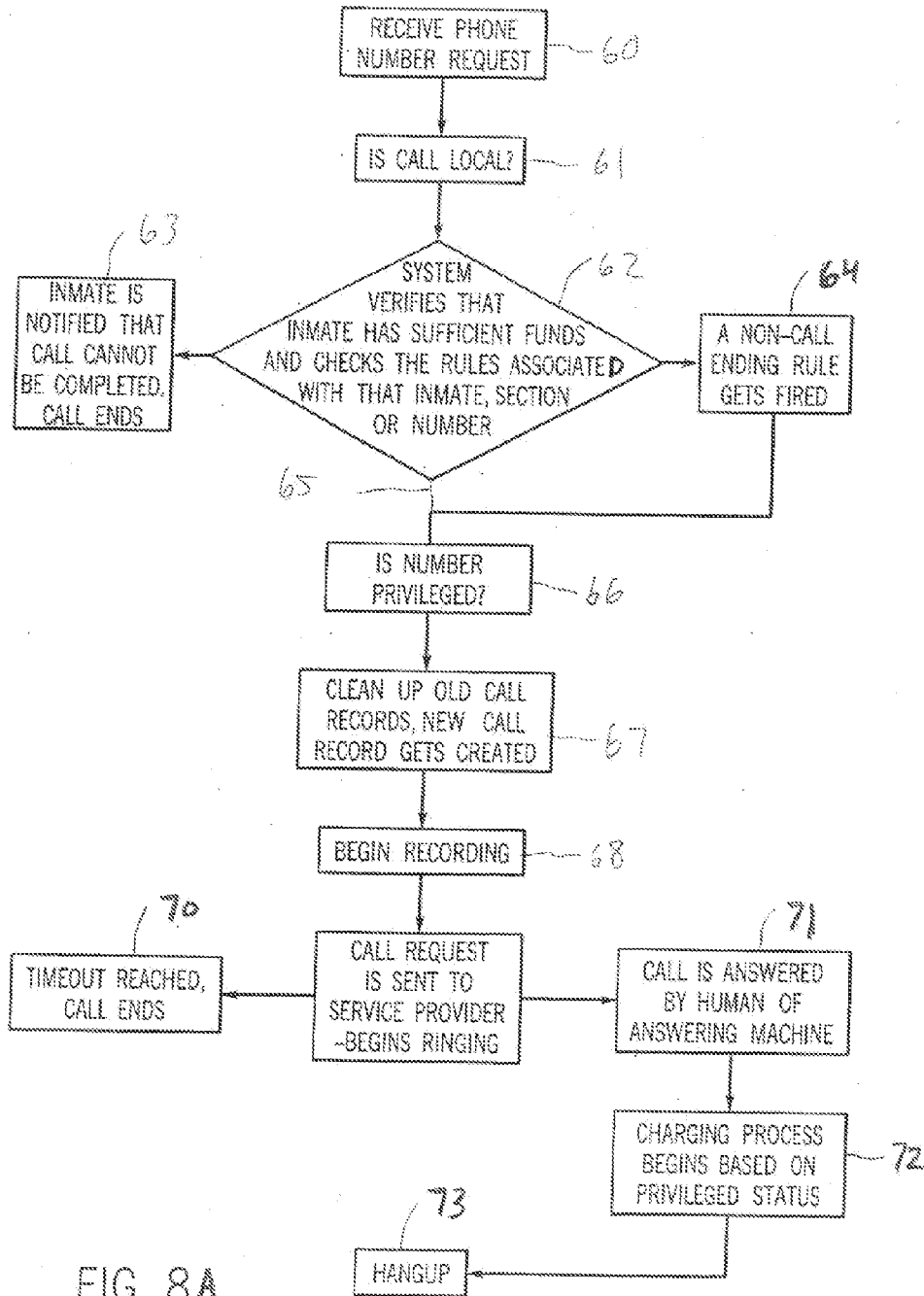


FIG. 8A

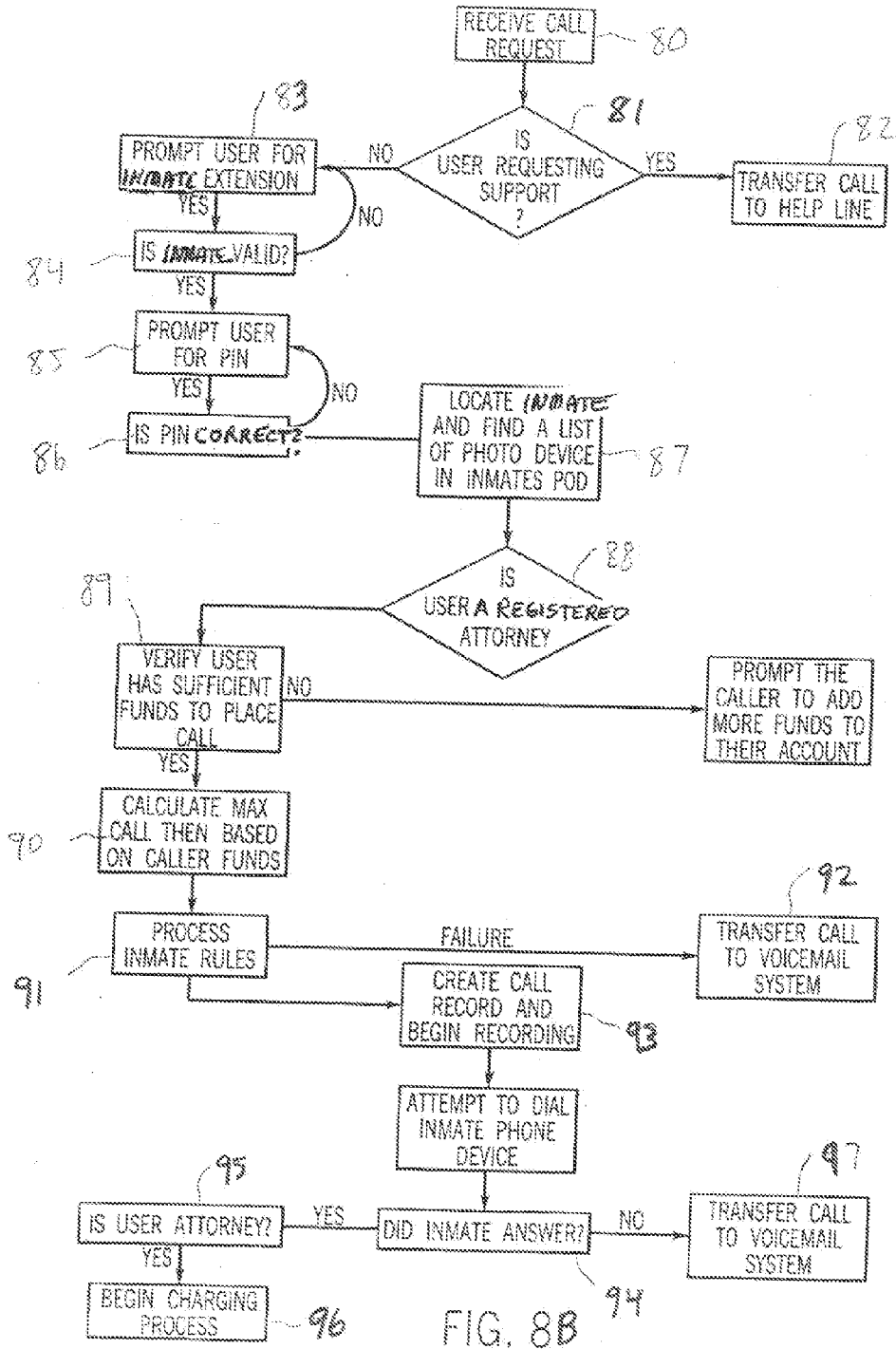


FIG. 8B

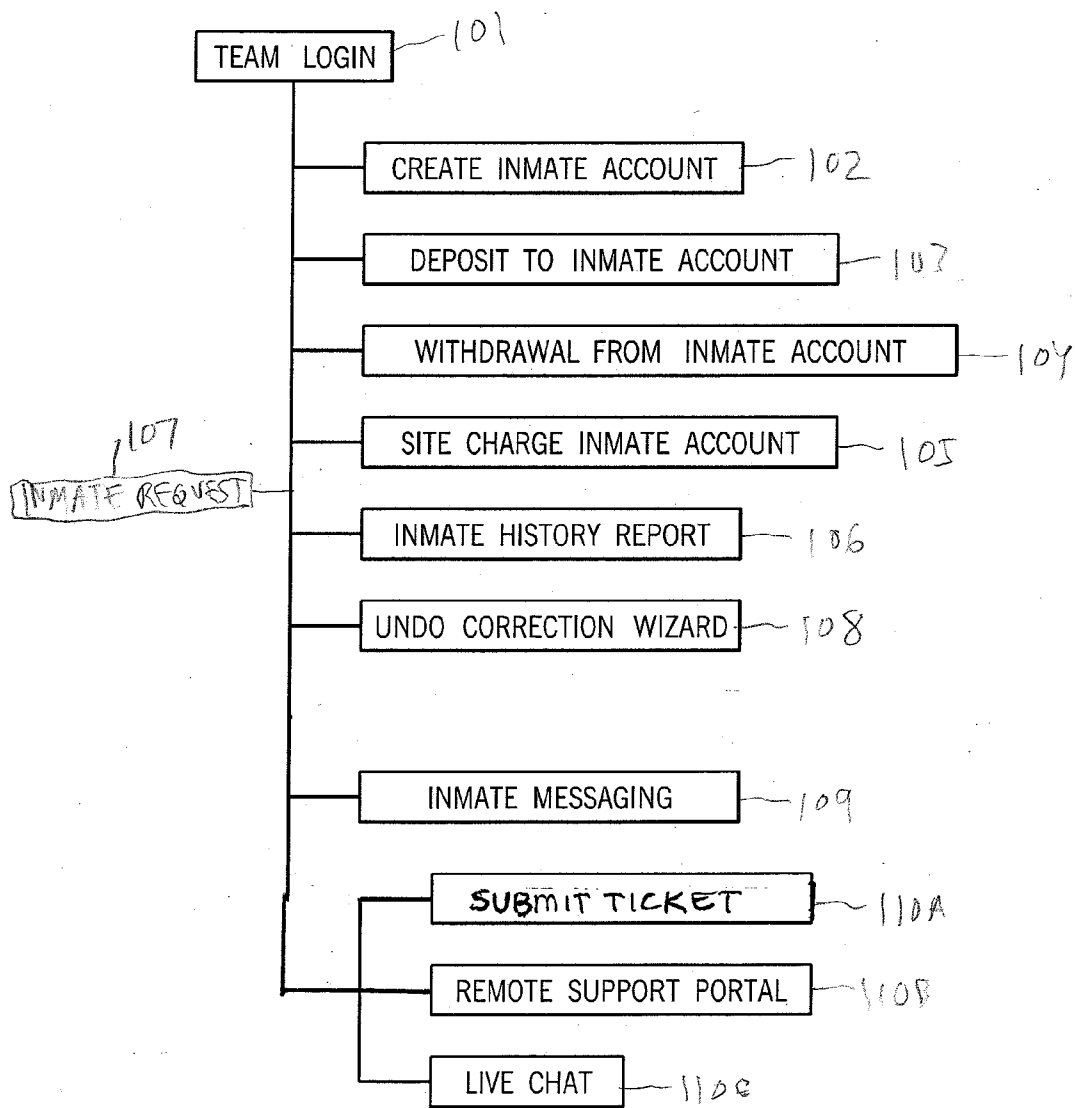


FIG. 9

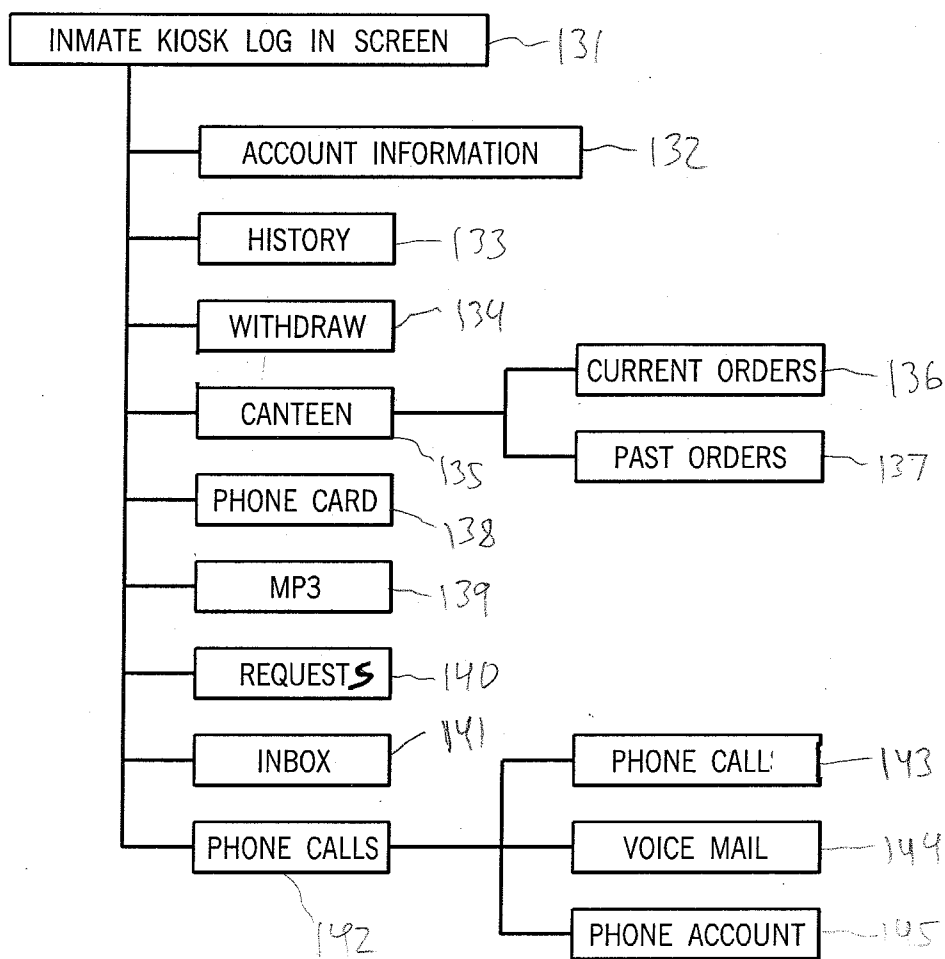


FIG. 10

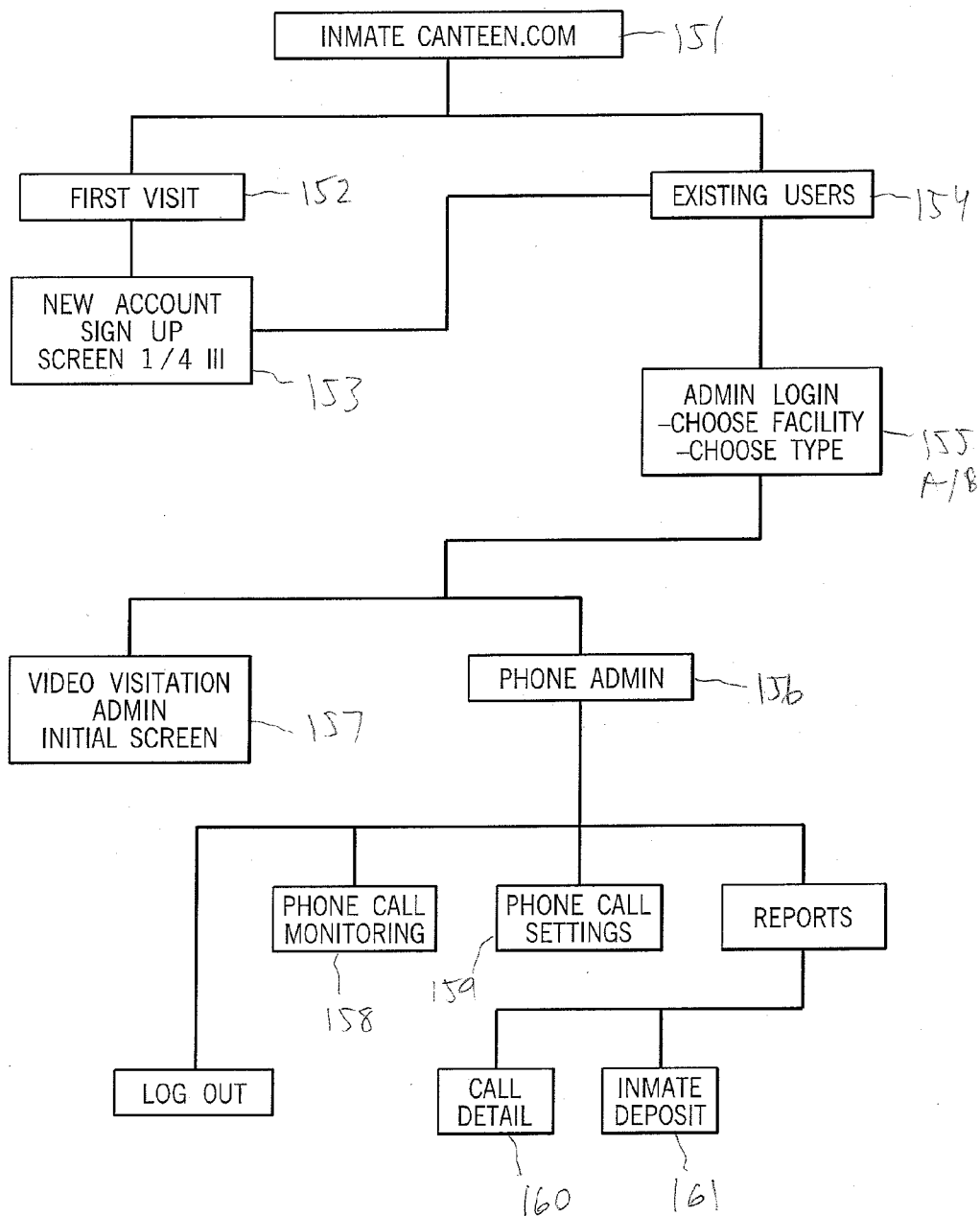


FIG. 11

101A
↓

TEAM ADMIN

WELCOME TO TEAM!
PLEASE ENTER YOUR USERNAME
AND PASSWORD TO LOGIN

TIME ZONE EASTERN 30000 [CHANGE]

USER NAME [SKINNER]

PASSWORD

SITE

LOGIN LOGOUT CANCEL [?]

QUESTIONS? PLEASE CALL US AT (715)3865700

TURTLE

FIG. 12

110c

START CHAT

YOUR NAME:

EMAIL:

COMPANY:

YOUR QUESTION:

DEPARTMENT:

SUPPORT (ONLINE)

START CHAT

FIG. 13

102

TEAM2 TEST SITE ON THE EASTERN TEAM TWENDING.NET SERVER PORT 30000
 SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME CREATE INMATE ACCOUNT

ACCOUNT INFO

ACCOUNT CODE FIRST NAME MIDDLE1 MIDDLE2 LAST NAME

ADDRESS HOME PHONE GENDER BYPASS DEPOSIT SPLIT
 ADDRESS 2 MOBILE PHONE CANTEEN GROUP STANDARD LOBBY VISIBLE
 CITY WORK PHONE LANGUAGE ENGLISH ESCROW
 STATE SITE CHANGE GROUP SELECT INMATE GROUP DATE OF BIRTH MM-DD-YYYY
 ZIP NOTES

DEPOSIT

DEPOSIT TYPE: CASH IN DEPOSIT
 AMOUNT: \$0.00
 ACCOUNT BALANCE: \$0.00

BILL ACCEPTOR STATUS:
 OFFLINE

NOTES

FIG. 14

2017 ✓

TEAM2 TEST SITE ON THE EASTERN.TEAM.TWENDING.NET SERVER PORT 30000
 SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP
 SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME CREATE INMATE ACCOUNT

ACCOUNT INFO

ACCOUNT CODE FIRST NAME MIDDLE1 MIDDLE2 LAST NAME

ADDRESS HOME PHONE GENDER
 ADDRESS 2 MOBILE PHONE CANTEN GROUP STANDARD LOBBY VISIBLE
 CITY WORK PHONE LANGUAGE ENGLISH ESCROW
 STATE SITE CHANGE GROUP SELECT INMATE GROUP DATE OF BIRTH MM-DD-YYYY
 ZIP NOTES

DEPOSIT

DEPOSIT TYPE:
 AMOUNT:
 ACCOUNT BALANCE:

BILL ACCEPTOR STATUS:
 OFFLINE

NOTES

FIG. 15

103

TEAM2 TEST SITE ON THE EASTERN TEAM TWENDING NET SERVER PORT 30000
SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME DEPOSIT

LOOKUP INMATE

GO TO: INMATE HISTORY INMATE MESSAGING EDIT ACCOUNT SITE CHARGE DEPOSIT WITHDRAWAL

ACCOUNT CODE FIRST NAME LAST NAME STATUS SECTION RECENTLY FOUND SEARCH

OR

DEPOSIT

DEPOSIT TYPE: CASH IN DEPOSIT

AMOUNT: \$0.00

ACCOUNT BALANCE: \$0.00

BILL ACCEPTOR STATUS: OFFLINE

NOTES

SUBMIT DEPOSIT

FIG. 16

104

TEAM2, TEST SITE ON THE EASTERN TEAM.TWENDING.NET SERVER PORT 30000
 SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME WITHDRAWAL

GO TO: ?

ACCOUNT CODE OR FIRST NAME LAST NAME STATUS SECTION RECENTLY FOUND

SELECT TRANSACTION TYPE

AMOUNT:

CHECK#

PAY TO THE ORDER OF

FIG. 17

105

TEAM2 TEST SITE ON THE EASTERN TEAM TWENDING.NET SERVER PORT 30000
SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME SITE CHARGE

GO TO: INMATE HISTORY INMATE MESSAGING EDIT ACCOUNT SITE CHARGE DEPOSIT WITHDRAWAL ?

ACCOUNT CODE FIRST NAME LAST NAME STATUS SECTION RECENTLY FOUND (SEARCH)

OR

REMOVE SITE CHARGE AMOUNT NOTES STATUS

RESET TOTAL \$0.00 APPLY CHARGES

FIG. 18

906
↙

TEAM2 TEST SITE ON THE EASTERN TEAM TWENDING.NET SERVER PORT 30000
 SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME INMATE HISTORY REPORT

GO TO: INMATE HISTORY INMATE MESSAGING EDIT ACCOUNT SITE CHARGE DEPOSIT WITHDRAWAL

ACCOUNT CODE FIRST NAME LAST NAME STATUS SECTION RECENTLY FOUND SEARCH

OR

STARTING TUESDAY, SEPTEMBER 25, 2012 AM 12 : 00 ENDING TUESDAY, SEPTEMBER 25, 2012 PM 11 : 59 TODAY RUN RUN DETAIL

REPORT VIEW PRINT PREVIEW

TOTAL \$0.00
SUBMIT WITHDRAWAL

FIG. 19

✓ 107

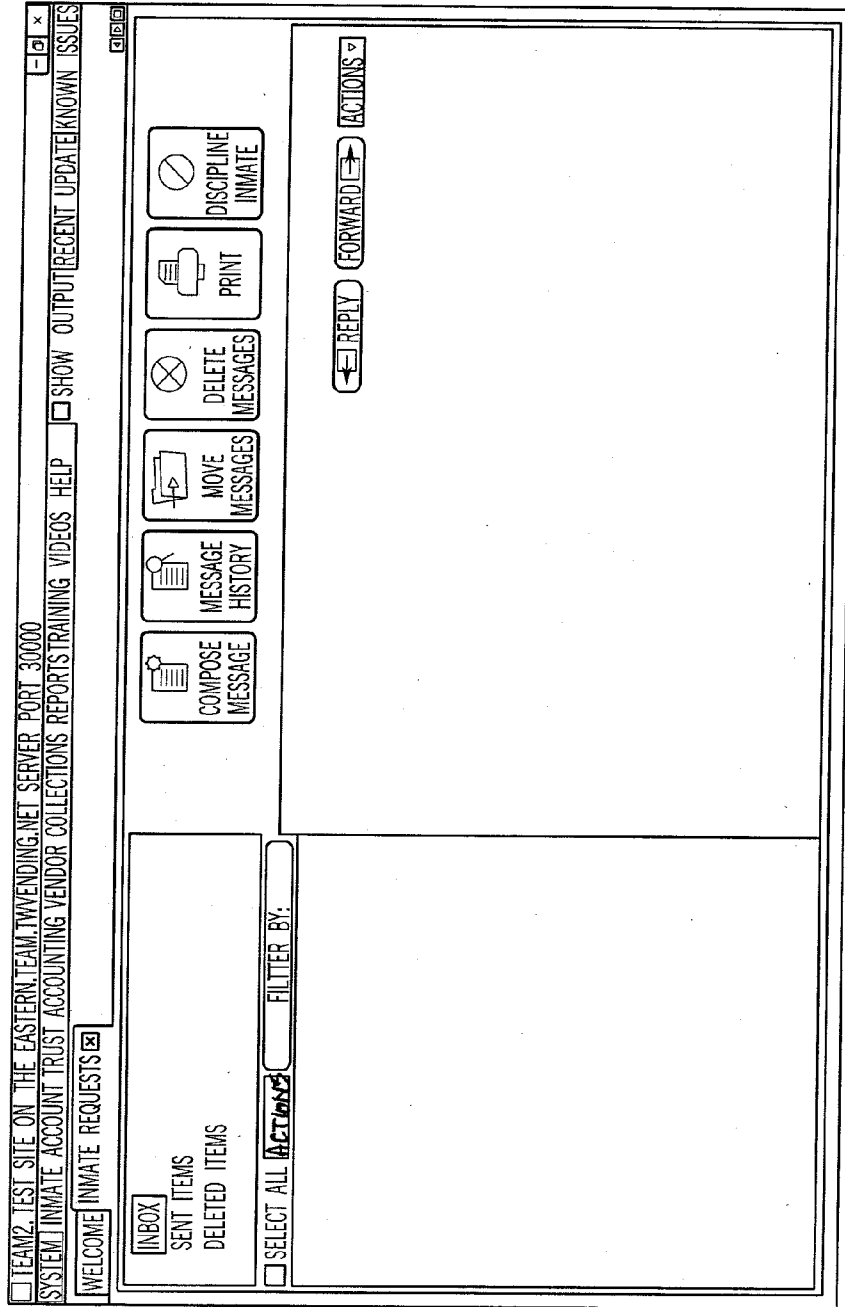


FIG. 20

801 ↘

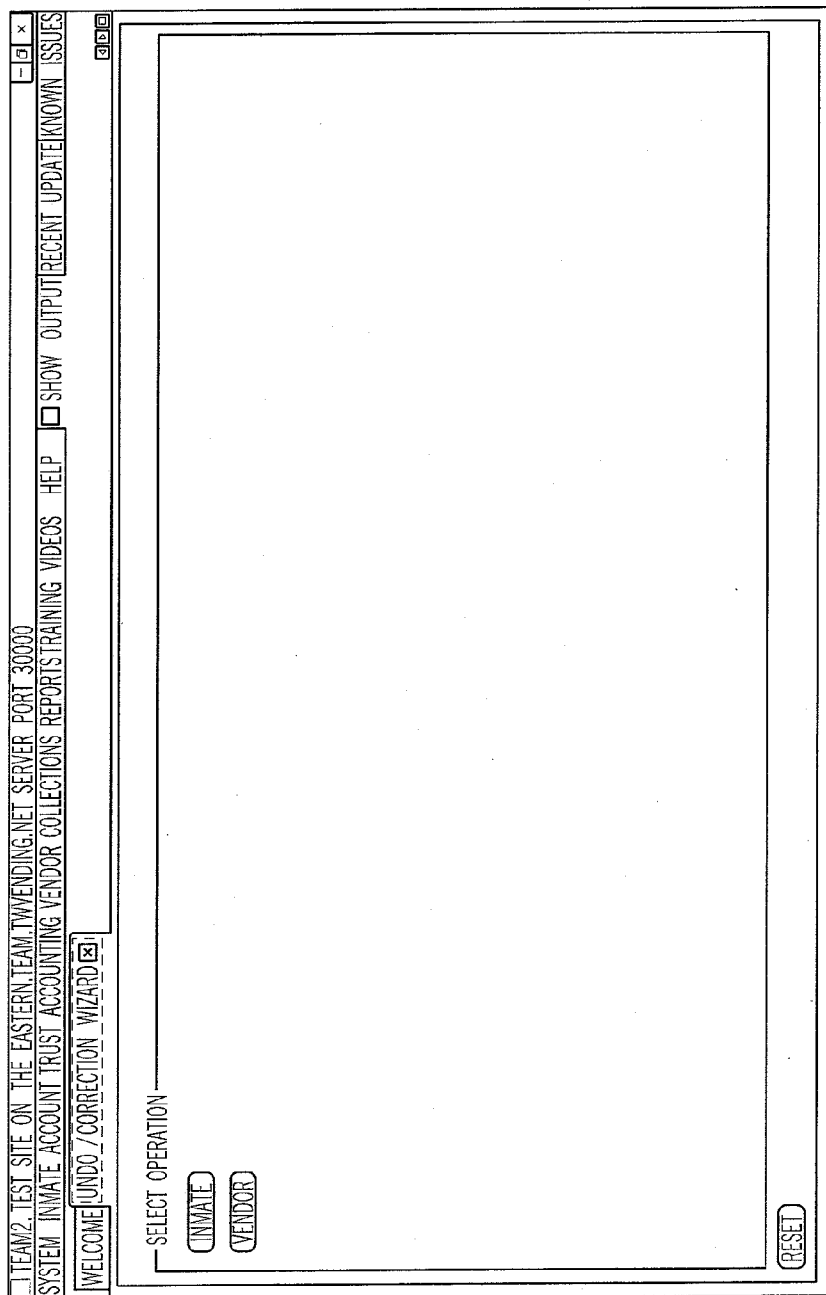


FIG. 21

110A ↙

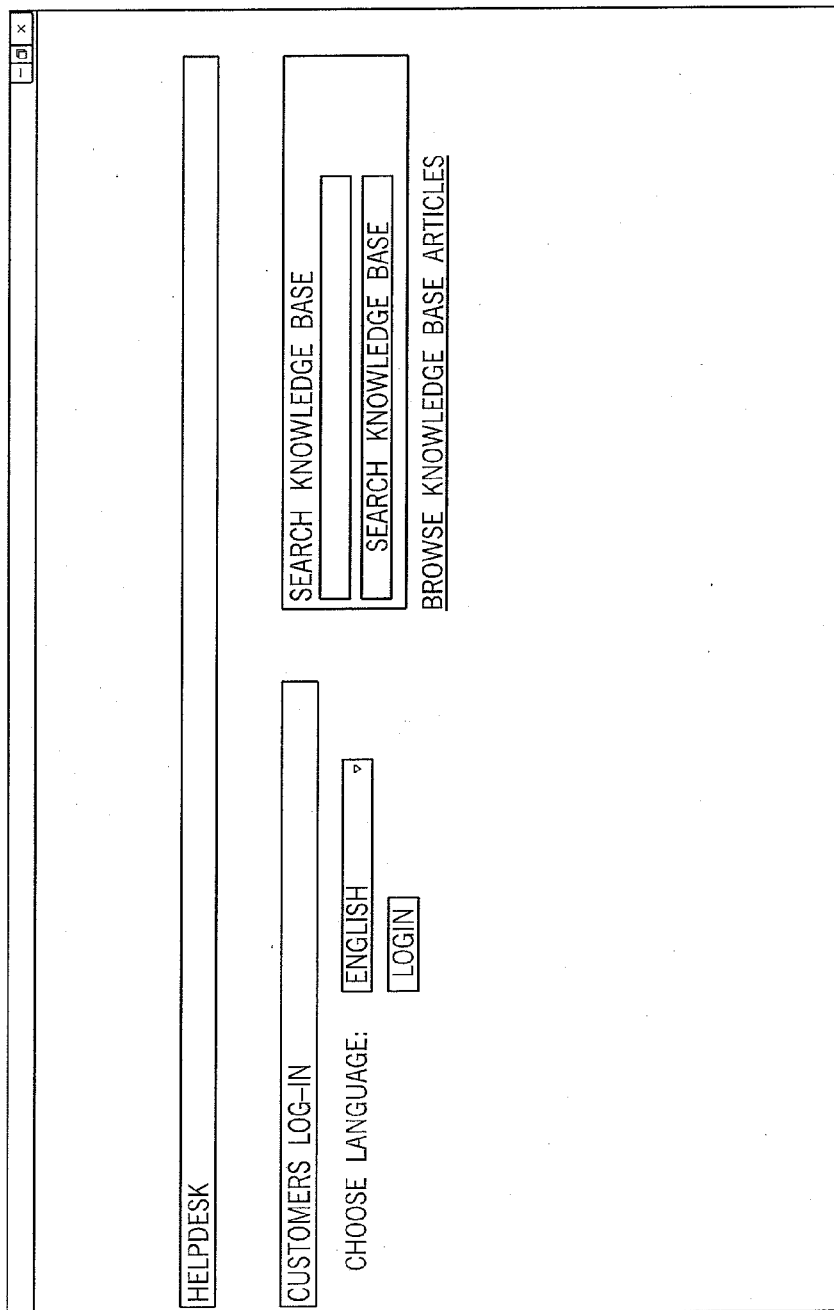


FIG. 22

✓ 116B

SUPPORT PORTAL ENGLISH (US)

REPRESENTATIVES ?

1-BEN*OBI*WANLESS

ISSUE SUBMISSION ?

-PLEASE CHOOSE AN ISSUE-

YOUR ISSUE

YOUR NAME

COMPANY NAME

DESCRIBE YOUR ISSUE

SUBMIT

FIG. 23

110c
↓

START CHAT

YOUR NAME:	<input type="text"/>
EMAIL:	<input type="text"/>
COMPANY:	<input type="text"/>
YOUR QUESTION:	<input type="text"/>
DEPARTMENT:	<input type="text"/>

FIG. 24



TEAM2, TEST SITE ON THE EASTERN.TEAM.TWENDING.NET SERVER PORT 30000
SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME

ACCOUNT CODE FIRST NAME LAST NAME STATUS SECTION RECENTLY FOUND

REMOVE SITE CHARGE AMOUNT NOTES STATUS

TOTAL \$0.00

FIG. 25

112
↓

TEAM2 TEST SITE ON THE EASTERN TEAM TWENDING NET SERVER PORT 30000
SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME ASSIGN INMATE SMART CARD

LOOKUP INMATE

ACCOUNT CODE FIRST NAME LAST NAME STATUS SECTION RECENTLY FOUND SEARCH

CHECK CARD BALANCE READ CARD

ASSIGN A NEW CARD ASSIGN CARD UNLOAD CARD

ASSIGNED SMART CARDS

SERIAL NUMBER STATUS INACTIVATE SUSPEND ACTIVATE

FIG. 26

113
↓

TEAM2 TEST SITE ON THE EASTERN.TEAM.TWENDING.NET SERVER PORT 30000
 SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME **DISCIPLINE INMATE ACCOUNT**

LOOKUP INMATE

ACCOUNT CODE FIRST NAME LAST NAME STATUS SECTION RECENTLY FOUND

OR

LOCK KIOSK SELECTED INMATE(S) WILL NOT BE ABLE TO LOG INTO A KIOSK IF BOX IS CHECKED

CURRENT DISCIPLINE

DISC ID | USER | START DATE | END DATE | ENABLED | KIOSK ACCESS | CARD WITHDRAW | CANTEN | MESSAGING | REQUESTS | PHONE | COMMENTS

DISCIPLINE START DAY
 TUESDAY, SEPTEMBER 25, 2012

DISCIPLINE END DAY
 TUESDAY, SEPTEMBER 25, 2012

COMMENTS

FIG. 27

114
↙

TEAM2 TEST SITE ON THE EASTERN TEAM TWENDING.NET SERVER PORT 30000
 SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES
 WELCOME

GO TO:
 ACCOUNT CODE FIRST NAME LAST NAME STATUS SECTION RECENTLY FOUND

ACCOUNT CODE FIRST NAME MIDDLE NAME SECOND MIDDLE NAME LAST NAME ACCOUNT STATUS ACCOUNTING GROUP

ADDRESS1 HOME PHONE GENDER BYPASS ESCROW
 ADDRESS 2 MOBILE PHONE LANGUAGE ENGLISH VISIBLE AT LOBBY
 CITY WORK PHONE ESCROW ACCOUNT
 STATE DATE OF BIRTH MM-DD-YYYY
 ZIP NOTES NOTES

FIG. 28

115

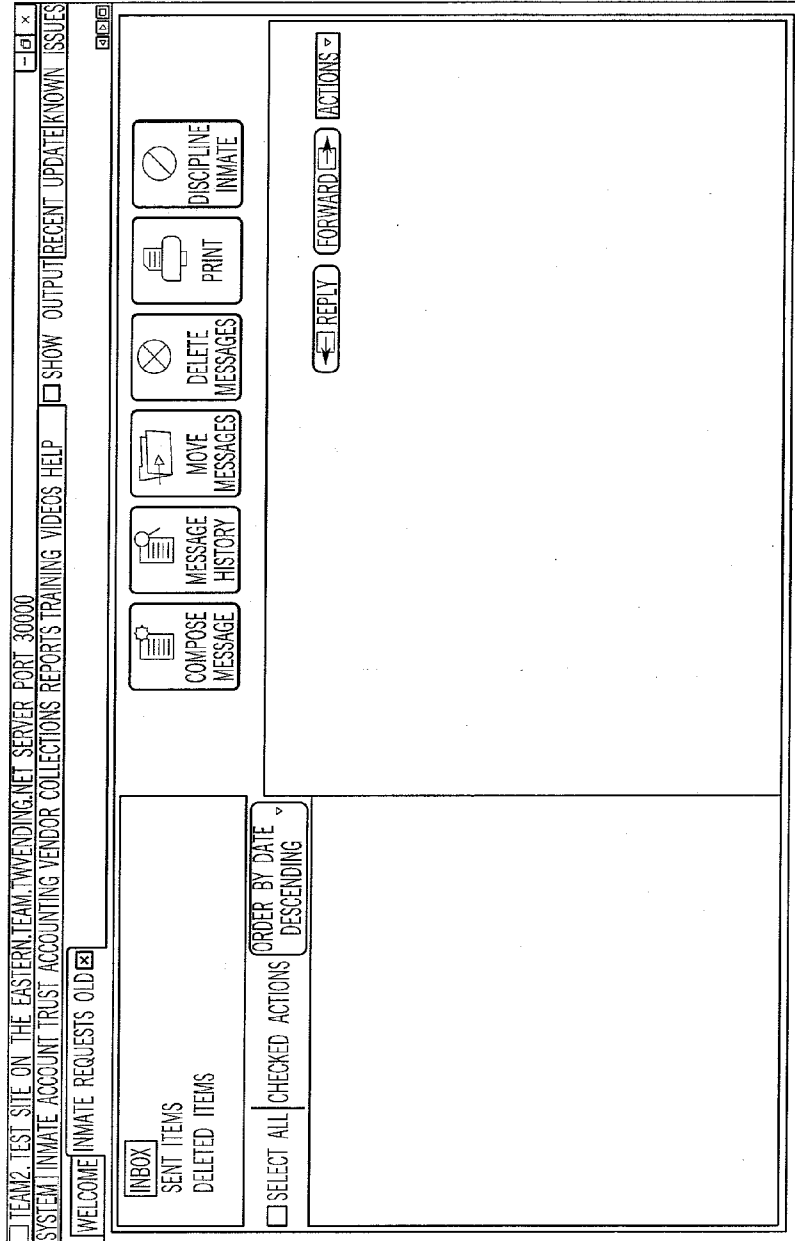


FIG. 29

116
↓

<input type="checkbox"/> TEAM2 TEST SITE ON THE EASTERN TEAM.TWENDING.NET SERVER PORT 30000							
SYSTEM: INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP <input type="checkbox"/> SHOW OUTPUT RECENT UPDATE KNOWN ISSUES							
WELCOME <input checked="" type="checkbox"/> VIEW INMATE CANTEEN ORDERS <input checked="" type="checkbox"/>							
ACCOUNT CODE	FIRST NAME	LAST NAME	<input checked="" type="checkbox"/> STATUS	SECTION	RECENTLY FOUND		
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		
<input type="text"/>	OR	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		
<input type="button" value="SEARCH"/>							
<input type="button" value="REFRESH"/> <input type="checkbox"/> VIEW RECEIVED <input type="checkbox"/> VIEW CANCELLED							
BATCH	ORDER	TOTAL	DATE	PULLED	RECEIVED	CANCELLED	UPDATED
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

FIG. 30

117 ↘

TEAM2 TEST SITE ON THE EASTERN TEAM TWINNING NET SERVER PORT 30000
SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME BANK DEPOSIT

UNDEPOSITED CASH BALANCE
UNDEPOSITED COIN BALANCE
UNDEPOSITED CHECK BALANCE
UNDEPOSITED TRANSFER IN BALANCE
UNDEPOSITED MISC DEPOSIT
UNDEPOSITED FUNDS FOR DEPOSIT

END CURRENT SESSION

CASH COIN CHECKS TRANSFER IN MISC

AMOUNT	TYPE	DATE	CASH	TRANS

CASH TOTAL
COIN TOTAL
CHECK TOTAL
TRANSFER IN TOTAL
MISC TOTAL
TOTAL DEPOSIT

NOTES SAVE

FIG. 31

811 ↘

TEAM2 TEST SITE ON THE EASTERN TEAM.TWENDING.NET SERVER PORT 30000
 SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME | DEPOSIT TO VENDOR

VENDOR CHECK NUMBER
DEPOSIT TYPE CHECK DEPOSIT TO VENDOR PAYOR
DEPOSIT TYPE \$0.00 PAY TO THE ORDER OF

TRANSACTION NOTES

FIG. 32

119
↓

TEAM2 TEST SITE ON THE EASTERN TEAM TWENDING.NET SERVER PORT 30000
 SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME PAY VENDOR

VIEW VENDOR BALANCES ON TUESDAY, SEPTEMBER 25, 2012

CHECK TOTAL	CHECK NUMBER	PAY TO THE ORDER OF	CHECK TOTAL	MEMO	ADDITIONAL MEMO	INCLUDE	VENDOR NAME	BALANCE	CHECK AMOUNT
						<input type="checkbox"/>	MEDIA COMM VENDOR	40.00	40.00

BACKDATE TRANSACTION

NOTES
PRINT CHECK

FIG. 33

120
↓

TEAM2 TEST SITE ON THE EASTERN TEAM TWENDING NET SERVER PORT 30000
 SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME **BATCH ORDERS** [X]

VIEW INMATES ORDER CREATE BATCH VIEW BATCHES

ACCOUNT CODE OR FIRST NAME LAST NAME STATUS SECTION RECENTLY FOUND

VIEW RECEIVED VIEW CANCELLED

BATCH ORDER	TOTAL	DATE	PULLED	RECEIVED	CANCELLED	UPDATED

FIG. 34

121
↓

TEAM2 TEST SITE ON THE EASTERN TEAM TWENDING.NET SERVER PORT 30000
SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING Videos Help SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME MANAGE SITE CANTEEN SYSTEM

MANAGE WAREHOUSE MANAGE GROUPS

SELECT WAREHOUSE RECALC PENDING

FILTER BY CATEGORY ALL FILTER BY SUPPLIER ALL / ANY VIEW DISABLED

CHANGED ITEM DESC BARCODE DESCRIPTION MIN PAR AUTO ADJUST SUPPLIER BIN # CANTEEN VENDING ENABLED

QUICK ADD ITEM

SAVE CHANGED

FIG. 35

122
↓

TEAM2. TEST SITE ON THE EASTERN TEAM TWENDING.NET SERVER PORT 30000

SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME MANAGE WAREHOUSE

SELECT WAREHOUSE

FIG. 36

123
↓

TEAM2 TEST SITE ON THE EASTERN TEAM TWENDING.NET SERVER PORT 30000
 SYSTEM INMATE ACCOUNT TRUST ACCOUNTING VENDOR COLLECTIONS REPORTS TRAINING VIDEOS HELP SHOW OUTPUT RECENT UPDATE KNOWN ISSUES

WELCOME MANAGE WAREHOUSE **ORDERS SYSTEM**

VIEW RECEIVED ORDERS VIEW CANCELLED ORDERS TEST SITE

CHECKED	WAREHOUSE NAME	ORDER ID	DATE	PRINTED	RECEIVED	CANCELLED	EDIT	PRINT

MARKED CHECKED AS

FIG. 37

131
↓

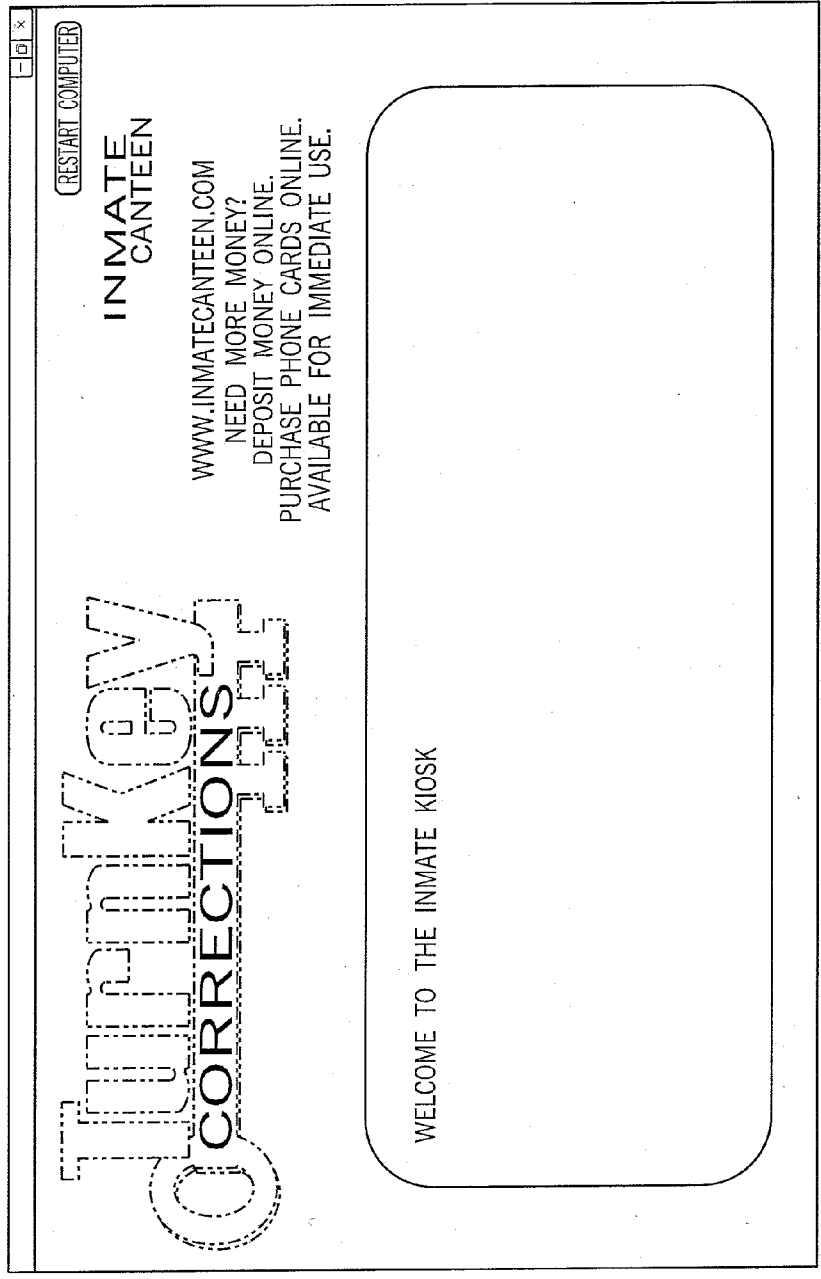


FIG. 38

132
↓

<div style="text-align: right;"> [-] [x] [c] RESTART COMPUTER </div>	
INMATE NAME	
ACCOUNT INFO HISTORY CHANGE PIN WITHDRAWAL CANTEEN PHONE CARD MP3 REQUESTS INBOX PHONE CALL EXIT	ACCOUNT INFORMATION ACCOUNT CODE 1471 INMATE NAME ADMIN LANGUAGE ENGLISH ACCOUNT BALANCES \$68.80 TRUST BALANCE \$0.00 LIEN BALANCE \$0.00 BAIL BALANCE \$0.00 SMART CARD BALANCE \$0.00 PHONE REQUESTS
NOTICES YOU HAVE 1 UNREAD MESSAGES, PLEASE GO TO INBOX TAB TO VIEW THEM.	
JAIL NOTICE	

FIG. 39

133
↓

ACCOUNT INFO		SELECT		INMATE NAME		RESTART COMPUTER	
DATE		DAY		WEEK		AMOUNT BALANCE	
HISTORY		MONTH		YEAR		ALL	
CHANGE PIN		TRANSACTION TYPE		YEAR		ALL	
WITHDRAWAL		TRANSACTION TYPE		YEAR		ALL	
CANTEEN		TRANSACTION TYPE		YEAR		ALL	
PHONE CARD		TRANSACTION TYPE		YEAR		ALL	
MP3		TRANSACTION TYPE		YEAR		ALL	
REQUESTS		TRANSACTION TYPE		YEAR		ALL	
INBOX		TRANSACTION TYPE		YEAR		ALL	
PHONE CALL		TRANSACTION TYPE		YEAR		ALL	
EXIT		TRANSACTION TYPE		YEAR		ALL	

FIG. 40

✓ 134

ACCOUNT INFO		INMATE NAME		RESTART COMPUTER	
QUICK WITHDRAW		CURRENT ACCOUNT BALANCE \$68.80		CURRENT CARD BALANCE \$0.00	
HISTORY	\$5	\$10			
CHANGE PIN	\$15	\$20			
WITHDRAWAL					
CANTEEN	CLEAR	WITHDRAWAL AMOUNT	\$0.00		
PHONE CARD	1	2	3		
MP3	4	6	6		
REQUESTS	7	8	9		
INBOX					
PHONE CALL					
EXIT					
WITHDRAW					

FIG. 41

135A ↙

[RESTART COMPUTER]											
INMATE NAME											
VIEW CURRENT ORDER						VIEW PAST ORDERS					
ACCOUNT INFO	HISTORY	CHANGE PIN	WITHDRAWAL	CANTEEN	PHONE CARD	MP3	REQUESTS	INBOX	PHONE CALL	EXIT	

← 136

← 137

FIG. 42

135B ✓

ACCOUNT INFO		INMATE NAME		RESTART COMPUTER	
HISTORY		PICTURE	CATEGORY	ITEM DESCRIPTION	PRICE PICTURE ON HAND ADD ONE
CHANGE PIN		POSTAGE			
WITHDRAWAL		ACCOUNT BALANCE \$68.80 LESS \$0 UNPAID IN CURRENT ORDER LEAVES \$68.80 REMAINING			
CANTEEN		QTY	ITEM DESCRIPTION	PRICE SUB TOTAL ADD ONE REMOVE ONE	
PHONE CARD					
MP3					
REQUESTS					
INBOX					
PHONE CALL					
EXIT		PLACE ORDER			

FIG. 43

138
↓

ACCOUNT INFO		PLEASE SELECT A PHONE CARD TO PURCHASE		INMATE NAME		RESTART COMPUTER	
HISTORY		PRICE PURCHASE					
CHANGE PIN							
WITHDRAWAL		DATE		PRICE		PIN ▲	
CANTEEN							
PHONE CARD							
MP3							
REQUESTS							
INBOX							
PHONE CALL							
EXIT							

FIG. 44

139
↓

ACCOUNT INFO	INMATE NAME	RESTART COMPUTER
HISTORY	HISTORY	
CHANGE PIN	VIEW MP3 PLAYER	
WITHDRAWAL	SEARCH ARTISTS	
CANTEEN	SEARCH SONGS	
PHONE CARD	SEARCH ALBUMS	
MP3		
REQUESTS		
INBOX		
PHONE CALL		
EXIT		

FIG. 45

140
↓

ACCOUNT INFO		TOP		BACK		INMATE NAME		RESTART COMPUTER		VIEW		-		+	
HISTORY		REQUEST TYPE		IOCC MESSAGES											
CHANGE PIN															
WITHDRAWAL															
CANTEEN															
PHONE CARD															
MP3															
REQUESTS															
INBOX															
PHONE CALL															
EXIT															

FIG. 4b

141
↓

ACCOUNT INFO		INMATE NAME		RESTART COMPUTER	
UNREAD MESSAGES		VIEW MAIL		GO BACK	
FOLDER		NAME		MESSAGE COUN	
VIEW DELETED ITEMS				0	
VIEW INBOX				1	
VIEW SENT ITEMS				0	
VIEW DATE REMOVE		SUBJECT			
ACCOUNT INFO		HISTORY		PHONE CARD	
CHANGE PIN		WITHDRAWAL		MP3	
CANTEEN		PHONE CALL		REQUESTS	
		EXIT		INBOX	

FIG. 47

143
↓

ACCOUNT INFO	SAVED CONTACTS	PHONE CALL	INMATE NAME	PHONE ACCOUNT	RESTART COMPUTER
HISTORY	NICKNAME	PHONE #	VOICEMAIL (3)	COLLECT CALLING IS UNAVAILABLE AT THIS KIOSK	
CHANGE PIN	NAME	715-781-4987	SELECT DELETE	COLLECT CALLER NUMBER	PIN
WITHDRAWAL					
CANTEEN					
PHONE CARD	1	2	3		CLEAR SAVE
MP3	4	5	6	PHONE ACCOUNT BALANCE:	\$4.65
REQUESTS	7	8	9	CALL RATE:	\$0.35
INBOX					
PHONE CALL		0		CALL	
EXIT	ONLINE:			VOLUME	+ -

FIG. 48

144
↓

ACCOUNT INFO		INMATE NAME		PHONE CALL		VOICEMAIL (3)		PHONE ACCOUNT		RESTART COMPUTER	
HISTORY		CALLER	DATE								
CHANGE PIN		TKC SUPPORT	9 /14 /2012	8:19 AM							
WITHDRAWAL		TKC SUPPORT	9 /28 /2012	12:55 AM							
CANTEEN		TKC SUPPORT	10 /14 /2012	6:37 AM							
PHONE CARD											
MP3											
REQUESTS											
INBOX											
PHONE CALL											
EXIT											

FIG. 49

145
↙

ACCOUNT INFO		PHONE CALL		INMATE NAME		RESTART COMPUTER	
HISTORY		VOICE MAIL (3)		PHONE ACCOUNT			
CHANGE PIN		CURRENT TRUST ACCOUNT BALANCE \$68.80		WITHDRAW TO PHONE ACCOUNT			
WITHDRAWAL		CURRENT DEBIT ACCOUNT BALANCE \$4.65		\$5		\$10	
CANTEEN		DAY		WEEK		\$20	
PHONE CARD		DATE		ALL			
MP3		DEBIT					
REQUESTS		CREDIT					
INBOX							
PHONE CALL							
EXIT							

FIG. 50

FIG 7
↓

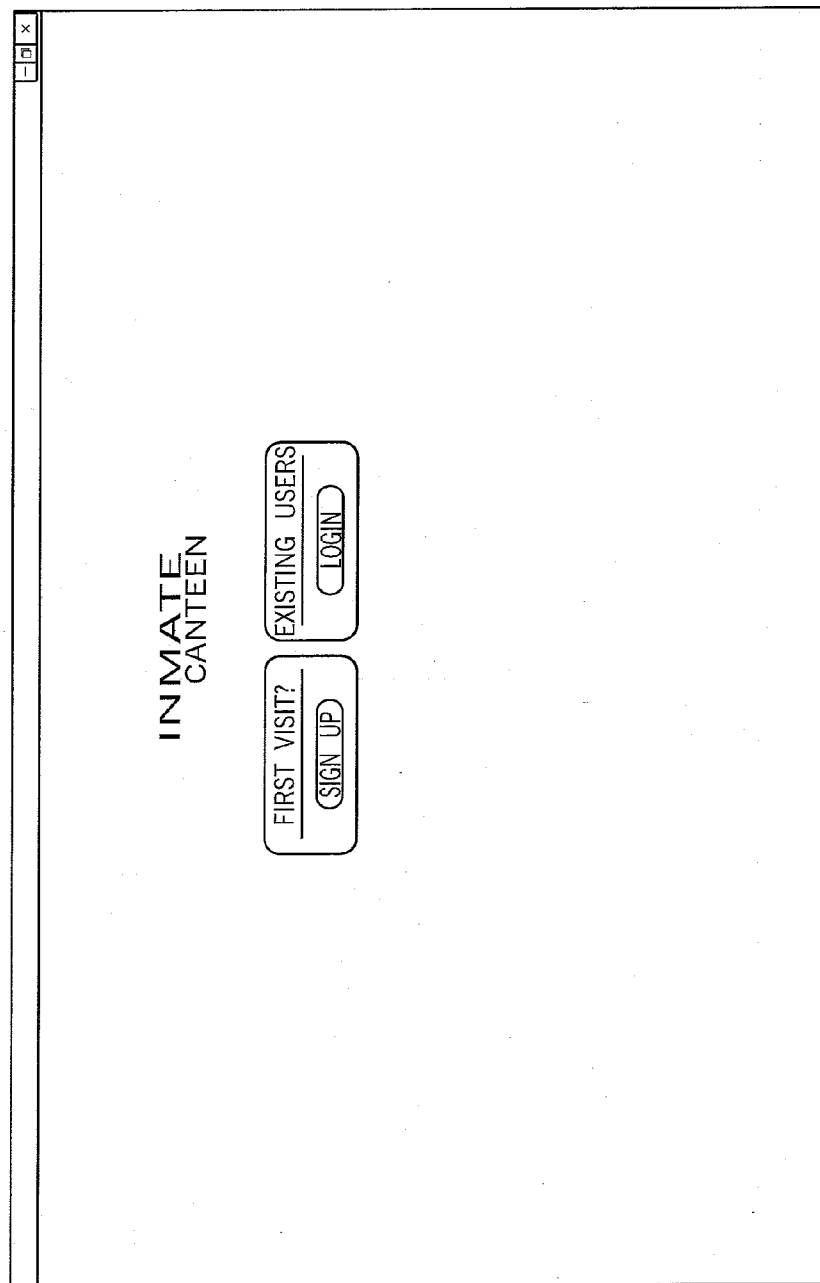


FIG. 51

153
↓

INMATE CANTEEN

HOME FAQ CONTACT

NEW ACCOUNT SIGNUP

STEP 1 OF 4

AN INMATE CANTEEN ACCOUNT GIVES YOU DIRECT ACCESS TO A VARIETY OF SPECIALIZED SERVICES DESIGNED SPECIFICALLY FOR FAMILY AND FRIENDS OF INMATES IN CORRECTIONAL FACILITIES AROUND THE U.S.

CURRENTLY YOU MAY DEPOSIT FUNDS DIRECTLY INTO AN INMATE'S TRUST ACCOUNT, AND SOON YOU WILL BE ABLE TO SEND CARE PACKAGES, PURCHASE PRE-PAID PHONE CARDS, AND SEND ELECTRONIC MESSAGES TO INMATES AS WELL.

PLEASE ENTER YOUR FIRST AND LAST NAME BELOW

FIRST NAME:

LAST NAME:

PHONE NUMBER:

NEXT

FIG. 52

155A
↓

The image shows a login form within a window frame. The window title bar at the top contains standard minimize, maximize, and close icons. The form is titled "INIMATE CANTEEN" in a bold, sans-serif font. Below the title, the text "PLEASE LOGIN" is centered. There are two input fields: the first is labeled "USERNAME (E-MAIL ADDRESS)" and the second is labeled "PASSWORD:". To the right of these fields is a button labeled "LOGIN".

FIG. 53

1558
↓

INMATE
CANTEEN

ADMIN LOGIN

CHOOSE FACILITY: AJININ COUNTY, MI

ADMIN TYPE: VIDEO ADMIN

SELECT

FIG. 54

156 ↘

<p>INMATE CANTEEN PHONE CALL MONITORING PHONE SITE SETTINGS REPORTS ▾ LOGOUT</p> <p>TEST SITE TELPHONY SITE SETTINGS</p>											
<p>EMAIL NOTIFICATIONS</p> <p>ADD NEW NOTIFICATION <input type="button" value="⊕"/></p> <p>EMAIL ADDRESS: <input type="text" value="A@JAILCOMB@JAIL.COM"/> <input type="button" value="⊕"/></p> <p>PER APPROVED WEBUSER: <input type="text" value="NO WEBUSERS AVAILAB"/> ▾</p> <p>PER INMATE: <input type="text" value="-SELECT-"/> ▾</p> <p>PER SECTION: <input type="text" value="-SELECT-"/> ▾</p> <p>PER INMATE GROUP: <input type="text" value="-SELECT-"/> ▾ <input type="button" value="ADD SETTING"/></p>											
<p>BLACKLISTING</p> <p>BLACKLIST INMATES AND WEBUSERS FROM PHONE CALLS <input type="button" value="⊕"/></p> <p>SELECT AN APPROVED WEBUSER: <input type="text" value="NO WEBUSERS AVAILAB"/> <input type="button" value="⊕"/></p> <p>SELECT AND INMATE: <input type="text" value="-SELECT-"/> ▾</p> <p>SELECT A SECTION: <input type="text" value="-SELECT-"/> ▾</p> <p>SELECT A GROUP: <input type="text" value="-SELECT-"/> ▾</p> <p>ENTER A PHONE NUMBER: <input type="text"/> <input type="button" value="ADD SETTING"/></p> <p>SEARCH FOR BLACKLISTED NUMBER: <input type="text"/> <input type="button" value="SEARCH"/></p>											
<p>PHONE CALL HOURS</p> <p>EDIT PHONE INCOMING / OUTGOING HOURS</p> <p>DAY: <input type="text" value="-SELECT-"/> ▾ START TIME: <input type="text" value="11:24:00AM"/> <input type="button" value="⊕"/> END TIME: <input type="text" value="11:24:00AM"/> <input type="button" value="⊕"/> <input type="button" value="ADD SETTING"/></p> <p>MONDAY'S CALL HOURS:</p> <table border="1"> <tr> <td>MONDAY</td> <td><input type="text" value="15:00 AM"/></td> <td>TO</td> <td><input type="text" value="10:00 PM"/></td> <td><input type="button" value="⊕"/></td> </tr> <tr> <td>MONDAY</td> <td><input type="text" value="9:30 AM"/></td> <td>TO</td> <td><input type="text" value="9:30 PM"/></td> <td><input type="button" value="⊕"/></td> </tr> </table>		MONDAY	<input type="text" value="15:00 AM"/>	TO	<input type="text" value="10:00 PM"/>	<input type="button" value="⊕"/>	MONDAY	<input type="text" value="9:30 AM"/>	TO	<input type="text" value="9:30 PM"/>	<input type="button" value="⊕"/>
MONDAY	<input type="text" value="15:00 AM"/>	TO	<input type="text" value="10:00 PM"/>	<input type="button" value="⊕"/>							
MONDAY	<input type="text" value="9:30 AM"/>	TO	<input type="text" value="9:30 PM"/>	<input type="button" value="⊕"/>							
<p>PHONE CALL MONITORING</p> <p>PHONE CALL SETTINGS</p> <p>REPORTS ▾</p>											

FIG. 55

651 ↘

<p>INMATE CANTEN PHONE CALL MONITORING PHONE SITE SETTINGS REPORTS ▾ LOGOUT</p> <p>TEST SITE TELPHONY SITE SETTINGS</p>											
<p>PHONE CALL MONITORING</p> <p>PHONE CALL SETTINGS</p> <p>REPORTS ▾</p>											
<p>EMAIL NOTIFICATIONS</p> <p>ADD NEW NOTIFICATION <input type="button" value="⊕"/></p> <p>EMAIL ADDRESS: <input type="text" value="A@JAIL.COM@JAIL.COM"/> <input type="button" value="⊕"/></p> <p>PER APPROVED WEBUSER: <input type="text" value="NO WEBUSERS AVAILAB"/> ▾</p> <p>PER INMATE: <input type="text" value="-SELECT-"/> ▾</p> <p>PER SECTION: <input type="text" value="-SELECT-"/> ▾</p> <p>PER INMATE GROUP: <input type="text" value="-SELECT-"/> ▾ <input type="button" value="ADD SETTING"/></p>											
<p>BLACKLISTING</p> <p>BLACKLIST INMATES AND WEBUSERS FROM PHONE CALLS</p> <p>SELECT AN APPROVED WEBUSER: <input type="text" value="NO WEBUSERS AVAILAB"/> <input type="button" value="⊕"/></p> <p>SELECT AND INMATE: <input type="text" value="-SELECT-"/> ▾</p> <p>SELECT A SECTION: <input type="text" value="-SELECT-"/> ▾</p> <p>SELECT A GROUP: <input type="text" value="-SELECT-"/> ▾</p> <p>ENTER A PHONE NUMBER: <input type="text"/> <input type="button" value="ADD SETTING"/></p> <p>SEARCH FOR BLACKLISTED NUMBER: <input type="text"/> <input type="button" value="SEARCH"/></p>											
<p>PHONE CALL HOURS</p> <p>EDIT PHONE INCOMING / OUTGOING HOURS</p> <p>DAY: <input type="text" value="-SELECT-"/> ▾ START TIME: <input type="text" value="11:24:00AM"/> END TIME: <input type="text" value="11:24:00AM"/> <input type="button" value="ADD SETTING"/></p> <p>MONDAY'S CALL HOURS:</p> <table border="1"> <tr> <td>MONDAY</td> <td><input type="text" value="5:00 AM"/></td> <td>TO</td> <td><input type="text" value="10:00 PM"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MONDAY</td> <td><input type="text" value="9:30 AM"/></td> <td>TO</td> <td><input type="text" value="9:30 PM"/></td> <td><input type="checkbox"/></td> </tr> </table>		MONDAY	<input type="text" value="5:00 AM"/>	TO	<input type="text" value="10:00 PM"/>	<input type="checkbox"/>	MONDAY	<input type="text" value="9:30 AM"/>	TO	<input type="text" value="9:30 PM"/>	<input type="checkbox"/>
MONDAY	<input type="text" value="5:00 AM"/>	TO	<input type="text" value="10:00 PM"/>	<input type="checkbox"/>							
MONDAY	<input type="text" value="9:30 AM"/>	TO	<input type="text" value="9:30 PM"/>	<input type="checkbox"/>							

FIG. 56

160
↓

PHONE CALL MONITORING PHONE CALL MONITORING PHONE SITE SETTINGS REPORTS > LOGOUT

INMATE
CANTEEN PHONE

TEST SITE CALL DETAIL

PHONE CALL MONITORING
PHONE CALL SETTINGS
REPORTS >

CALL TYPE: FILTER BY: START DATE END DATE PHONE NUMBER

FIG. 57

161
↓

The screenshot shows a web browser window with a title bar containing a maximize icon, a close icon, and the number '161'. The main content area is titled 'INMATE CANTEEN' and features a horizontal navigation menu with the following items: 'PHONE CALL MONITORING', 'PHONE SITE SETTINGS', 'REPORTS >', and 'LOGOUT'. Below the navigation menu is a search section titled 'TEST SITE INMATE DEPOSITS'. This section includes a 'FILTER BY:' label, a 'SELECT INMATE' button, a 'START DATE' input field, a 'CLICK ME->' button, an 'END DATE' input field, another 'CLICK ME->' button, a 'SEARCH' button, and a 'CLEAR' button. On the left side of the search section, there is a vertical menu with the following items: 'PHONE CALL MONITORING', 'PHONE CALL SETTINGS', and 'REPORTS' with a right-pointing triangle icon.

FIG. 58

157
↓

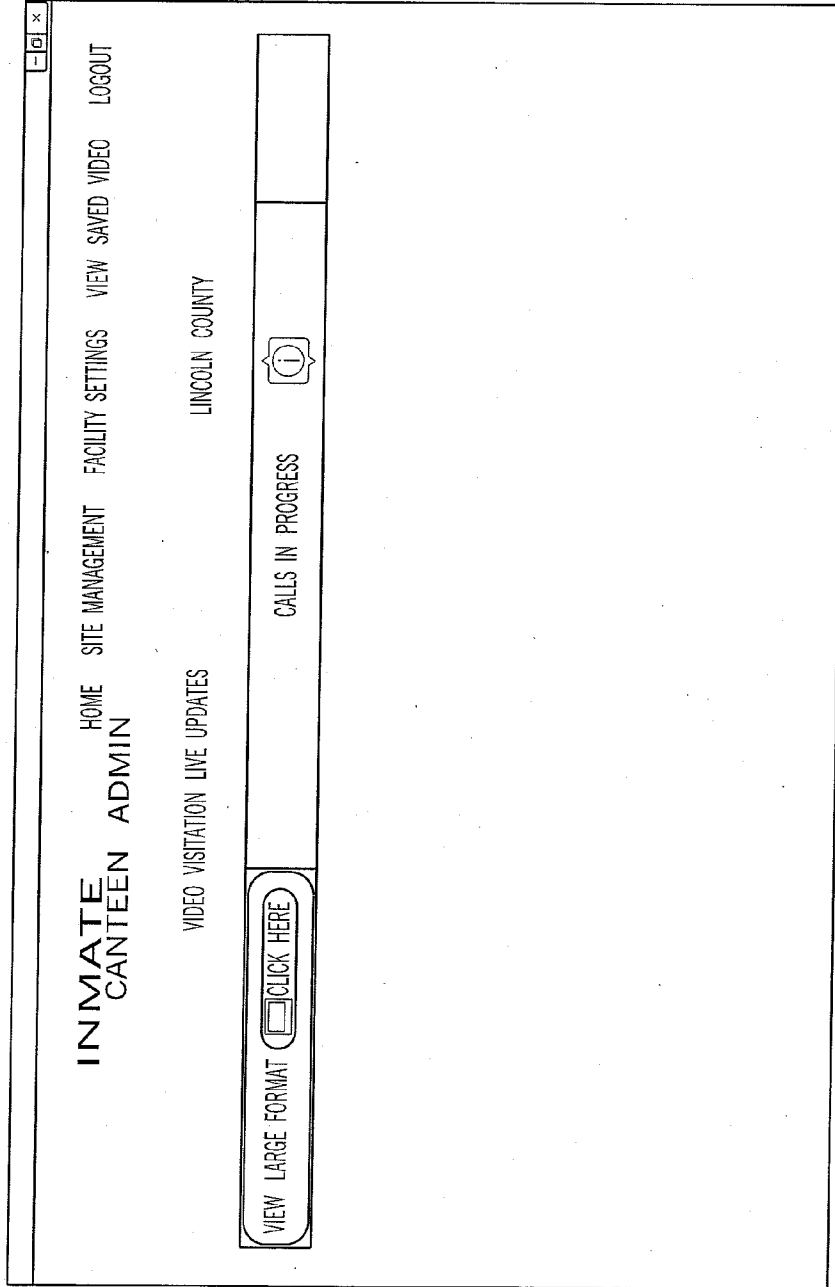


FIG. 59

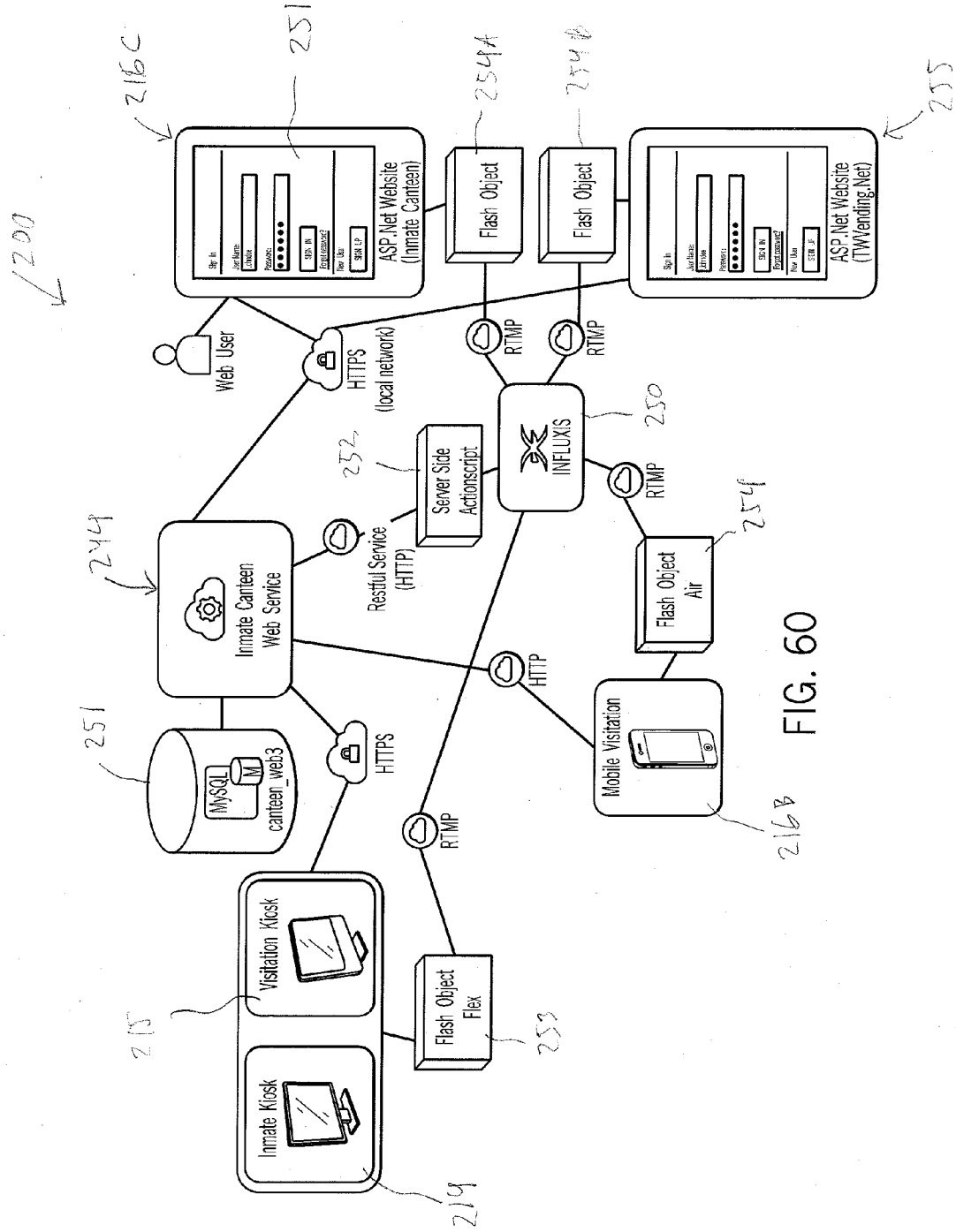


FIG. 60

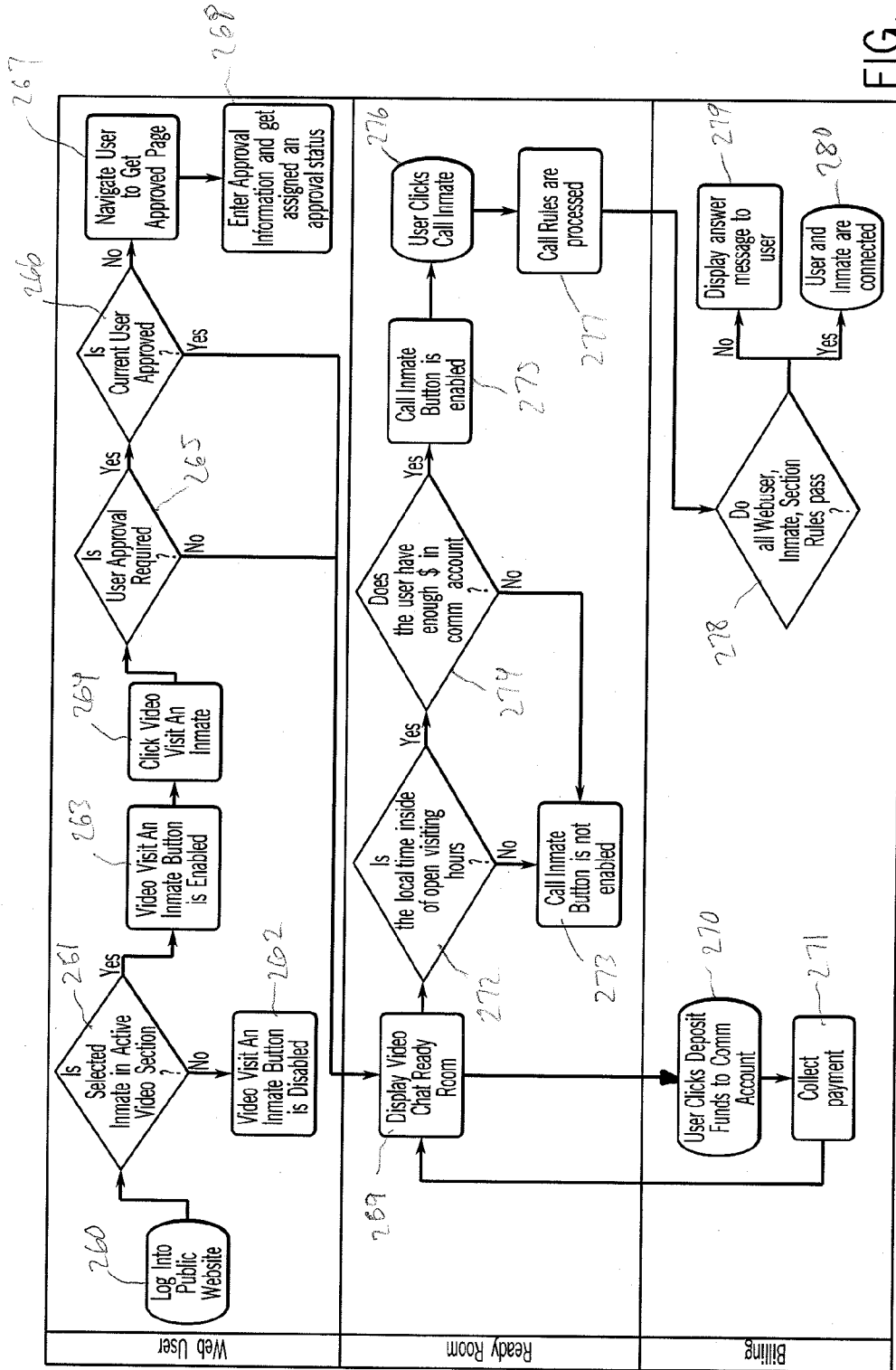


FIG. 62

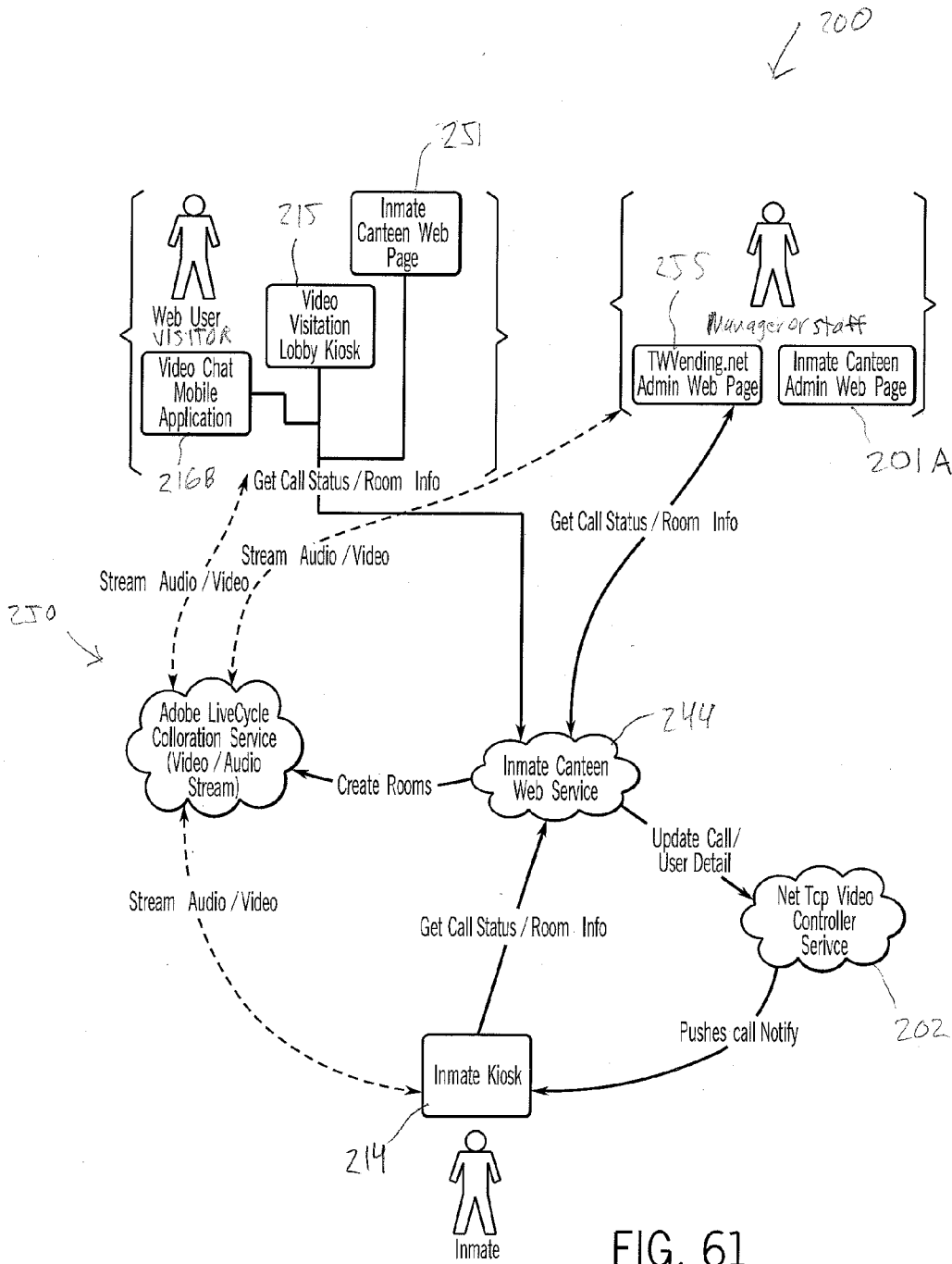


FIG. 61

020
↓

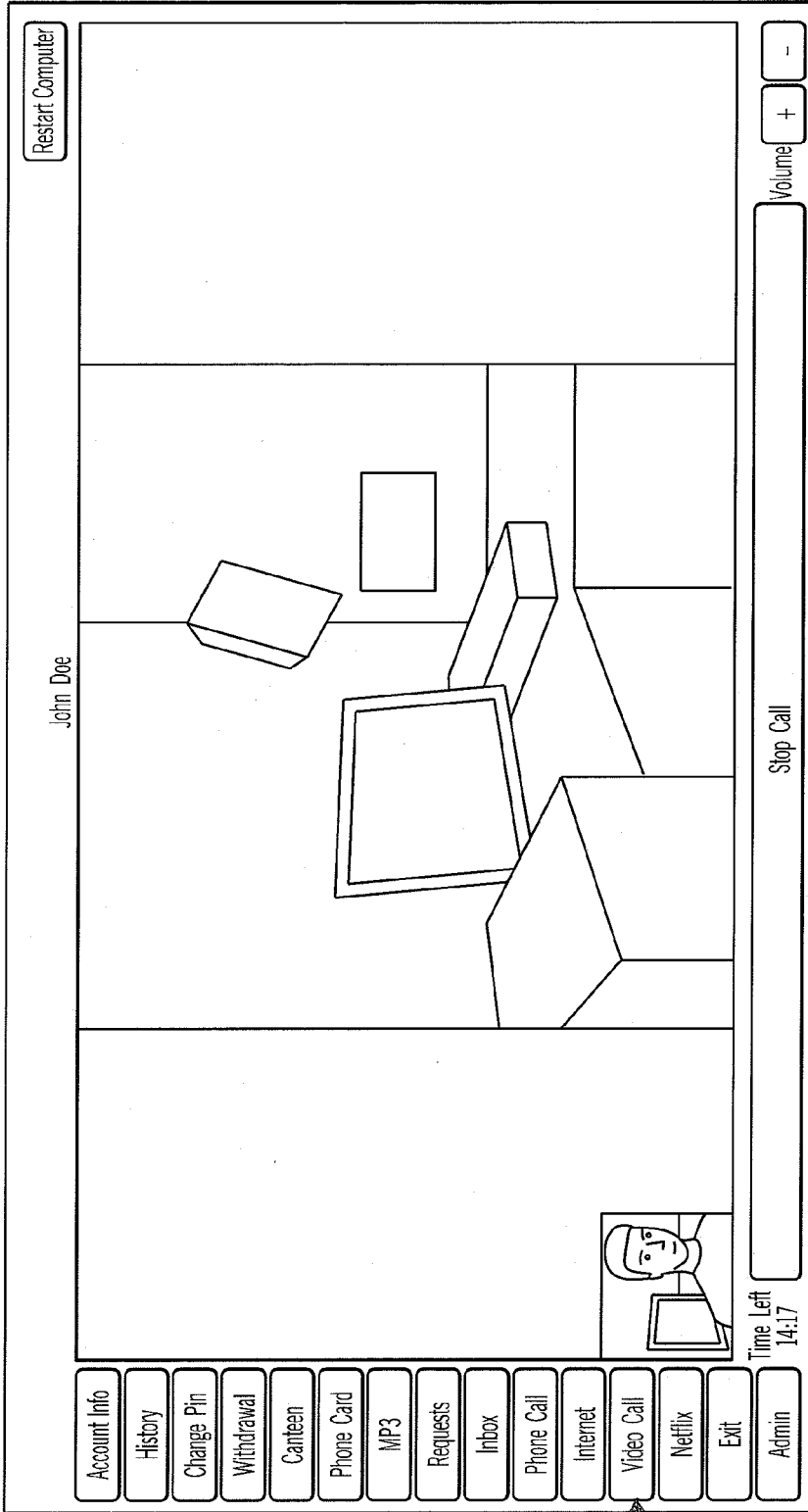


FIG. 63

291 ↓

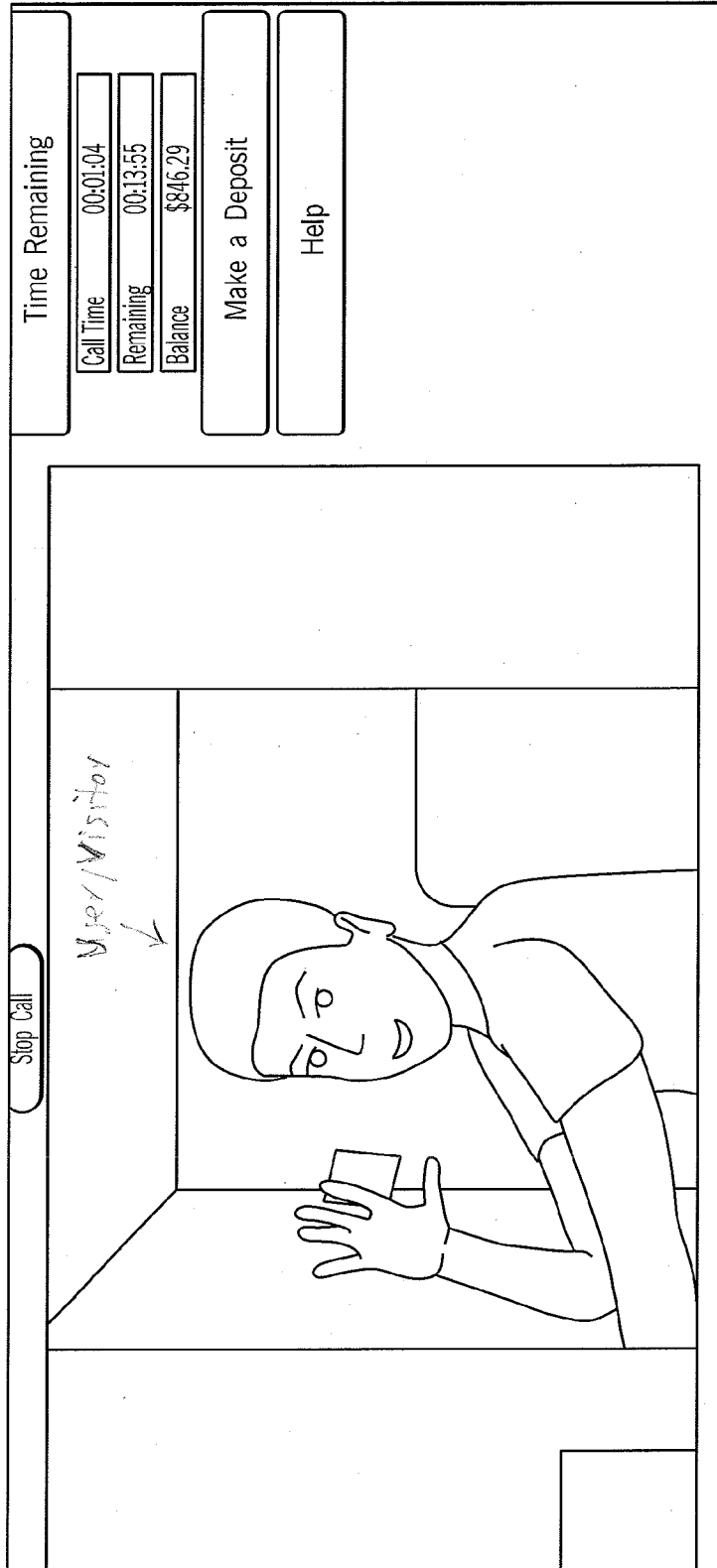


FIG. 64

4262 ↙

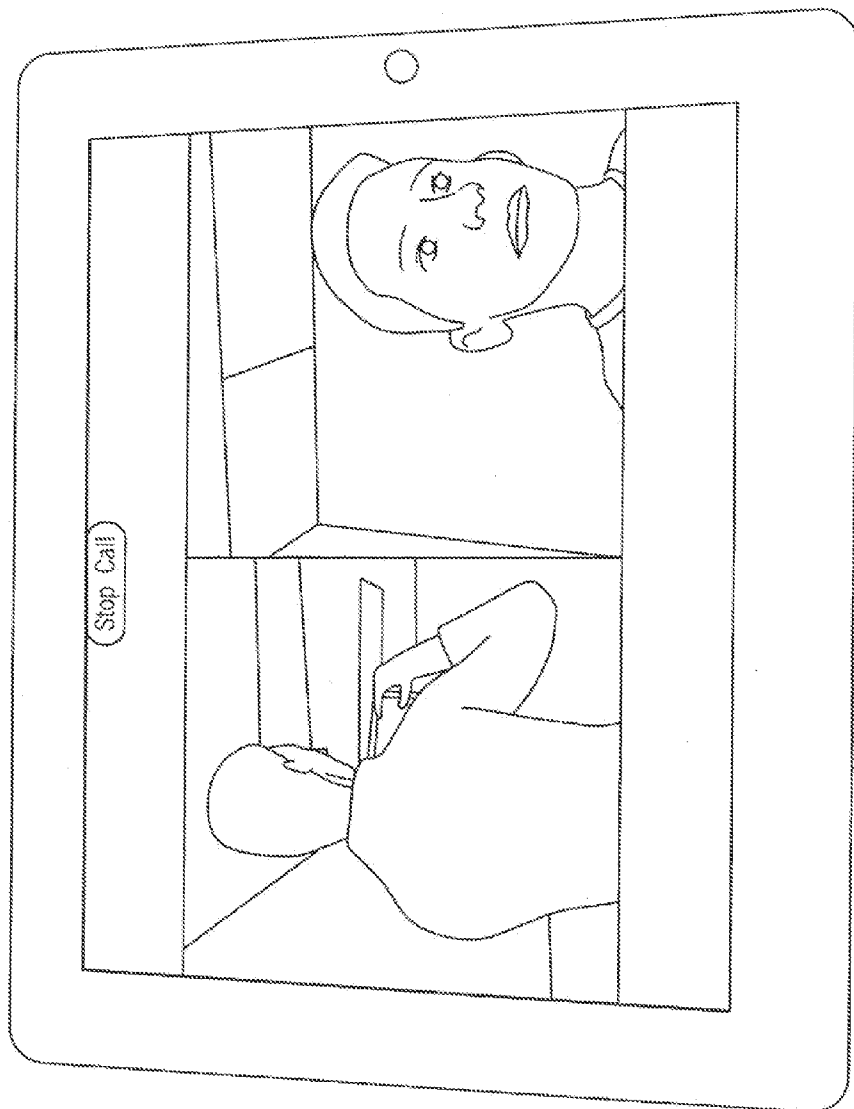


FIG. 65A

292B

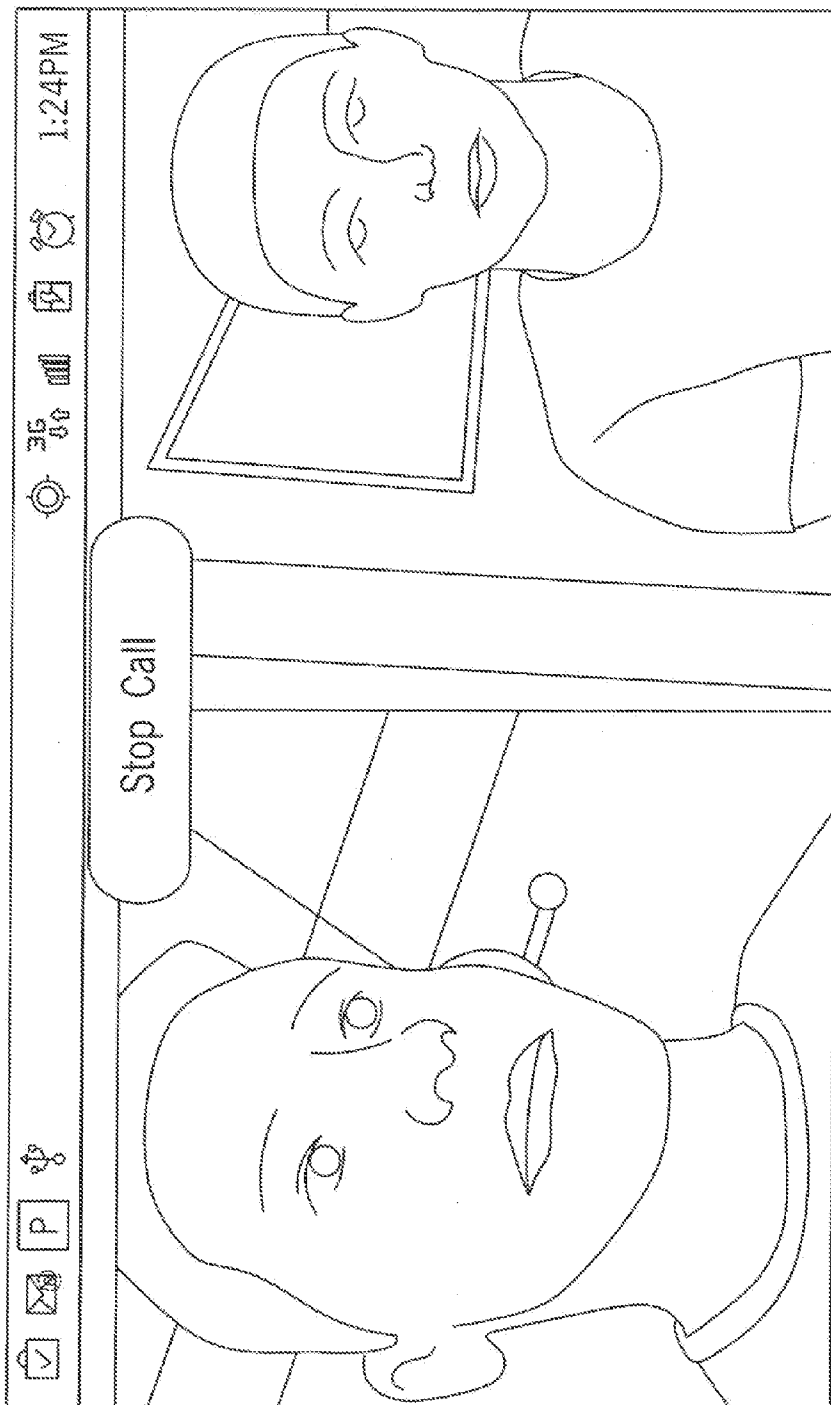
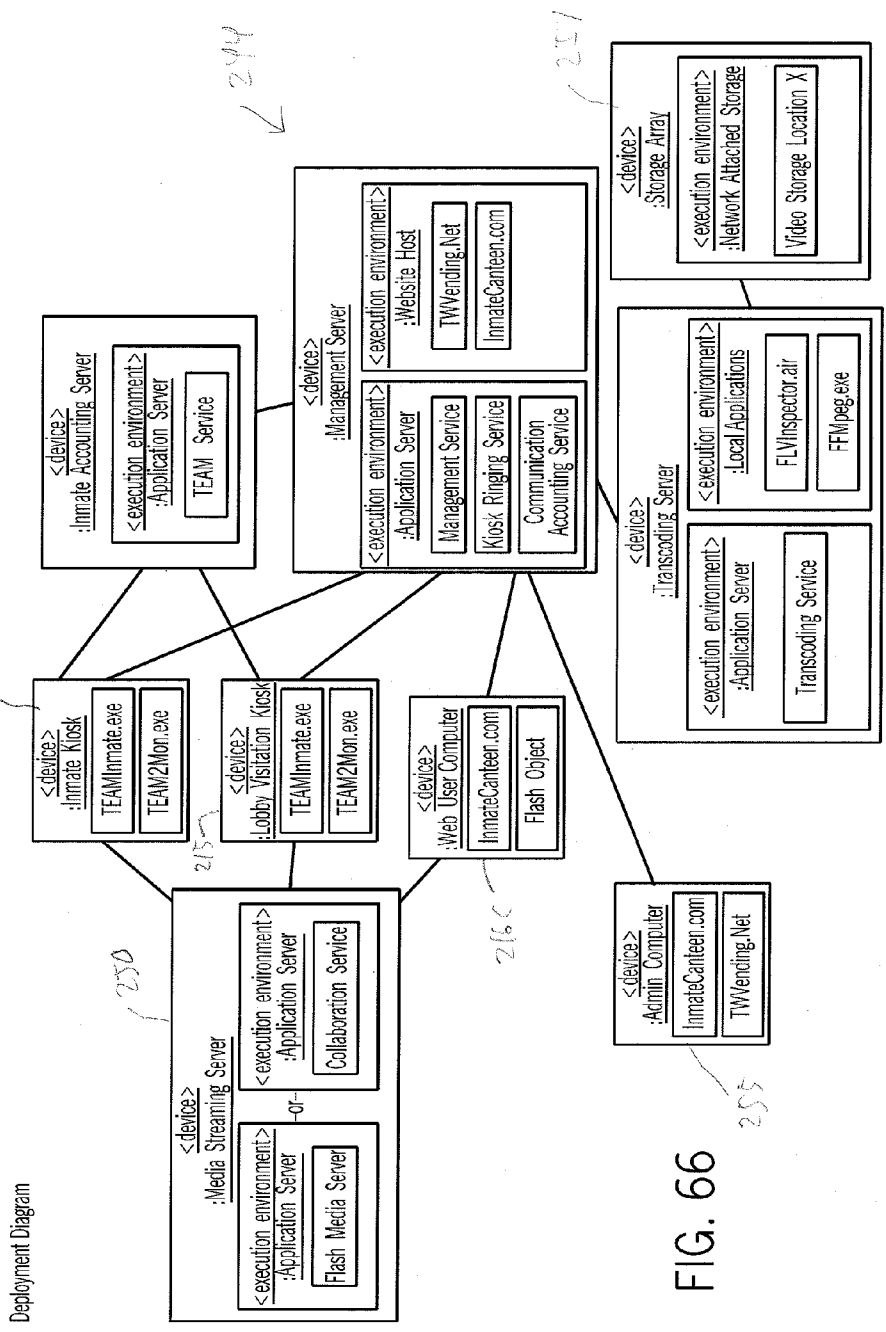


FIG. 65B



Deployment Diagram

FIG. 66

294
↓

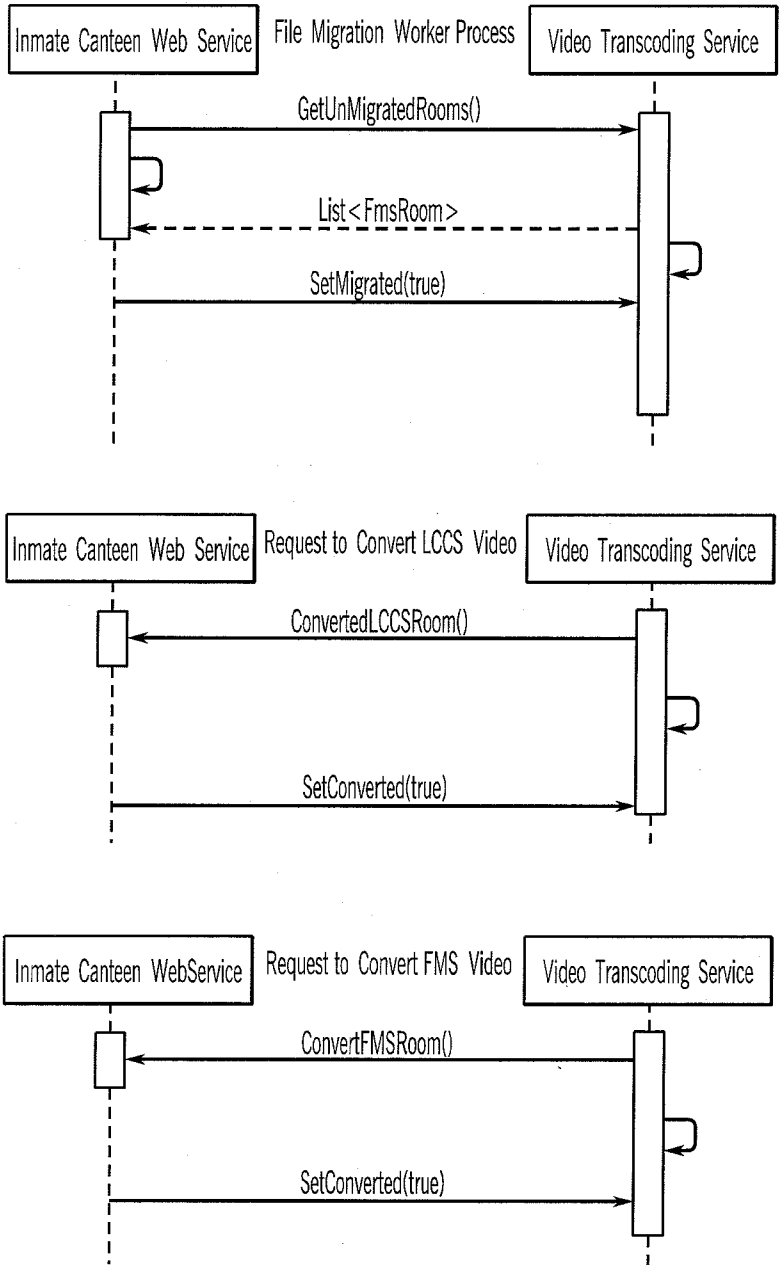


FIG. 67

295 ✓

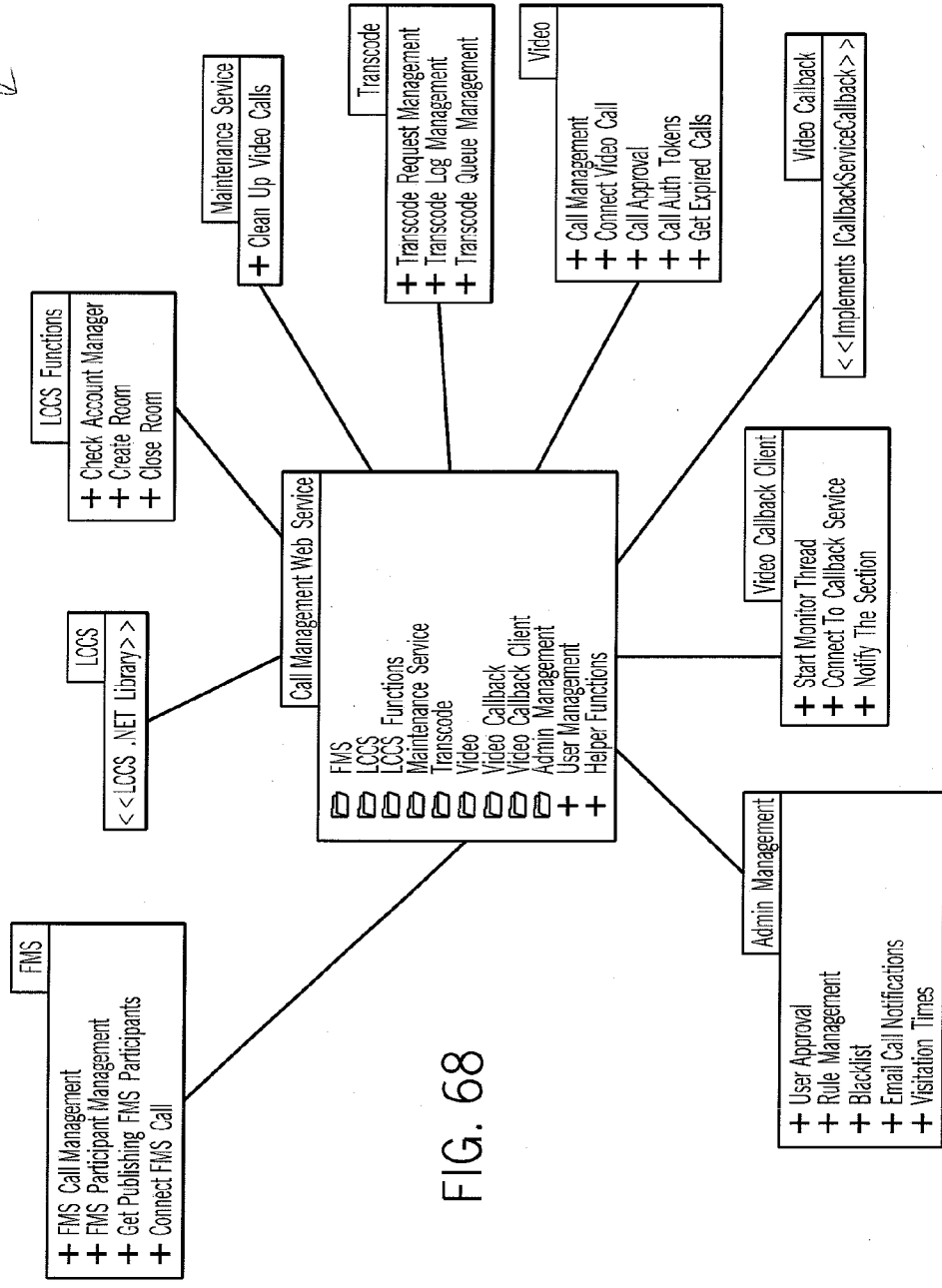


FIG. 68

296
↓

Hide Topics... **VIDEO VISITATION SITE SETTINGS** ST. CROIX COUNTY

Adding an Email Notification **Add New Notification**
 Blacklisting
 Editing Visitation Hours **Email Address:**
 Editing Connection Settings **Per Approved WebUser:**
Per Inmate:
Per Section:
Per Inmate Group:

BlackList Inmates or Webusers from Video Calls - View Full List

Select an Approved Webuser:
Select an Inmate:
Select a Section:
Select a Group:

Edit Allowed Hours to receive video calls

to

Rules for connecting video calls

Connect Calls without Admin Approval
 Allow all Webusers to visit without background check

Rules that apply per section

Active Sections for Video Visitation:

Booking
 Vid / Phone Testing

Setting Name	Start Date	
Active Sectoin: Admin	9 / 11 / 2012 8:11:06 AM	<input type="button" value="Remove"/>
Active Section: Booking	9 / 11 / 2012 8:11:06 AM	<input type="button" value="Remove"/>
Active Section: Lobby	9 / 11 / 2012 8:11:06 AM	<input type="button" value="Remove"/>

FIG. 69

✓ 297

Inmate Canteen Home My Account Logout

Converting Progress / Downloads - St. Croix County

Request Date	Call Date	Web User	Inmate	Reset	Progress	Download
12 / 13 / 2012 2:16:47 PM	12 / 6 / 2012 5:06:40 PM	TKC Support	John Doe	<input type="button" value="↩"/>	0%	<input checked="" type="checkbox"/>
12 / 5 / 2012 10:53:08 AM	11 / 30 / 2012 2:25:54 PM	TKC Support	John Doe	<input type="button" value="↩"/>	100%	<input type="checkbox"/>
12 / 5 / 2012 10:53:05 AM	11 / 16 / 2012 6:38:00 PM	TKC Support	John Doe	<input type="button" value="↩"/>	100%	<input type="checkbox"/>
⋮						
11 / 15 / 2012 8:49:22 AM	11 / 12 / 2012 3:59:19 PM	TKC Support	John Doe	<input type="button" value="↩"/>	0%	<input checked="" type="checkbox"/>

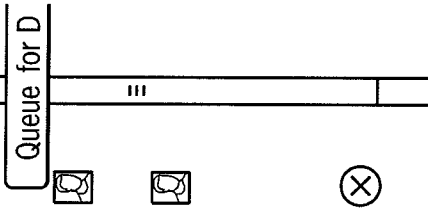


FIG. 70

298
↓

Start Date	End Date	Name	Category	Detail	Remove	Team User
7 / 11 / 2012 1:43:11 PM	12 / 31 / 9999 11:59:59 PM	DEAN, JASON	Inmate	+ Detail	<input type="checkbox"/>	tkceric
7 / 11 / 2012 1:43:11 PM	12 / 31 / 9999 11:59:59 PM	DEAN, JASON	Inmate	+ Detail	<input type="checkbox"/>	tkceric
7 / 11 / 2012 1:43:11 PM	12 / 31 / 9999 11:59:59 PM	Smith, Bob	WebUser	+ Detail	<input type="checkbox"/>	tkceric
⋮						
7 / 25 / 2012 2:16:36 PM	12 / 31 / 9999 11:59:59 PM	art, mike	WebUser	+ Detail	<input type="checkbox"/>	dgdx5
7 / 25 / 2012 2:16:36 PM	12 / 31 / 9999 11:59:59 PM	art, mike	WebUser	+ Detail	<input type="checkbox"/>	dgdx5

Inmate Canteen Admin

Home Site Management Facility Settings View Saved Video Logout

Full Blacklist List - Dakota County

FIG. 71

682
↓

Inmate Canteen Admin Home Site Management Facility Settings View Saved Video Logout

Search Video By:

Inmate Selected

Acct Code: 31 First Name: John Last Name: Doe

Video Archives					
10 / 15 / 2012 11:58:30 AM	John Doe	TKC Support	.18Mb	<input type="text" value="View Online"/>	<input type="text" value="Request Download"/>
11 / 5 / 2012 1:42:44 PM	John Doe	TKC Support	.17Mb	<input type="text" value="View Online"/>	<input type="text" value="Request Download"/>
⋮					
11 / 13 / 2012 10:34:42 AM	John Doe	TKC Support	.16Mb	<input type="text" value="View Online"/>	<input type="text" value="Request Download"/>

FIG. 72

300
↓

<p>Turnkey Corrections – St. Croix County Notification</p>	<p>Inmate Canteen</p>	<p>Video Visitation Notification</p> <p>The WebUser TKC Support and Inmate John Doe are using Inmate Canteen Video Visitation! Follow this link to view the call in progress: Click Here</p> <p>When the Session is completed, you may watch the recorded video here: Click Here.</p>	<p>You're receiving this because you have opted in to E-mail Notifications.</p>
--	---------------------------	---	---

FIG. 73

✓ 301A

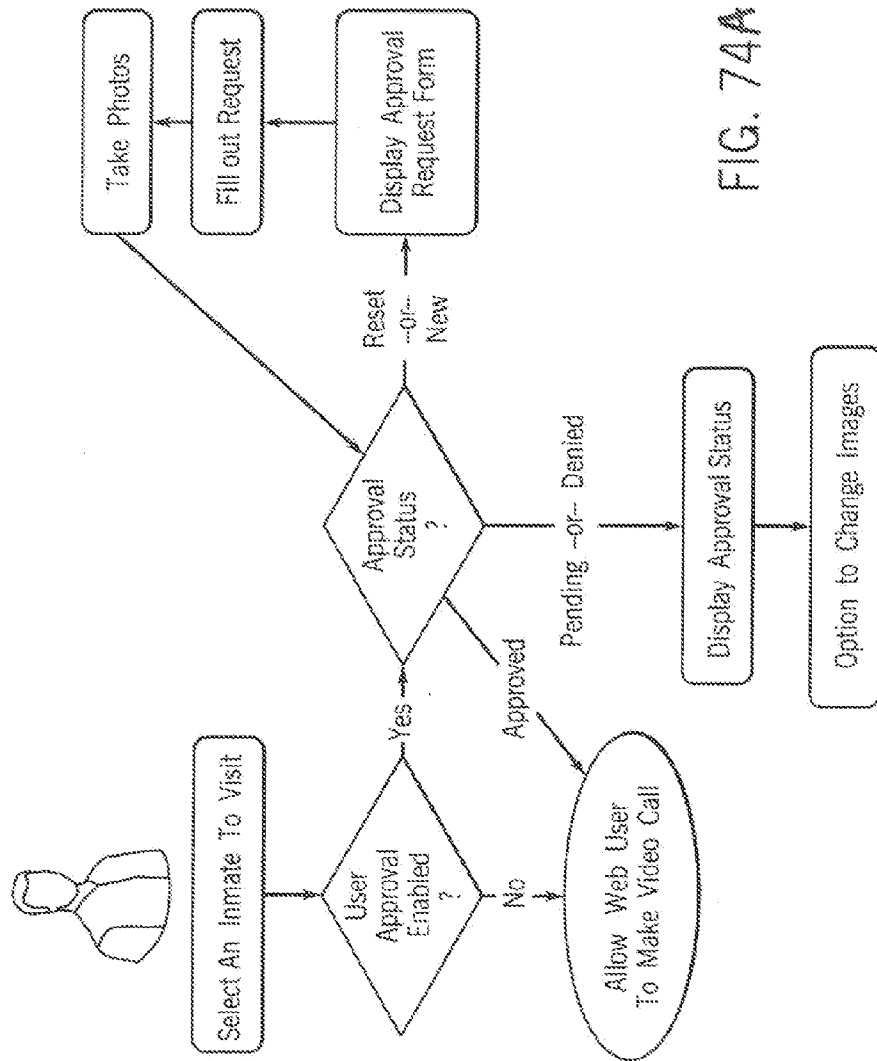


FIG. 74A

1701B

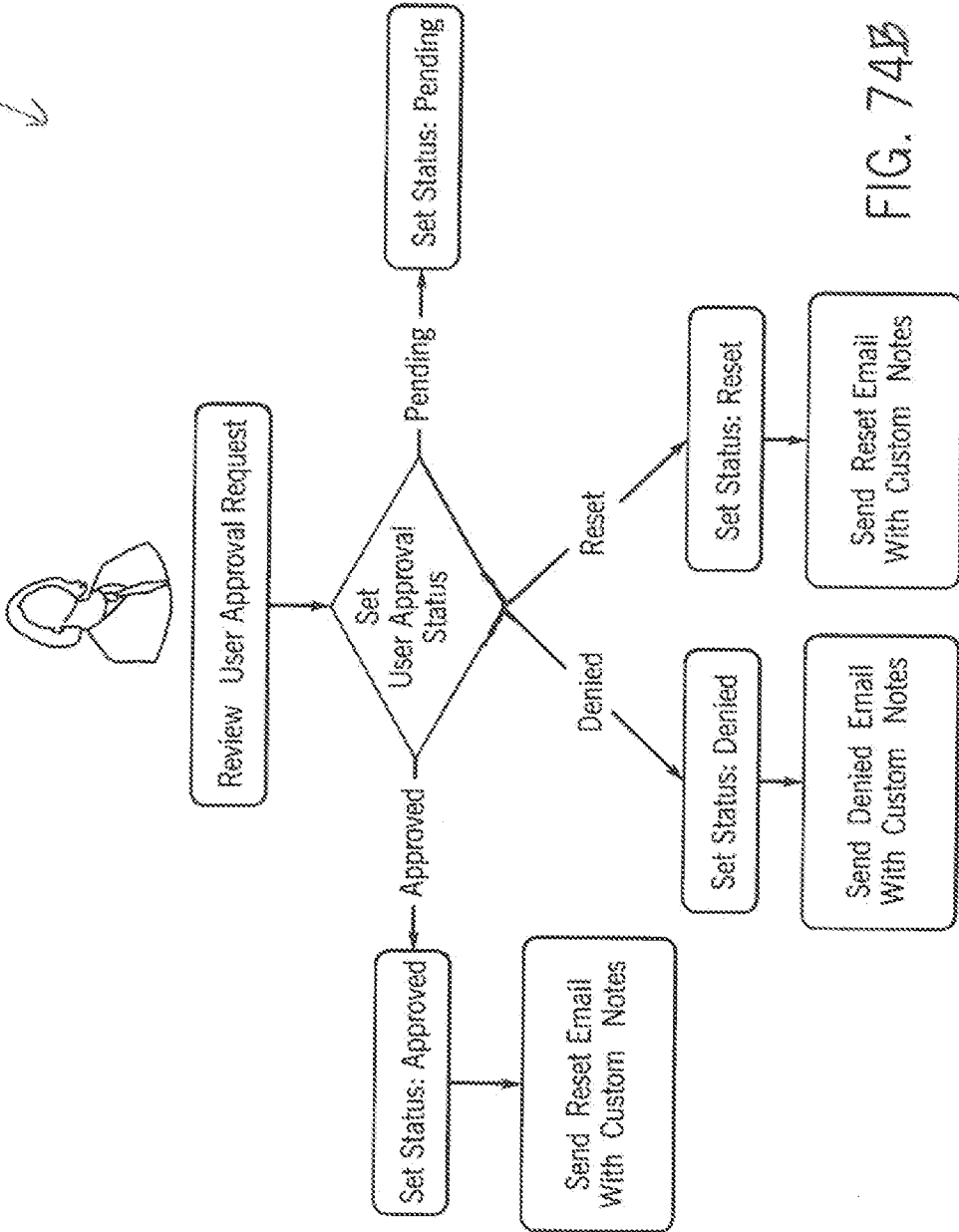


FIG. 74B

302
↓

Inmate Home My Account Audition Room Logout
Canteen Video


 Get Approved

St. Croix County requires an approval before you can visit.
Your information will be reviewed by the facility as soon as possible.

Approval Status: No Approval Submitted

VIDEO CHAT APPROVAL FORM

Facility: St. Croix County

Date of Birth: 

Drivers License Number:

Relationship To Inmate:

Address:

Address 2:

City:

Zip:

Deposit for Inmate

FIG. 75

303
↙

Inmate
Canteen Video Home My Account Audition Room Logout

VIDEO APPROVAL PHOTO

- Step 1: Place your drivers license in front of the camera.
- Step 2: When the picture is good, click the 'Snap' button.
- Step 3: Take another picture with 'Snap', or click 'Save' button to keep the image.

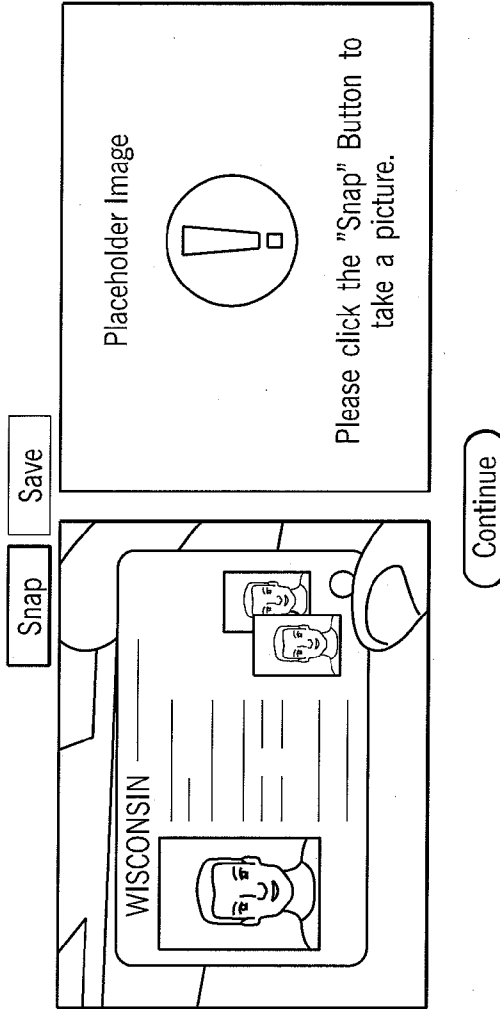


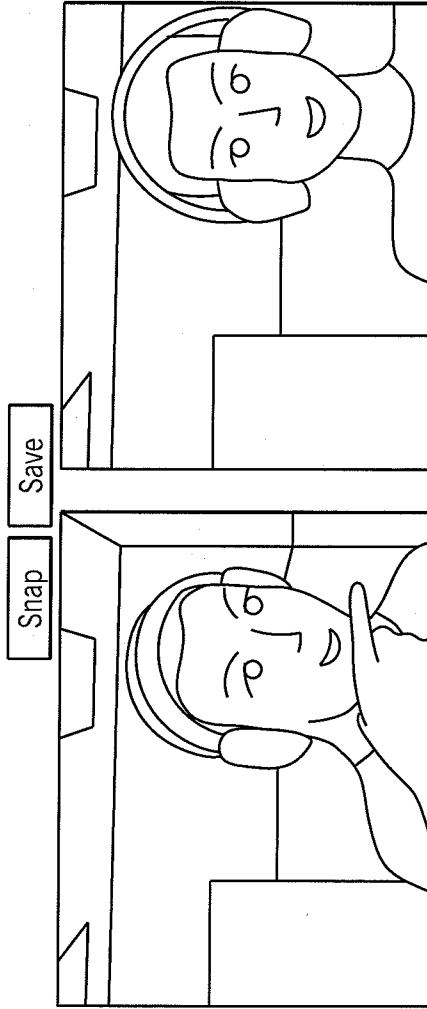
FIG. 76

304 ↓

Inmate Home My Account Audition Room Logout
Canteen Video

ALMOST THERE...WE NEED A PICTURE OF YOUR FACE!

- Step 1: Position yourself in front of the camera. Your face from the shoulders up.
- Step 2: When the picture is good, click the 'Snap' button.
- Step 3: Take another picture with 'Snap', or click 'Save' button to keep the image.




Continue

FIG. 77

205
↓

Inmate Canteen Video Home My Account Audition Room Logout

 **Get Approved**


St. Croix County requires an approval before you can visit.
Your information will be reviewed by the facility as soon as possible.


Approval Status: Pending

VIDEO CHAT APPROVAL FORM

Facility: St. Croix County

Congratulations – You have submitted a request for approval! Your current status is: Pending

 Test Video

 Deposit for Inmate


 Approval Photos

FIG. 78

306
↓

<p>Turnkey Corrections Approval Notification</p>	<p>Inmate Canteen</p>	<p>Approval Request – Denied Unfortunately, you have been denied the ability to visit online at St. Croix County. Please contact the facility for further information regarding this denial.</p>	<p>You're receiving this because you have opted in to E-mail Notifications.</p>
--	----------------------------------	---	---

FIG. 79

Inmate Canteen Video Home My Account Audition Room Logout

307

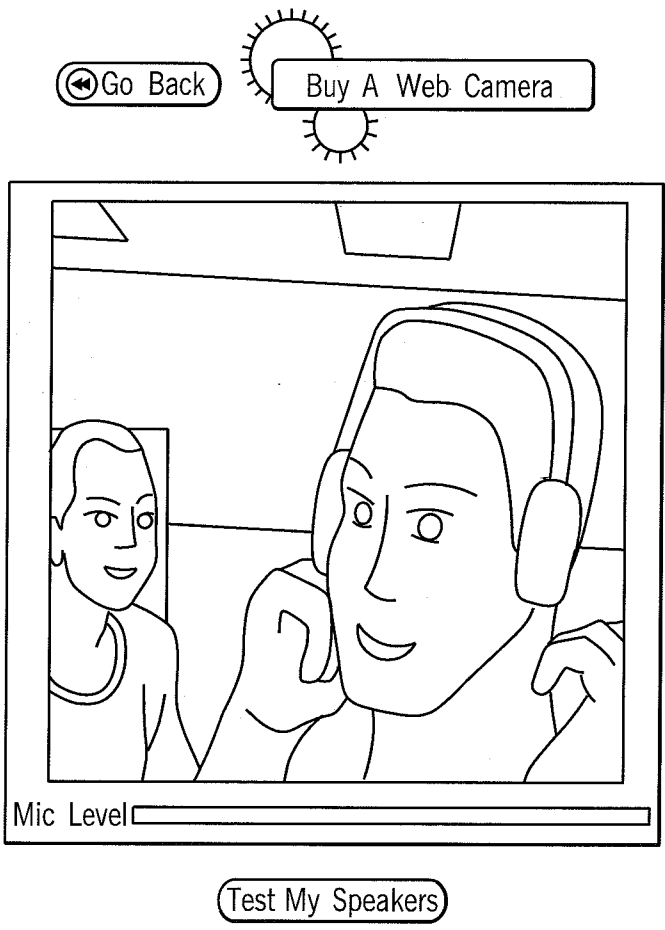


FIG. 80

308
↓

Inmate Home My Account Audition Room Logout
Canteen Video

INMATE CANTEEN
VIDEO VISITATION



JOHN DOE

Visitation Hours

Day	Time
Monday	12:02 AM to 11:58 PM
Tuesday	12:02 AM to 11:58 PM
Wednesday	12:02 AM to 11:58 PM
Thursday	12:02 AM to 11:58 PM
Friday	12:02 AM to 11:58 PM
Saturday	12:02 AM to 11:58 PM
Sunday	12:02 AM to 11:58 PM

Current Status
Open

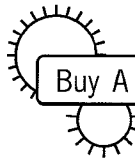
I agree to the video agreement

Call Inmate

\$0.35 /min -- may change per facility



Communication Account
Balance: \$856.79



Buy A Web Camera

ADD FUNDS TO YOUR ACCOUNT BALANCE

Please Select a Credit Card:

Please Enter Deposit Amount: \$ + \$8.00 Fee

I agree to the video agreement



Questions or comments? Please call 715-386-5700

FIG. 81

309

Inmate Home My Account Audition Room Logout
Canteen Video

INMATE CANTEEN
VIDEO VISITATION



JOHN DOE

Visitation Hours

Day	Time
Monday	12:02 AM to 11:58 PM
Tuesday	12:02 AM to 11:58 PM
Wednesday	12:02 AM to 11:58 PM
	58 PM
	58 PM
	58 PM
	58 PM

Current Status
Open

ATTEMPTING TO CALL INMATE
2:46

⋮

Cancel

The kiosk inside of the facility is ringing.
The Inmate will not have access to this kiosk at all times.

The inmate may not be available for the following reasons:

- The inmate is in Lockdown
- The inmate is in Recreation
- The inmate is in Programs

Com Camera

ADD FUNDS TO YOUR ACCOUNT BALANCE

Please Select a Credit Card:

Please Enter Deposit Amount: \$ + \$8.00 Fee

I agree to the video agreement



Questions or comments? Please call 715-386-5700

FIG. 82

310
↓

Inmate Canteen Admin		Home	Site Management	Facility Settings	View Saved Video	Logout
Full User Approval List – St. Croix County						
Date	Name	Status	Suggested Inmate	Detail	Reset	Approve Deny Pending
12 / 7 / 2012 3:23:06 PM	Ge Link	Denied	Doe, John	+ Detail	<input type="checkbox"/>	<input checked="" type="radio"/> <input type="checkbox"/>
9 / 28 / 2012 8:02:38 AM	Al Lance	Pending	Doe, John	+ Detail	<input type="checkbox"/>	<input checked="" type="radio"/> <input type="checkbox"/>
9 / 13 / 2012 1:39:56 PM	TKC Support	Approved		+ Detail	<input type="checkbox"/>	<input checked="" type="radio"/> <input type="checkbox"/>
<div style="display: flex; justify-content: space-between;"> <div>Home Lookup Receipt FAQ Contact</div> <div>Login Sign Up My Account</div> </div>						

FIG. 83

7.311
↓

Inmate Canteen Admin		Approval Detail		Logout
Date	Name	Status	View Saved Video	Deny
12 / 7 / 2012 3:23:06 PM	Ge Link	Denied	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9 / 28 / 2012 8:02:38 AM	Al Lance	Pending	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9 / 13 / 2012 1:39:56 PM	TKC Support	Approved	<input checked="" type="checkbox"/>	<input type="checkbox"/>

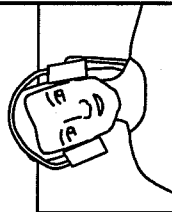
Name: Ge Link Birthdate: 05-31-1985 Age: 27 WISCONSIN  Email: John.Doe@TK.com Phone: (715) 000-0000 Relationship: Father DL#: B0000000 Suggested Inmate: Doe, John Address: 123 Corellia St Internal Notes: (Optional) Notes for Webuser: (Optional) Reason if Denied: Other (See Notes)	[Reset] [Approve] [Deny] [Cancel] [Approve]
--	---

FIG. 84

✓ 312

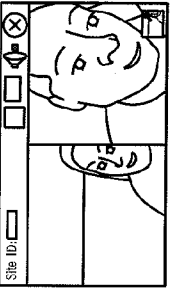
VIDEO VISITATION LIVE UPDATES		<input type="checkbox"/> County
View large Format <input type="checkbox"/> Click Here	Calls in Progress <input checked="" type="radio"/>	
		
Home Lookup Receipt FAQ Contact		Login Sign Up My Account

FIG. 85

313
↓

TWWENDING.NET					tkeric [Log Out]			
Home	Email Video	Visitation Video	About	ACT	Seed	Submit Ticket	Application	Support Portal
Test Video	Monthly Credit Card	View All Video	View	Online Kiosks	Credit Card Errors	Phone Directory		
Online Transaction Info	Canteen Items	Auto Removed	Recent Video	Calls	Phone Cards	Email Sales		
<u>Site Name</u>	<u>Section</u>	<u>Station</u>	<u>Call Time</u>		<u>Play</u>			
Dakota County	8100	T10-375	12 / 8 / 2012	9:57:14 PM	<input type="checkbox"/>			
Dakota County	9100	T12-580	12 / 8 / 2012	7:02:59 PM	<input type="checkbox"/>			
⋮								
Daviess-Dekalb County	C Tank	T10-303	12 / 8 / 2012	10:27:12 PM	<input type="checkbox"/>			

FIG. 86

314

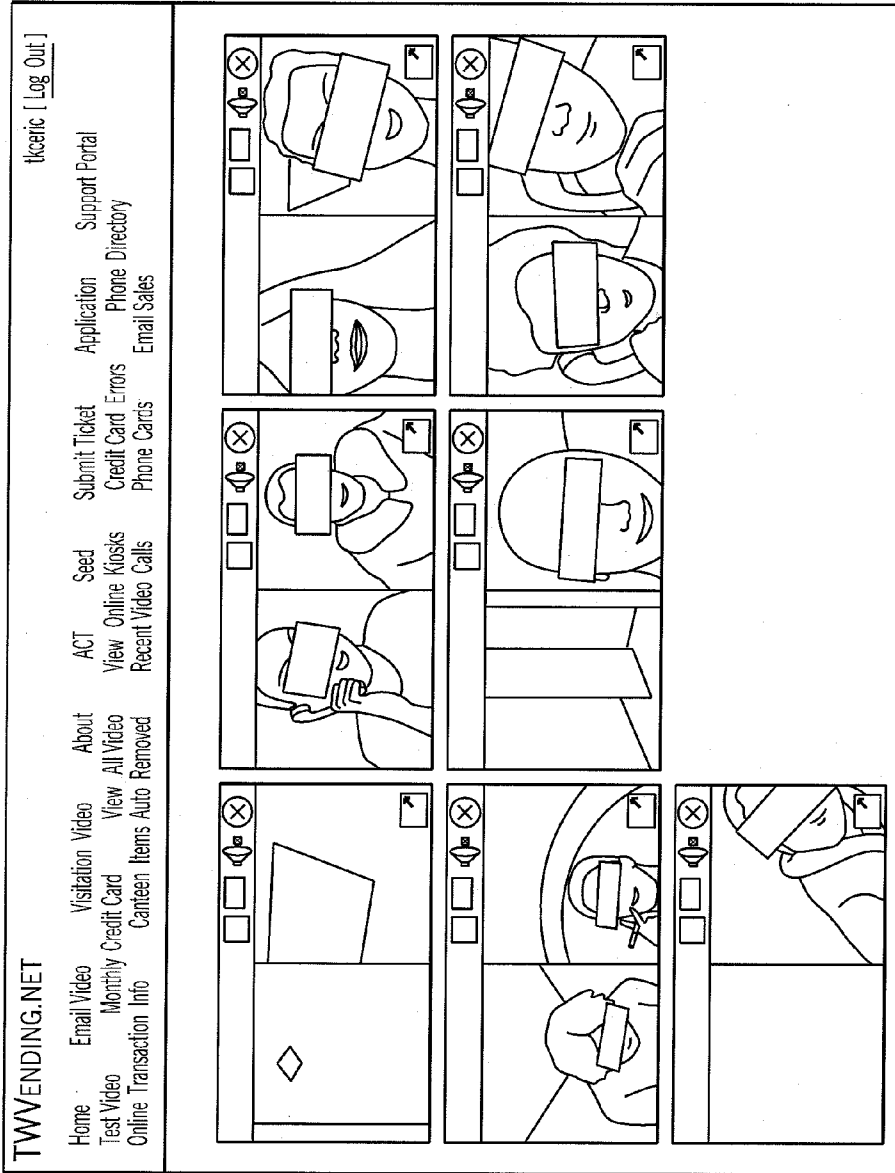


FIG. 87

**AUDIO-VIDEO REMOTE VISITATION
TELECOMMUNICATIONS TECHNOLOGY**

**CROSS REFERENCE TO RELATED
APPLICATIONS, IF ANY**

[0001] This application claims the benefit under 35 U.S.C. §119(e) of co-pending U.S. Provisional Patent Application Ser. No. 61/848,148, filed Dec. 21, 2012, which is hereby incorporated by reference.

37 C.F.R. §1.71(E) AUTHORIZATION

[0002] A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the US Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

**STATEMENT REGARDING FEDERALLY
SPONSORED RESEARCH OR DEVELOPMENT**

[0003] Not applicable.

**REFERENCE TO A MICROFICHE APPENDIX, IF
ANY**

[0004] Not applicable.

BACKGROUND OF THE INVENTION

[0005] 1. Field of the Invention

[0006] The present invention relates, generally, to telecommunications systems, apparatus and methods. Particularly, the invention relates to a telecommunications system for use in a secure facility such as a jail, prison or the like. Most particularly, the invention provides audio-visual telecommunications services for inmates of a secure facility with respect to family, friends and others.

[0007] 2. Background Information

[0008] Existing technology in this field is believed to have significant limitations and shortcomings.

[0009] All US patents and patent applications, and all other published documents mentioned anywhere in this application are incorporated by reference in their entirety.

BRIEF SUMMARY OF THE INVENTION

[0010] The present invention provides a telecommunications apparatus and methods which are practical, reliable, secure, accurate and efficient, and which are believed to constitute an improvement over the background technology.

[0011] In one aspect, the invention relates to systems, devices and methods for providing telecommunications, audio-visual communication and visitation, email, other messaging, financial services, vending, and commissary or canteen services for inmates of a secure facility with respect to family, friends and others.

[0012] In one aspect, the invention provides a system for providing telecommunications between a resident inside a secure facility and at least one person outside the secure facility, and for management of such telecommunications by an administrator of the secure facility, comprising: a phone server adapted to be communicatively connected to an external service provider; a monitoring station communicatively connected to the phone server: an account manager server

communicatively connected to the phone server, and at least one telecommunications device disposed at the secure facility for use by the resident and being communicatively connected to the phone server.

[0013] In another aspect, the invention provides a method for telecommunicating between a resident inside a secure facility and at least one person outside the secure facility, and for management of such telecommunication by an administrator of the secure facility, comprising the step of making an incoming voice call from at least one person outside the secure facility to the resident inside the secure facility.

[0014] The secure facility is an institution such as a jail, a detention center, a short term corrections facility, a penitentiary, a prison and a mental health institution. The resident is a person such as an inmate, a prisoner and a patient. The administrator is a person such as a sheriff, an officer, a guard, a warden, a jailer, and a mental health worker. The at least one person outside the secure facility is a person such as a family member, a friend, an acquaintance, and an attorney. The telecommunications between the resident of the secure facility and the at least one person outside the secure facility is a communication mode such as voice, SMS text, IM, email, and/or audio-visual. Management of telecommunications is selected from the group of activities consisting of monitoring, recording, controlling and documenting communications and transactions of the resident. Controlling activities may involve call blocking, blacklisting, email notification, section/station setting, attorney call status, and/or deferred call status. The at least one telecommunications device disposed at the secure facility is a device such as a land line telephone, a mobile telephone, a personal computer (PC), and a telecommunications kiosk. And, the person outside the secure facility communicatively connects with the system by a device adapted to connect to the phone server selected from the group of devices consisting of a land line telephone, a mobile telephone, a smart phone, a PC and a telecommunications kiosk.

[0015] The person outside the secure facility is further able to electronically deposit funds or credits to an account of the resident at the secure facility. The account funding products and services may be voice communications, audio-visual communications, vending drink, snacks and food items, and commissary items such as personal care items, books, videos, clothing and apparel, and blankets. The administrator is further able to monitor, audit and manage the account of the resident.

[0016] The present invention is believed to involve novel elements, combined in novel ways to yield more than predictable results. The problems solved by the invention were not fully recognized in the prior art.

[0017] The aspects, features, advantages, benefits and objects of the invention will become clear to those skilled in the art by reference to the following description, claims and drawings.

**BRIEF DESCRIPTION OF THE SEVERAL
VIEWS OF THE DRAWING**

[0018] FIG. 1 is a diagram showing an embodiment of the system of the present invention for providing telecommunications, email, other messaging, financial services, vending, and commissary or canteen services for inmates of a secure facility with respect to family, friends and others.

[0019] FIG. 2 is a perspective view of an embodiment of an inmate kiosk of the system of the present invention.

- [0020] FIG. 3 is another perspective view of the kiosk.
- [0021] FIG. 4 is diagram of a prior art telecommunications system.
- [0022] FIG. 5 is a more detailed diagram of the system of the invention, including the interconnection of a phone server and an account manager server, and a monitoring station of the system.
- [0023] FIG. 6 a diagram showing an embodiment of the communicative interconnection of the phone server with elements of the system which are disposed inside the secure facility.
- [0024] FIG. 7 is a diagram showing an embodiment of the communicative interconnections of the phone server with elements of the system which are preferably disposed outside the secure facility.
- [0025] FIG. 8A is a flowchart of an embodiment of an outgoing call process of the invention.
- [0026] FIG. 8B is a flowchart of an embodiment of an incoming call process of the invention.
- [0027] FIG. 9 is a chart of an embodiment of the user screens of the administrator controls and tools of the system.
- [0028] FIG. 10 is a chart of an embodiment of the user screens of the inmate management tools of the system.
- [0029] FIG. 11 is a chart of an embodiment of the user screens of the family/friend management tools of the system.
- [0030] FIGS. 12 to 24 show embodiments of user screens of the administrator controls and tools of the system as outlined in the Chart of FIG. 9, with FIG. 12 illustrating a Login interface.
- [0031] FIG. 13 discloses a chat initiation screen.
- [0032] FIG. 14 shows a Create Inmate Account screen.
- [0033] FIG. 15 also shows a Create Account screen.
- [0034] FIG. 16 discloses a Deposit Funds to Inmate Account screen.
- [0035] FIG. 17 illustrates a Withdraw Funds from Inmate Account screen.
- [0036] FIG. 18 shows a Charge (Site Charge) An Inmate's Account for Money Owed to a Vendor screen.
- [0037] FIG. 19 discloses a Inmate History Report user interface.
- [0038] FIG. 20 shows a Inmate Request screen.
- [0039] FIG. 21 shows an Undo/Correction Wizard interface.
- [0040] FIG. 22 shows a submit a ticket screen.
- [0041] FIG. 23 shows a remote support screen.
- [0042] FIG. 24 shows a live chat screen.
- [0043] FIGS. 25-37 show further administrator control functions and user interfaces, with FIG. 25 illustrating a Close Inmate Account screen.
- [0044] FIG. 26 shows an Assign Inmate Smart Card screen.
- [0045] FIG. 27 discloses a Discipline Inmate Account interface.
- [0046] FIG. 28 illustrates an Edit Inmate Account screen.
- [0047] FIG. 29 shows an Inmate Requests—Old screen.
- [0048] FIG. 30 shows a View Inmate Canteen Order screen.
- [0049] FIG. 31 shows a Bank Deposit interface.
- [0050] FIG. 32 shows a Deposit To Vendor screen.
- [0051] FIG. 33 shows a Pay Vendor user interface.
- [0052] FIG. 34 shows a Batch Order screen.
- [0053] FIG. 35 shows a Manage Site Canteen System interface.
- [0054] FIG. 36 shows a Manage Warehouse screen.
- [0055] FIG. 37 discloses a Manage Warehouse Order System user interface.
- [0056] FIGS. 38 to 50 show embodiments of user screens of the inmate management tools of the system outlined in the Chart of FIG. 10, with FIG. 38 illustrating the login screen.
- [0057] FIG. 39 shows an example of the Account Information screen.
- [0058] FIG. 40 shows an embodiment of the Account History screen.
- [0059] FIG. 41 shows a Withdrawal Information screen.
- [0060] FIG. 42 shows a Canteen Information screen with Current Order and Past Order selections.
- [0061] FIG. 43 shows a further Canteen Information Screen Current Order screen.
- [0062] FIG. 44 shows a Phone Card screen.
- [0063] FIG. 45 shows an MP3 screen.
- [0064] FIG. 46 shows a Requests screen.
- [0065] FIG. 47 shows an Inbox 141 screen
- [0066] FIG. 48 shows a Phone Call screen.
- [0067] FIG. 49 shows a Voice Mail screen.
- [0068] FIG. 50 shows a preferred embodiment of the Phone Account screen.
- [0069] FIGS. 51 to 59 show embodiments of user screens of the family/friend management tools of the system, as outlined in the Chart of FIG. 11, with FIG. 51 showing a login screen.
- [0070] FIG. 52 shows an embodiment of the New Account Sign Up Screen.
- [0071] FIG. 53 shows an admin screen for user name and password.
- [0072] FIG. 54 shows a facility selection screen.
- [0073] FIG. 55 shows an example interface for phone administration.
- [0074] FIG. 56 shows a phone call setting screen.
- [0075] FIG. 57 illustrates a call detail screen.
- [0076] FIG. 58 discloses an inmate deposit user interface.
- [0077] FIG. 59 shows a video visitation admin screen.
- [0078] FIG. 60 illustrates an embodiment of the system of the invention from the perspective of the audio-visual video visitation hardware and software elements of the invention.
- [0079] FIG. 61 illustrates an embodiment of the video visitation method of the invention.
- [0080] FIG. 62 is a flow chart of an embodiment of another aspect of the method of the invention.
- [0081] FIG. 63 is a screen shot showing an embodiment of the user interface and display of a video visitation kiosk of the invention.
- [0082] FIG. 64 is a screen shot showing an embodiment of the user interface and display of a video visitation from the perspective of an outside user family or friend using a personal computer.
- [0083] FIG. 65A is a screen shots showing an embodiment of the user interface and display of a video visitation from the perspective of an outside user family or friend using a mobile device such as an iPad or Android device.
- [0084] FIG. 65B is another screen shot showing an embodiment of the user interface and display of a video visitation from the perspective of an outside user family or friend using a mobile device such as an iPad or Android device.
- [0085] FIG. 66 is a diagram of an embodiment of the deployment of devices in the video visitation system of the invention.
- [0086] FIG. 67 is a flow chart of an embodiment of the file migration worker process of the invention.
- [0087] FIG. 68 is a diagram of an embodiment of a call management web service package of the invention.

[0088] FIG. 69 is a web shot of an embodiment of a user interface for a secure facility administrator for controlling video visitation settings for the system.

[0089] FIG. 70 is a web shot of an embodiment of a user interface for an administrator for listing and monitoring downloads for the system.

[0090] FIG. 71 is a web shot of an embodiment of a user interface for an administrator for listing and controlling blacklist information for the system.

[0091] FIG. 72 is a web shot of an embodiment of a user interface for an administrator for listing and controlling inmate video visitations for the system.

[0092] FIG. 73 is a web shot of an embodiment of an email notification for an administrator that a particular inmate has used video visitation for the system.

[0093] FIG. 74A is an activity diagram of an embodiment of a portion of a method of approving video visitation for a user.

[0094] FIG. 74B is an activity diagram of a further portion of the method.

[0095] FIG. 75 is a web shot of an embodiment of a user interface for a first step in the method of obtaining approval.

[0096] FIG. 76 is a web shot of an embodiment of a user interface for a second or subsequent step in the method of obtaining approval.

[0097] FIG. 77 is a web shot of an embodiment of a user interface for a third or subsequent step in the method of obtaining approval.

[0098] FIG. 78 is a web shot of an embodiment of a user interface for a fourth or subsequent step in the method of obtaining approval.

[0099] FIG. 79 is a web shot of an embodiment of a user interface for a final step in the method of obtaining approval, wherein a request is denied or approved.

[0100] FIG. 80 is a web shot of an embodiment of a user interface for an optional audition room feature in the method of obtaining approval.

[0101] FIG. 81 is a web shot of an embodiment of a user interface for a first step in the method of making a video visitation call by an outside family member or friend.

[0102] FIG. 82 is a web shot of an embodiment of a user interface for a second or subsequent step in the method of obtaining approval, wherein the video visitation caller is waiting for the video visitation call to connect with the inmate. Upon connection, a video visitation screen appears as for example is shown in FIG. 65 or 65.

[0103] FIG. 83 is a web shot of an embodiment of a user interface for an administrator who is manually approving requests for video visitation rights for a caller.

[0104] FIG. 84 is a web shot of an embodiment of a subsequent user interface for an administrator who is manually approving requests for video visitation rights for a caller.

[0105] FIG. 85 is a web shot of an embodiment of a user interface for a system administrator for monitoring live updates of video visitation calls in progress in the overall system.

[0106] FIG. 86 is a web shot of an embodiment of a user interface for a system administrator for monitoring and controlling video visitation calls in the overall system.

[0107] FIG. 87 is a web shot of an embodiment of a user interface for a system administrator for monitoring plural video visitation calls in progress in the overall system.

DETAILED DESCRIPTION

[0108] The invention provides systems, devices and methods for providing audio-visual telecommunications for inmates of a secure facility (i.e. a jail or prison) with respect to family, friends and others. The system optionally provides a Phone System, email, other messaging, financial services, vending, and commissary or canteen services in the secure facility environment.

[0109] FIG. 1 shows an embodiment of the system 10 of the invention for providing communications (including phone communications and audio-visual video visitation), financial transactions and delivery of goods and services between an inmate 11 and family member 12 at the inmate facility (such as the booking area or the lobby of the jail) or remote from the facility (such as a home or work location), and which can be monitored and controlled by a facility (jail) administrator(s) 13. The system 10 provides telecommunications (voice, text, email, and in some cases audiovisual) between a person (for example an inmate) inside a closed facility (for example a jail, work house, detention center, prison or the like) with one or more persons (for example family, spouse, children, fiends or the like) outside the facility (for example in the lobby of the facility, booking station of the facility, or completely outside the facility such as home, work or public place either in the community of the facility or even outside the city, state or country of the facility). The inmate uses a kiosk 14, an example embodiment of which is shown in FIGS. 2 and 3 (including a housing 20, a receiver/transmitter handset 21, a touch screen user interface 22, control and communications circuitry, and a power supply), inside the secure section of the secure facility to send and receive telecommunications. The other person receiving or sending communications may use a kiosk 15a or b inside the facility, but outside the secure section thereof (i.e. a lobby or booking kiosk 17a/b), or a land line type or cell type telephone 16a (POTS) for voice or SMS text, a smart mobile phone 16b for voice, text, email or AV, or a PC 16c for email or AV. The system 10 also provides means for family or friends to electronically send or deposit funds or credits to the inmate that may then be used by the inmate to purchase or acquire telecommunication services of the system, vending of drinks, candy, snacks, personal items, or the like by way of one or more vending machines 17 inside the secure section of the facility or commissary 18 (aka “canteen”) items such as clothing, blankets and other larger personal items delivered by facility staff or administration, via so called “brown-bag” services. The system further provides a means for the facility staff or administration to monitor, record, and document communications and transactions between the inmate and his or her family, friends or others. The facility staff can safely and securely monitor communications for prohibited, illegal or unsafe activity, limit inmate access based on normal rules, funds or credit availability, or rule violations, and can suspend inmate accounts when warranted or necessary.

[0110] A preferred embodiment of the system 10 of the invention uses VoIP to communicatively connect the Kiosks 14 and 15, staff hardware and users of PCs 16c, land line telephones 16a and mobile phones and other mobile devices such as smart phones 16b. VoIP stands for Voice over IP or voice over Internet Protocol. It encompasses the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet 19. Internet telephony refers to communications services—voice, SMS, and/or voice-mes-

saging applications—that are transported via the Internet, rather than the public switched telephone network (PSTN). The steps involved in originating an outgoing VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving or incoming side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Even though IP telephony and VoIP are used interchangeably, IP telephony refers to all use of IP protocols for voice communication by digital telephony systems, while VoIP is one technology used by IP telephony to transport phone calls. VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. The choice of codec varies between different implementations of VoIP depending on application requirements and network bandwidth: some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs. Some popular codecs include u-law and a-law versions of G.711, G.722 which is a high-fidelity codec marketed as HD Voice by Polycom, a popular open source voice codec known as iLBC, a codec that only uses 8 Kbit/s each way called G.729, and many others. VoIP is available on many smart phones and Internet devices so that users of portable devices that are not phones, may place calls or send SMS text messages over 3G or Wi-Fi.

[0111] FIG. 4 illustrates a traditional process for using telephones inside a jail or other secure facility to contact persons outside the jail. In the prior art, the inmate picks up a telephone 30 and is automatically connected to a switch, which prompts the inmate with call 31 or account management 32 options. To manage their account, the switch checks into the inmate's balance and prompts the inmate with deposit 33 options. Funds may be deposited into the inmates' account assuming all validation checks pass. To manage a call, the switch check the inmate's balance and then prompts the inmate for the number to be called and checks for various rule settings. The rule settings may include blacklistings, email notifications, section/station settings, attorney call status, and deferred payment call status. The call is placed with a telecommunications service provider 34 via Session Initiation Protocol (SIP). The telephone called is answered by a user 35 (for example the inmate's friend, family member or attorney) outside the jail or other secure facility, or if not answered it routes to voicemail. A non-blocking call identifying prompt is played in the background while the call continues. Either the calling device or the telephony switch will charge the inmate account for the call.

[0112] The system 10 of the invention is described below first in terms of its telephone or phone aspects in Section 1 and FIGS. 4-59 and then with respect to its audio-visual or video visitation aspects in Section 2 and FIGS. 60-87.

1. Phone Features

[0113] Referring to FIG. 5, an embodiment of the phone system 10 of the invention comprises a Phone Server 41, a telephony switch which is connected to a Service Provider 42. The Service Provider 42 is any provider with Session Initiated Protocol (SIP) capability. The Phone Server 41 negotiates SIP communication between various SIP endpoints. It handles

call permissions as well as charging, recording and monitoring. The Phone Server 41 is communicatively connected to a Monitoring Station 43 which requests recorded and live streams from the Phone Server 41. Based on a request, the monitoring station 43 has the ability to pause, fast forward and rewind the recorded stream as well as to stop a live call in progress. It also enables calling rules. The Phone Server 41 is also communicatively connected to an Account Manager Server 44. The account manager 44 provides a means for the telephones to know the details of the caller and the person or entity being called. A most preferred example of the account manager server 44 is a Team Server provided by Team Software of Hudson, Wis. USA. However, the account manager server 44 can be any server that handles TCP/IP protocols over any IP network. The Phone Server 41 and Account Manager Server 44 are communicatively connected to the Inmate Kiosk(s) 15 or other devices inside the jail or other facility. Such other devices include traditional inmate telephones 19a and mobile or hand held devices inside the secure facility or jail. The Phone Server 41 is also communicatively connected to the telephones and devices 16a-c outside the facility.

[0114] FIG. 6 shows an embodiment of the communications connections 40a between the phone server 41 and certain elements of the system 10 located inside the secure facility (the kiosk(s) 15, traditional inmate phone(s) 45, other mobile devices 16 in the facility, and the admin monitoring station 44) via the Internet 19 and through the facility firewall 46.

[0115] FIG. 7 shows an embodiment of the communication connections 40b between the phone server 41 and other servers and elements of the system 10 which are disposed outside the secure facility. The phone server 41 is preferably a software element which makes the calls. A phone management interface 47 is an additional layer of software that controls the phone server 41. The phone management interface 47 processes information such as outgoing and incoming rules, the inmate rate, and the like. Connected through the Internet 19 are the account manager server 44, the call record server 48 (a hardware element which actually stores recorded calls), and a communication account server 49. The communication account server 49 is preferably software which debits and credits accounts at the manager of the system 10, and other similar business functions. The manager of the system 10 is preferably an independent third party business, such as Applicant's assignee. However, it is within the purview of the invention that the system 10 manager may be the jail or secure facility itself, or some other governmental, quasi-governmental or non-profit entity.

[0116] FIG. 8A is a flow chart showing an embodiment of the process of making an outgoing call from a jail according to the invention. The outgoing call process of the invention is preferably implemented by the system 10 of the invention. The first step of the process involves receiving 60 a request for an outside phone number of a family member, friend or other call recipient, and then determine 61 whether the call is local or long distance. Next, the system verifies 62 that the inmate has sufficient funds or credit, and checks associated rules for that inmate account. The call is either prohibited 63 (with notice to the inmate), a non-call ending rule is noted 64, or the system proceeds 65 to determination 66 whether the call number is privileged as for example in the case of an attorney telephone number. Proceeding with the call, next records are logged and created 67, recording is initiated 68 and the call is

sent **69** to the service provider to ring the call recipient. If a timeout timer period is reached **70** the call ends. If the call is answered **71** within the allotted time, the call proceeds. A charging process **72** begins in some cases. The call proceeds until termination or hang up **73**.

[0117] Significantly, the system of the invention provides a means of receiving **80** an incoming call to the inmate in the facility from a person outside. Referring to FIG. **8B**, a preferred embodiment of an incoming call process of the invention involves first receiving a call request and then determining **81** whether the outside caller is requesting support. If so, then the call is transferred **82** to a help line. If not, the user is prompted **83** to dial or otherwise input an extension for the inmate. Users may first obtain an inmate extension as well as a PIN number by utilizing the inmatecantee.com process shown in FIGS. **51-59**. Next, the system determines **84** if the extension is valid. If not, then the caller has an opportunity to enter another extension by another prompt **85**. If valid, the system inquires of the PIN and checks **86** whether it is valid. If the PIN is not entered correctly, the user again has an opportunity to correct. If the PIN is correct, the next step **87** is to find the Inmate's location and a list of phone devices in the inmate's POD (jail location). Phone devices may include, but are not limited to stand alone Kiosks, traditional hand held telephone devices and the like. The system then determines **88** whether the caller is a registered attorney. If the user is a registered attorney (again signed up at the inmatecanteen.com system of FIGS. **51-59**), the conversation is private and a reduced rate may apply. If not, the system verifies **89** that the user has sufficient funds to place the call (funds are deposited via inmatecanteen.com). Maximum call time is calculated **90** based on caller funds, and at a predetermined time, for example the 1 minute 30 second remaining mark of the call, a blocking prompt is played warning the user that they are about to run out of call minutes. Initially or at any time later, inmate rules **91** may be processed. Such rules may include, but are not limited to inmate blacklisting, section/pod blacklisting, email call notifications, and approved calling hours. If a call or call event or time fails a rule, the call is transferred **92** to a voicemail system. If all rules or some rules are met, a call record is created **93**, recording begins (unless attorney or other call), and the registered device is dialed. Recordings are processed in GSM format. Both sides of the stream are included in the recording. The next step is to wait **94** for an answer. If the inmate answers, the attorney rule is checked **95** and if positive, the charging **96** process begins. If the inmate does not answer, the call may be transferred **97** to a voicemail system.

[0118] FIG. **9** is a chart of an embodiment of the hierarchy or relationship of the user screens of the administrator controls and tools **100** of the system. At the Administration Login screen **101** a username and password are provided by the user. The following admin screens are available: Create Inmate Account **102**, Deposit Funds to Inmate Account **103**, Withdraw Funds from Inmate Account **104**, Charge (Site Charge) An Inmate's Account for money owed to a Vendor **105**, Inmate History Report **106**, Inmate Request Page **107**, an Undo Connection Wizard **108** and an Inmate Messaging page **109**. Additionally, the system provides means to submit a ticket **110A**, for remote support **110B**, and for live chat **110C**. FIGS. **12-24** show exemplary embodiments of user interfaces for these functions. FIG. **12** illustrates a LogIn interface **101**. FIG. **14** shows a Create Inmate Account **102**. FIG. **16** discloses a Deposit Funds to Inmate Account screen **103**. FIG. **17**

illustrates a Withdraw Funds from Inmate Account screen **104**. FIG. **18** shows a Charge (Site Charge) An Inmate's Account for Money Owed to a Vendor **105** screen. FIG. **19** discloses a Inmate History Report user interface **106**. FIG. **20** shows a Inmate Request screen **107**. Additionally, the system provides means to submit a ticket **110A**, for remote support **110B**, and for live chat **110C** shown in FIGS. **22, 23** and **24** respectively.

[0119] Additional administrator control functions and user interfaces therefor are shown in FIGS. **25-37**. FIG. **25** illustrates a Close Inmate Account screen **111**. FIG. **26** shows an Assign Inmate Smart Card screen **112**. FIG. **27** discloses a Discipline Inmate Account interface **113**. FIG. **28** illustrates an Edit Inmate Account screen **114**. FIG. **29** shows an Inmate Requests—Old screen **115**. FIG. **30** shows a View Inmate Canteen Order screen **116**. FIG. **31** shows a Bank Deposit interface **117**. FIG. **32** shows a Deposit To Vendor screen **118**. FIG. **33** shows a Pay Vendor user interface **119**. FIG. **34** shows a Batch Order screen **120**. FIG. **35** shows a Manage Site Canteen System interface **121**. FIG. **36** shows a Manage Warehouse screen **122**. FIG. **37** discloses a Manage Warehouse Order System user interface **123**.

[0120] FIG. **10** is a chart of an embodiment of the user screens of the inmate management tools **130** of the system. At the Login Screen **131** a username and password are input. The following options are provided: Account information **132**, Account History **133**, Withdrawal Information **134**, Canteen Information **135A/B** (including Current Order **136** and Past Orders **137**). Phone Cards **138**, MP3 **139**, Requests **140**, Inbox **141**, and phone calls **142**, including Phone Calls **143**, Voice Mail **144** and Phone Account **145**. FIGS. **38** to **50** show embodiments of user screens of the inmate management tools of the system outlined in the Chart of FIG. **10**, with an example of the login screen **131** shown in FIG. **38**. An example of the Account Information screen **132** is shown in FIG. **39**. The Account History screen **133** is shown in FIG. **40**. The Withdrawal Information screen **134** is shown in FIG. **41**. The Canteen Information screens **135a/b** are shown in FIGS. **42** and **43**, including Current Order selection **136** and a Past Orders selection **137**. The Phone Card screen **138** is shown in FIG. **44**. The MP3 screen **139** is shown in FIG. **45**. The Requests screen **140** is shown in FIG. **46**. The Inbox **141** is shown in FIG. **47**. The Phone Call screen **143** is shown in FIG. **48**. The Voice Mail screen **144** is shown in FIG. **49**. And, a preferred embodiment of the Phone Account screen **145** is shown in FIG. **50**.

[0121] FIG. **11** is a chart of an embodiment of the user screens of the family/friend management tools **150** of the system. An on-line web based login screen **151** are for input of a username and password. First time visitors **152** are routed to a New Account Sign Up screen **153** and sub screens (not shown) for input of user information. Holders **154** of accounts are routed to a screen **155a/b** permitting selection of a facility (jail) and a choice of communication administration between phone **156** and video visitation **157** (audio-visual). For phone administration **156**, phone call monitoring **157**, phone call setting **158** and reports (call details **159** and inmate deposit **160**) are available. FIGS. **51-59** show exemplary embodiments of user interfaces for these functions for family/friend management. FIG. **51** illustrates the login screen **151**. FIG. **52** shows an embodiment of the New Account Sign Up Screen **153**. FIG. **53** shows an admin screen **155a** for user name and password. FIG. **54** shows a facility selection screen **155b**. FIG. **55** shows an example interface for phone administration

156. FIG. 56 shows a phone call setting screen 159. FIG. 57 illustrates a call detail screen 160. And, FIG. 58 discloses an inmate deposit user interface 161. FIG. 59 shows a video visitation admin screen 157

2. Video Visitation Features

[0122] FIGS. 60 and 66 illustrate an embodiment of the system 200 of the invention from the perspective of the audio-visual video visitation hardware and software elements of the invention. The system 200 enables persons outside the jail or other secure facility to visit audio-visually with an inmate or resident of a secure facility. The inmate uses an Inmate Kiosk 214. The outside visitor uses a Visitation Kiosk 215 disposed at the jail in the lobby, visitor center or booking station thereof, a mobile, smart device 216B or a PC/Mac web browser 216C (for example via sign on page 251) or the like. The kiosks 214 and 215 are communicatively connected to a remote, on-line streaming platform or infrastructure 250. The streaming platform 250 facilitates on-demand, live (real-time), interactive audiovisual communication between at least two parties. A preferred streaming platform is provided by Influxis of Valencia, Calif., USA. The kiosks 214 and 215 communicate with the streaming platform 250 preferably by real time messaging protocol (RTMP). The communication link preferably includes Flash Object Flex 253 attributes. Similarly, a mobile device 216B carried by an outside visitor is communicatively connected to the streaming platform 250 via RTMP (and preferably Flash Object Air 254). Further, the outside person's PC browser 216C is also communicatively connected to the streaming platform 250 via RTMP with Flash Object 254A. The kiosks 214/215, mobile device 216B and PC 216C audio-visual devices are further communicatively connected to a remote, Inmate Canteen Web service 244 via hypertext transfer protocol (HTTP or HTTPS). The Web Service 244 is connected to a database 251. The streaming platform 250 is communicatively connected to the Web Service 244 via an http protocol and a server side actionscript 252. This communication service preferably conforms to Representational State Transfer (REST) constraints. System management may monitor and control the system 200 via a web interface 255.

[0123] FIG. 61 illustrates an embodiment of the flow of information in the video visitation system 200 and method of the invention. Inmates access the video visitation system 200 via the inmate kiosk 214. Visitors access the system 200 via an app on their mobile smart device 216B, or visitor kiosk 215 or web browser 251. Jail staff or system managers access the system to monitor and control video visitation via the manager web interface 255 and admin web page 201A respectively. Video Chat Room information and call status information is shared between the inmate kiosk 214, visitor devices 216B, 215, and 251 and jail staff and system managers via the web service 244. Audio/Visual streams to and from the inmate kiosk 214 and the visitor devices 216B, 215, and 251 via a collaboration service 250. The web service 244 is also used to create AV chat rooms. The web service 244 updates calls and user details to a net TCP Video controller service 202. The controller service pushes call notifications to the inmate kiosk 214.

[0124] FIG. 62 is a flow chart of a preferred embodiment of the method of making a web based video visitation. The visitor logs on 260 the system via a web interface. A determination 261 is made whether the desired inmate is in an active video section. If not, the video visit option on the

visitor/user web interface is disabled 262. If present, the video visit option is enabled 263. Next, the visitor may actuate 264 the video visitation button. User approval requirement is determined 265. If required, a determination 266 is made whether the user is approved. If not, the user is navigated 267 to a web page to permit approval, whereupon information is entered 268 to assign approval status. If approved (already or after the approval process 267/268), the user is directed to a display video chat room ready 269. The user is so directed earlier if user approval is not required in step 265. The user is provided an opportunity to deposit additional funds or credits by clicking "Deposit Funds To Account" button, payment is collected 271, and video visitation processing continues. Next, determination 272 is made whether the visiting hours time window is open. If not, the call inmate button is not enabled 273. If so, determination 274 is made whether the user has sufficient funds. If not, the call inmate button is disable 273. If sufficient funds are available, the call inmate button is enabled 275. Upon clicking the call inmate button 276, call rules are processed 277. Determination 278 is made whether any necessary rules are met. If not, a message related to the rule is displayed 279 to the user. If rules are met, the user and the inmate are connected 280 for a video visitation.

[0125] FIG. 63 is screen shot showing an embodiment of the user interface and display 290 of a video visitation kiosk of the invention for a video call. FIG. 64 is a screen shot showing an embodiment of the user interface and display 291 of a video visitation from the perspective of an outside user family or friend using a personal computer. FIGS. 65A/B is a screen shots showing an embodiment of the user interface and display 292 of a video visitation from the perspective of an outside user family or friend using a mobile device such as an iPad.

[0126] FIG. 66 is another diagram 293 of the deployment of devices in the video visitation system 200 of the invention. FIG. 67 is a flow chart of an embodiment of the file migration worker process 294 of the invention. FIG. 68 is a diagram of an embodiment of a call management web service package 295 of the invention.

[0127] FIG. 69 is a web shot of an embodiment of a user interface 296 for a secure facility administrator for controlling video visitation settings for the system. FIG. 70 is a web shot of an embodiment of a user interface 297 for an administrator for listing and monitoring downloads for the system. FIG. 71 is a web shot of an embodiment of a user interface 298 for an administrator for listing and controlling blacklist information for the system. FIG. 72 is a web shot of an embodiment of a user interface 299 for an administrator for listing and controlling inmate video visitations for the system. FIG. 73 is a web shot of an embodiment of an email notification 300 for an administrator that a particular inmate has used video visitation for the system.

[0128] FIGS. 74 A/B are activity diagrams 301a/b of an embodiment of a method of approving video visitation for a user. FIG. 74A shows the steps from the perspective of the user. FIG. 74B shows the steps from the perspective of the staff. FIG. 75 is a web shot of an embodiment of a user interface 302 for a first step in the method of obtaining approval. FIG. 76 is a web shot of an embodiment of a user interface 303 for a second or subsequent step in the method of obtaining approval. FIG. 77 is a web shot of an embodiment of a user interface 304 for a third or subsequent step in the method of obtaining approval. FIG. 78 is a web shot of an embodiment of a user interface 305 for a fourth or subsequent

step in the method of obtaining approval. FIG. 79 is a web shot of an embodiment of a user interface 306 for a final step in the method of obtaining approval, wherein a request is denied or approved. FIG. 80 is a web shot of an embodiment of a user interface 307 for an optional audition room feature in the method of obtaining approval.

[0129] FIG. 81 is a web shot of an embodiment of a user interface 308 for a first step in the method of making a video visitation call by an outside family member or friend. FIG. 82 is a web shot of an embodiment of a user interface 309 for a second or subsequent step in the method of obtaining approval, wherein the video visitation caller is waiting for the video visitation call to connect with the inmate. Upon connection, a video visitation screen appears as for example is shown in FIG. 65 or 65.

[0130] FIG. 83 is a web shot of an embodiment of a user interface 310 for an administrator who is manually approving requests for video visitation rights for a caller. FIG. 84 is a web shot of an embodiment of a subsequent user interface 311 for an administrator who is manually approving requests for video visitation rights for a caller.

[0131] FIG. 85 is a web shot of an embodiment of a user interface 312 for a system administrator for monitoring live updates of video visitation calls in progress in the overall system. FIG. 86 is a web shot of an embodiment of a user interface 313 for a system administrator for monitoring and controlling video visitation calls in the overall system. FIG. 87 is a web shot of an embodiment of a user interface 314 for a system administrator for monitoring plural video visitation calls in progress in the overall system.

[0132] The descriptions above and the accompanying materials should be interpreted in the illustrative and not the limited sense. While the invention has been disclosed in connection with the preferred embodiment or embodiments thereof, it should be understood that there may be other embodiments which fall within the scope of the invention.

The invention claimed is:

1. A system for providing audio-visual telecommunications between a resident inside a secure facility and at least one person outside the secure facility, and for management of such audio-visual telecommunications by an administrator of the secure facility, comprising: at least one audio-visual telecommunications device disposed at the secure facility for use by the resident, the secure facility audio-visual telecommunications device adapted to be communicatively connected to an external streaming platform; and an audio-visual account management server communicatively connected to the at least one secure facility telecommunications device, and wherein the secure audio-visual telecommunications device and the audio-visual account management server are adapted to be communicatively connectible to at least one audio-visual communications device disposed outside the secure facility for use by at least one person outside the secure facility.

2. The system of claim 1, wherein the secure facility is an institution selected from the group of institutions consisting of a jail, a detention center, a short term corrections facility, a penitentiary, a prison and a mental health institution; wherein the resident is a person selected from the group of persons consisting of an inmate, a prisoner and a patient; wherein the administrator is a person selected from the group of persons consisting of a sheriff, an officer, a guard, a warden, a jailer, and a mental health worker, and wherein the at least one

person outside secure facility is selected from the group of persons consisting of a family member, a friend, an acquaintance, and an attorney.

3. The system of claim 1, wherein the telecommunications between the resident of the secure facility and the at least one person outside the secure facility further includes telecommunications selected from the group of communications consisting of voice, SMS text, IM, and email; and wherein management of telecommunications is selected from the group of activities consisting of monitoring, recording, controlling and documenting communications and transactions of the resident.

4. The system of claim 3, wherein the controlling activities are selected from the group of activities consisting of video visitation blocking, blacklisting, email notification, section/station setting, attorney video visitation status, and deferred video visitation status.

5. The system of claim 1, wherein the person outside the secure facility is further able to electronically deposit funds or credits to an account of the resident at the secure facility, the account funding products and services at the secure facility selected from the group of products and services consisting of audio-visual communications, voice communications, vending drink, snacks and food items, and commissary items such as personal care items, books, videos, clothing and apparel, and blankets; and wherein the administrator is further able to monitor, audit and manage the account of the resident.

6. The system of claim 1, wherein the at least one audio-visual telecommunications device disposed at the secure facility is a device selected from the group of devices consisting of a personal computer (PC), and an audio-visual telecommunications kiosk; and wherein the person outside the secure facility communicatively connects with the system by a device adapted to connect to the audio-visual management server and the external streaming platform, selected from the group of devices consisting of a smart phone, a PC and an audio-visual telecommunications kiosk.

7. The system of claim 1, wherein the at least one audio-visual telecommunications device disposed at the secure facility, and devices used by the at least one person outside the secure facility communicatively connect to the streaming platform via RTMP.

8. The system of claim 7, further comprising flash attributes applied to the RTMP communicative connections.

9. The system of claim 1, wherein the at least one audio-visual telecommunications device disposed at the secure facility, and devices used by the at least one person outside the secure facility communicatively connect to the audio-visual account management server via HTTP.

10. The system of claim 1, wherein the audio-visual account management server controls video visitation permissions, video visitation charging, recording and monitoring.

11. The system of claim 10, wherein the audio-visual account management server further functions to pause, fast forward, and rewind a recorded audio-visual telecommunications stream, and to stop a live call in progress.

12. The system of claim 11 wherein the audio-visual account management server further functions to process calling rules.

13. The system of claim 1, wherein the audio-visual account manager server is a server which communicates remotely via HTTP, and which stores and processes information about the resident, the at least one person outside the secure facility.

14. The system of claim **13**, wherein the audio-visual account manager server is a further comprises a TEAM Server provided by Team Software of Hudson, Wis. USA.

15. The system of claim **1**, further comprising storage means connected to the audio-visual account management server.

16. The system of claim **1**, further comprising server side action script communicatively connected to the audio-visual account management server.

17. The system of claim **1**, comprising a plurality of audio-visual resident kiosks.

18. The system of claim **1**, wherein the system is adapted to be used with an external streaming platform consisting of an Influxis streaming platform.

19. The system of claim **1**, wherein the system includes the external streaming platform.

20. A system for providing audio-visual telecommunications between an inmate inside a correctional facility, the facility being of the type having a public lobby, visitor center, or booking area in addition to secure inmate resident section, and at least one non-inmate family member, friend or attorney outside the secure facility, and for management of such audio-visual telecommunications by an administrator of the secure facility, comprising:

- a. at least one inmate audio-visual telecommunications kiosk disposed at the secure facility for use by the inmate, the inmate audio-visual kiosk adapted to be communicatively connected to an external streaming platform;
- b. an audio-visual account management server communicatively connected to the at least one secure facility telecommunications device, and wherein the secure audio-visual telecommunications device and the audio-visual account management server are adapted to be communicatively connectible to at least one audio-visual communications device disposed outside the secure facility for use by at least one person outside the secure facility;
- c. at least one public audio-visual telecommunications kiosk disposed in the public lobby, visitor center or booking area at the secure facility for use by the at least one non-inmate family member, friend or attorney, the at

least one public telecommunications kiosk being adapted to be communicatively connected to the external streaming platform; and

- d. wherein audio-visual telecommunications between the inmate and the at least one non-inmate family member, friend or attorney is selected from the group of communications consisting of voice, SMS text, IM, email, and audio-visual by way of the public and inmate kiosks; and wherein management of telecommunications is selected from the group of activities consisting of monitoring, recording, controlling and documenting audio-visual visitation and transactions of the inmate.

21. A method for audio-visually telecommunicating between a resident inside a secure facility and at least one person outside the secure facility, and for management of such telecommunication by an administrator of the secure facility, comprising the step of making an incoming audio-visual chat from at least one person outside the secure facility to the resident inside the secure facility.

22. The method for telecommunicating of claim **21**, wherein the step of making an incoming video chat comprises the steps of determining whether the resident is in an active video section, verifying that a chat is authorized, displaying an answer message to the resident, and connecting the at least one person outside the secure facility and the resident.

23. The method of claim **21** further comprising the step of making an outgoing video chat from the resident to at least one person outside the secure facility.

24. The method of claim **23**, wherein the step of making an outgoing call comprises the steps of receiving an video chat request, verifying that the resident is authorized to make an outgoing video chat, and sending a chat request to the at least one person outside the secure facility.

25. The method of claim **21** wherein the method is implemented by a system comprising at least one audio-visual telecommunications device disposed at the secure facility for use by the resident, the secure facility audio-visual telecommunications device adapted to be communicatively connected to an external streaming platform; and an audio-visual account management server communicatively connected to the at least one secure facility telecommunications device.

* * * * *



(19) **United States**
(12) **Patent Application Publication**
TORGERSRUD

(10) **Pub. No.: US 2014/0282926 A1**
(43) **Pub. Date: Sep. 18, 2014**

(54) **DOSSIER PACKAGING**

(71) Applicant: **TELMATE, LLC**, San Francisco, CA (US)

(72) Inventor: **Richard TORGERSRUD**, San Francisco, CA (US)

(73) Assignee: **Telmate, LLC**, San Francisco, CA (US)

(21) Appl. No.: **13/834,677**

(22) Filed: **Mar. 15, 2013**

Publication Classification

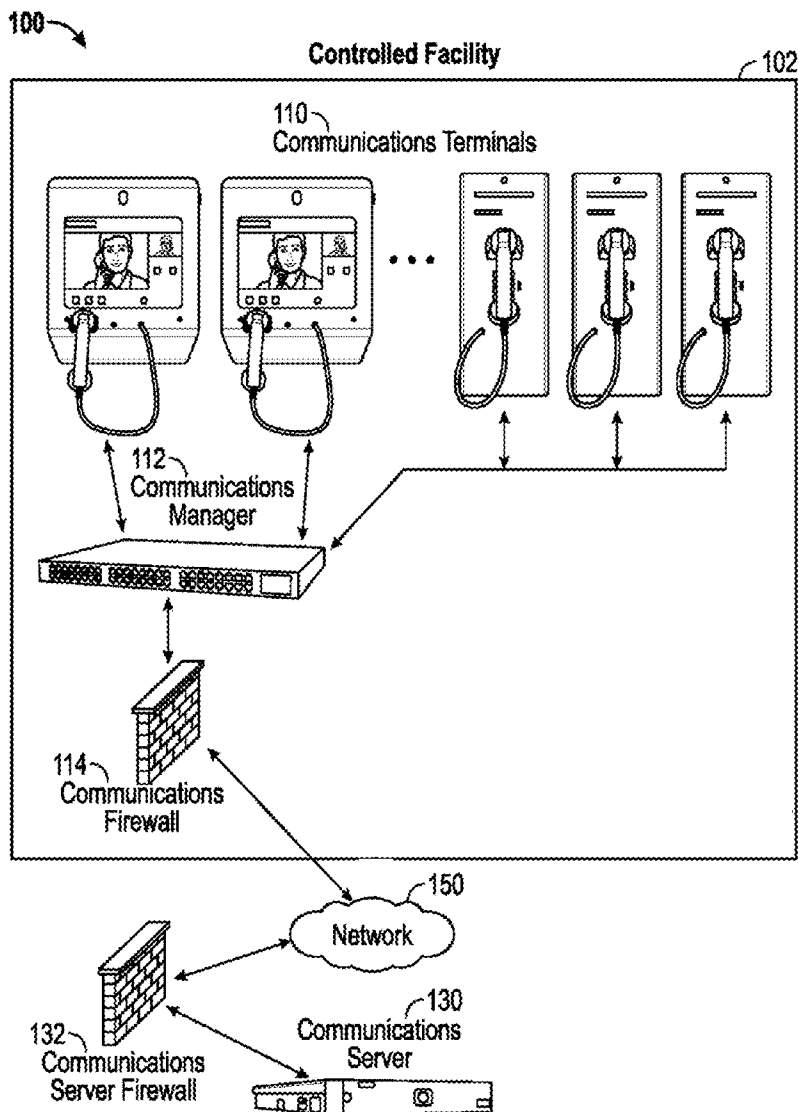
(51) **Int. Cl.**
G06F 21/31 (2006.01)

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

CPC **G06F 21/31** (2013.01)
USPC **726/5**

(57) **ABSTRACT**

The subject technology discloses configurations for receiving a request from a user to log into a communications server in which the request includes user credentials. The user is authenticated based on the included user credentials in the request. The user is then permitted to log into the communications server if the user is successfully authenticated. An input selecting a person of interest is received. The subject technology retrieves information associated with the selected person of interest. A dossier of information including the retrieved information associated with the selected person of interest is generated. The subject technology transmits the generated dossier to the user or an indicated recipient.



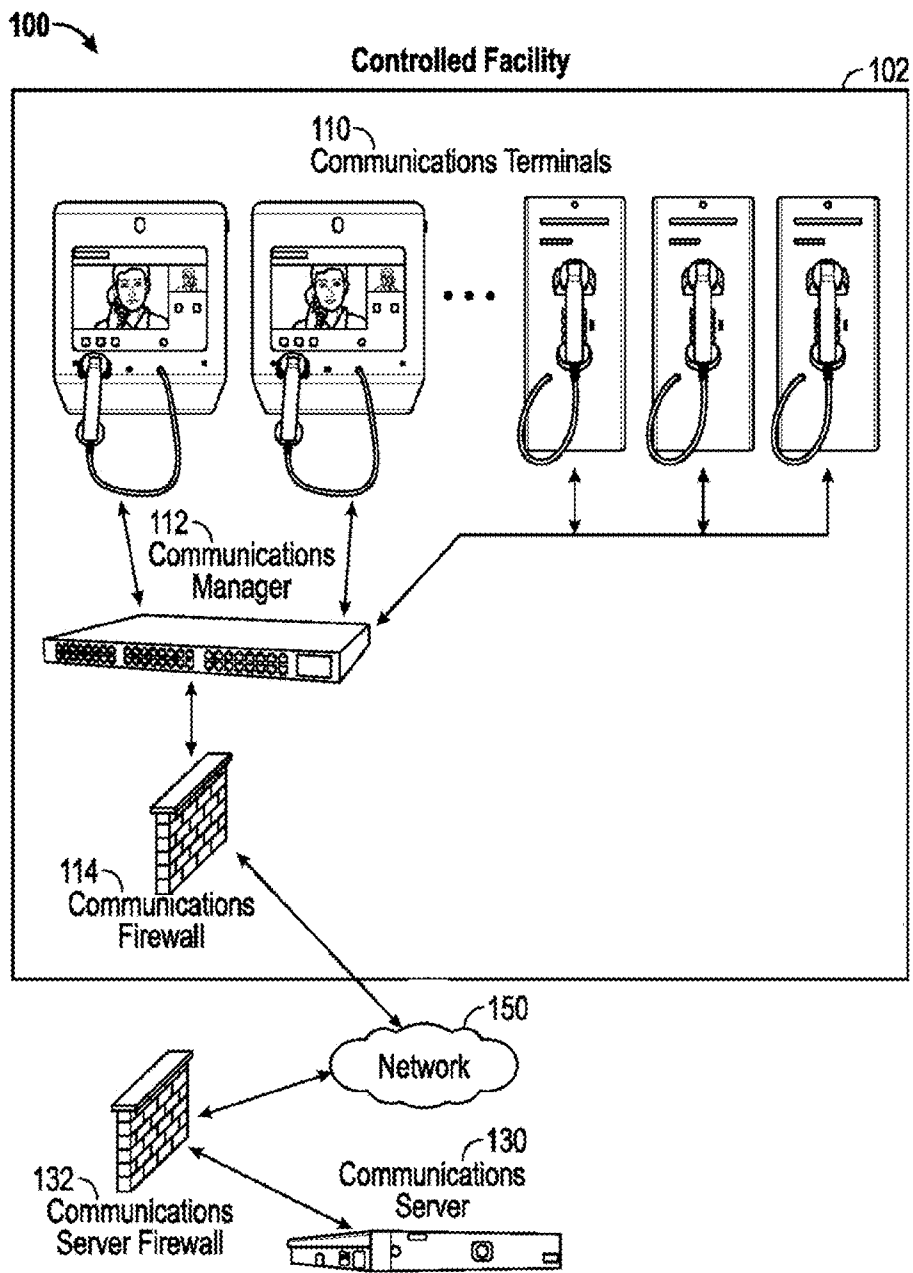


FIG. 1

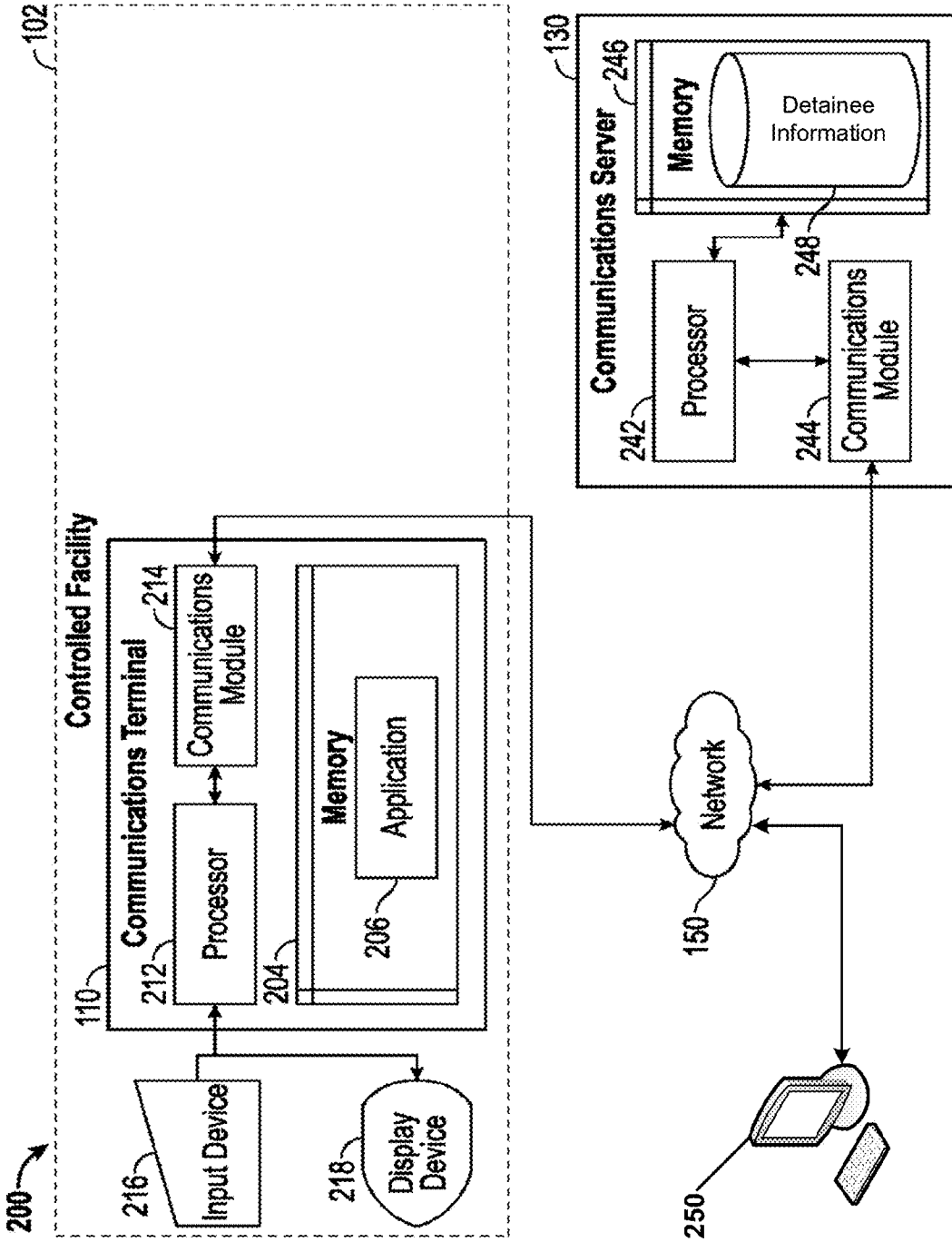


FIG. 2

300

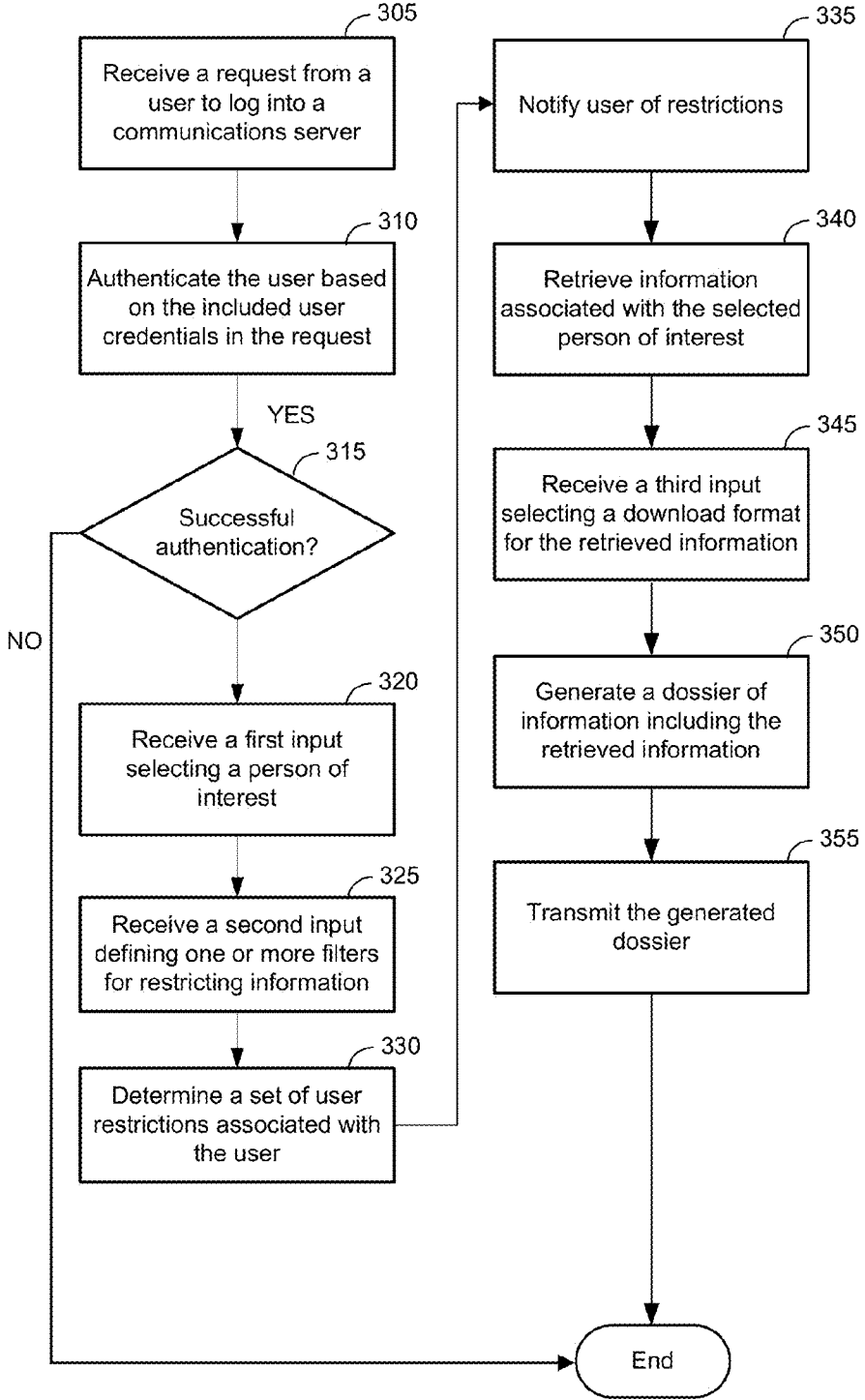


FIG. 3

400



Identity

Display Name: Text 1
Login: Text1
Password: [Redacted]
Confirm Password: [Redacted]
Next Login: Normal
Group: Facility-wide
Domain: Pinnacle Public
Organization: Demo
Expiration: [Redacted]
Disable User: []
Show PINs only: No

Privileges

Role: (No Role)

Call Monitor: Role Default
VoiceMail Broadcast: Role Default
Call History: Role Default
Inmates: Read/Write
Groups: Role Default
Kiosks: Read Only
Commissary: Role Default
Facility: Role Default
CSR: Role Default
Price Reports: Role Default
Accounting: Role Default
Basic: Role Default
Accounting: Role Default
Audit Report: Read/Write
Public Tickets: Role Default
Service Tickets: Role Default
Stations: Role Default
Destination Numbers: Role Default

Advanced Privileges:

Alarms / Contacts: Role Default
Burn Audio: Role Default
Free Calls: Deny
Flag Calls: Deny
Partner: Deny
Users: Role Default
Terminate Verified: Role Default
Investigation Tree: Deny
Snap: Role Default
Super Powers: Role Default
PREA Access: Role Default
Multi-Facility: Role Default
Intelmate: Deny
Super: Read Only
Ticket: Read/Write
Grievances: Role Default
Grievance Form Builder: Role Default

410

420

FIG. 4

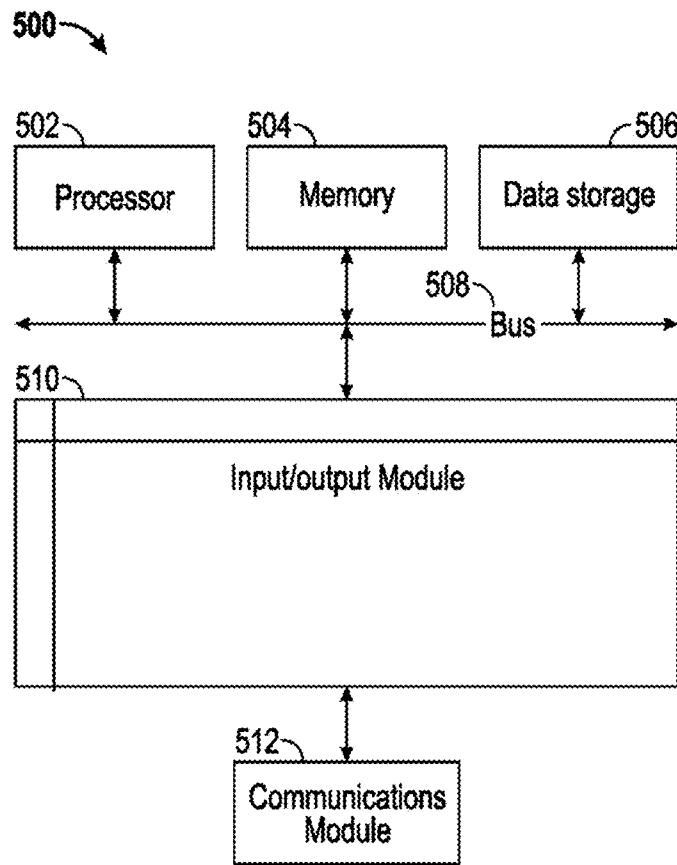


FIG. 5

DOSSIER PACKAGING

BACKGROUND

[0001] The present disclosure generally relates to computer systems, and more particularly to the use of a computer system to obtain information regarding an individual.

SUMMARY

[0002] The subject technology provides computer-implemented method including: receiving a request from a user to log into a communications server in which the request includes user credentials; authenticating the user based on the included user credentials in the request; permitting the user to log into the communications server if the user is successfully authenticated; receiving a first input selecting a person of interest; retrieving information associated with the selected person of interest; generating a dossier of information including the retrieved information associated with the selected person of interest; and transmitting the generated dossier to the user or an indicated recipient.

[0003] The subject technology further includes a system. The system includes a memory including instructions, and one or more processors configured to execute the instructions to: receive a request from a user to log into a communications server in which the request include user credentials; authenticate the user based on the included user credentials in the request; permit the user to log into the communications server if the user is successfully authenticated; receive a first input selecting a person of interest; receive a second input defining one or more filters for restricting information associated with the selected person of interest; determine a set of user restrictions associated with the user; retrieve information associated with the selected person of interest based on the defined one or more filters and the determined set of user restrictions; receive a third input selecting a download format for the retrieved information; generate a dossier of information including the retrieved information associated with the selected person of interest; and transmit the generated dossier to the user or an indicated recipient based on the selected download format.

[0004] The subject technology further provides a machine-readable medium including instructions stored therein, which when executed by a machine, cause the machine to perform operations including: receiving a request from a user to log into a communications server in which the request include user credentials; authenticating the user based on the included user credentials in the request; permitting the user to log into the communications server if the user is successfully authenticated; receiving a first input selecting a person of interest; receiving a second input defining one or more filters for restricting information associated with the selected person of interest; determining a set of user restrictions associated with the user; retrieving information associated with the selected person of interest based on the defined one or more filters and the determined set of user restrictions; receiving a third input selecting a download format for the retrieved information; generating a dossier of information including the retrieved information associated with the selected person of interest; and transmitting the generated dossier to the user or an indicated recipient based on the selected download format.

[0005] It is understood that other configurations of the subject technology will become readily apparent from the following detailed description, where various configurations of

the subject technology are shown and described by way of illustration. As will be realized, the subject technology is capable of other and different configurations and its several details are capable of modification in various other respects, all without departing from the scope of the subject technology. Accordingly, the drawings and detailed description are to be regarded as illustrative in nature and not as restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] The features of the subject technology are set forth in the appended claims. However, for purpose of explanation, several configurations of the subject technology are set forth in the following figures.

[0007] FIG. 1 illustrates an example architecture in which some configurations of the subject technology can be implemented.

[0008] FIG. 2 is a block diagram illustrating an example communications terminal and communications server in the architecture of FIG. 1 according to certain aspects of the disclosure.

[0009] FIG. 3 illustrates an example process for transmitting a dossier of information for a person of interest using the example communications server of FIG. 2.

[0010] FIG. 4 conceptually illustrates an example graphical user interface for setting user restrictions according to some configurations of the subject technology.

[0011] FIG. 5 is a block diagram illustrating an example computer system with which the communications terminal and communications server of FIG. 2 can be implemented.

DETAILED DESCRIPTION

[0012] The detailed description set forth below is intended as a description of various configurations of the subject technology and is not intended to represent the only configurations in which the subject technology may be practiced. The appended drawings are incorporated herein and constitute a part of the detailed description. The detailed description includes specific details for the purpose of providing a thorough understanding of the subject technology. However, the subject technology is not limited to the specific details set forth herein and may be practiced without these specific details. In some instances, structures and components are shown in block diagram form in order to avoid obscuring the concepts of the subject technology.

[0013] The process for obtaining all deposit, phone call, visitation, and other communication information involving a single detainee (e.g., inmate at a prison or jail) may be difficult and frequently requires multiple searches across multiple systems. Obtaining this data in a format that is appropriate for offline review, such as for archiving or legal discovery, may be even more difficult. The process is further complicated with newer communications systems, such as video visitation, text and video exchange, self-edited profiles, and other digital communication.

[0014] For instance, some existing systems may allow for a batch download of call recordings, but nothing else. Thus, for an investigator to download and organize the data available may require a tremendous amount of searching, downloading and organizing. Additionally, some data, such as customer service records, are not available to review or access in existing systems. Likewise, video visitation records typically require a separate login from the detainee phone system.

[0015] In particular, existing systems that manage communication records of detainees may have several drawbacks when it comes to offline review of files:

[0016] Existing systems may require multiple searches across multiple systems, sometimes requiring multiple logins

[0017] Frequently, acquiring call data information may require running one or more reports

[0018] Downloaded files are not organized in a way that allows the simple sorting of information into a timeline of activity, or the filtering of information to show or hide specific types of information

[0019] Many types of data may not be accessible to facility staff (such as call center recordings)

[0020] Once downloaded, there may be no mechanism to verify that the files have not been altered or comprised

[0021] In view of the above, the subject technology allows investigators and other users to download a single file or organized collection of files allowing offline review of content (such as for an investigation), offline storage (such as on a CD, or flash drive for archiving), legal discovery (such as the sharing of files with attorneys), and for use as courtroom evidence. As described herein, this package of offline data may be referred to as a “dossier.”

[0022] FIG. 1 illustrates an example architecture 100 in which some configurations of the subject technology can be implemented. The architecture 100 illustrates a detention environment 102 that includes communications terminals 110 connected to a network 150 through a communications firewall 114 using a communications manager 112. The architecture 100 further includes a communications server 130 as described herein connected to the network 150 through a communications server firewall 132. The firewalls 114 and 132 can be software-based or hardware-based.

[0023] Each of the communications terminals 110 is connected to a communications manager 112. In certain aspects, for purposes of load balancing, the communications terminals 110 can be connected to many communications managers. The communications terminals 110 can be audio communication terminals, video communication terminals, tactile communications terminals (e.g., for the visual and/or hearing impaired), or other terminals configured for communication between two individuals. In certain aspects, the communication terminals can be mobile, such as mobile smartphones or mobile kiosks. The communications manager 112 to which the communications terminals 110 are connected can be, for example, a networking device such as a router, gateway, or switch. The communications manager 112 can be configured for various protocols of communication including, for example, Internet Protocol (IP), voice over IP (VoIP), audio and video Internet telephony network protocols, or telephone switching.

[0024] The communications manager 112 is connected to the network 150, such as the Internet, a metropolitan area network (MAN), a wide area network (WAN), a broadband network (BBN), and the like. Further, the network 150 can include, but is not limited to, any one or more of the following network topologies, including a bus network, a star network, a ring network, a mesh network, a star-bus network, tree or hierarchical network, and the like. In certain aspects where the communications server 130 is located at the detention environment 102, the network 150 can include, for example, any one or more of a personal area network (PAN), a local area network (LAN), or a campus area network (CAN). The

connection between the communications manager 112 and the network 150 can be protected using a communications firewall 114, which can be particularly relevant to protecting the security of the detention environment 102 by limiting log ins to devices in the detention environment 102 to authorized individuals or processes.

[0025] The communications server 130 is connected to the network 150 through the communications server firewall 132. The communications server 130 is responsible for hosting resident location information provided by the communications terminals 110 for individuals in the detention environment 102. The communications server 130 can be any device having an appropriate processor, memory, and communications capability for hosting the terminal-based resident location information.

[0026] FIG. 2 is a block diagram 200 illustrating an example communications terminal 110 and communications server 130 in the architecture 100 of FIG. 1 according to certain aspects of the disclosure. The communications terminal 110 and communications server 130 are connected over the network 150 via respective communications modules 214 and 244. The communications modules 214 and 244 are configured to interface with the network 150 to send and receive information, such as data, requests, responses, and commands to other devices on the network 150. The communications modules 214 and 244 can be, for example, modems or Ethernet cards.

[0027] The communications terminal 110, which can be a telephone, videophone, or camera, includes a processor 212 (or connected downstream to a processor, e.g., at communications server 130), the communications module 214, and a memory 204 that includes an application 206. Although the communications terminal 110 is illustrated as including the processor 212 for example only, it is understood that in certain aspects where, for example, the communications terminal 110 is a telephone, the processor 212 is not included in the communications terminal. The application is configured to control log ins to the communications terminal 110. The communications terminal 110 also includes an input device 216 and an output device 214, such as a display. The input device 216 can include, for example, a keyboard, a touchpad, a microphone, a camera, touchscreen, or mouse. The processor 212 of the communications terminal 110 is configured to execute instructions, such as instructions physically coded into the processor 212, instructions received from software (e.g., application 206) in memory 240, or a combination of both.

[0028] The processor 212 of the communications terminal 110 is configured to execute instructions, such as instructions physically coded into the processor 212, instructions received from software (e.g., application 206) in memory 240, or a combination of both, to restrict logging in based on the location of the communications terminal 110 within a detention environment 102. For example, the processor 212 of the communications terminal 110 executes instructions from the application 206 to receive (e.g., by input device 216) a request from a user to log into the communications terminal 110.

[0029] In some configurations, a processor 242 of the communications server 130 is configured to execute instructions, such as instructions physically coded into the processor 242, instructions received from software in memory 246, or a combination of both. For example, the communications server 130 may provide an interface, such as a web-based application, that allows users to set parameters, such as select-

ing a person of interest (e.g., a detainee of a jail or prison), and trigger a download of files or data associated with the selected person of interest stored in the detainee information 248 of the memory 246. As illustrated in FIG. 2, a client computing system 250 (e.g., desktop computer, laptop, tablet, mobile device, etc.) may be configured to send a request to the communications server 130 in order to log in the web-based application. The client computing system 250 may then provide inputs from the user to the communications server 130 for interacting with the web-based application.

[0030] Although the disclosed block diagram 200 illustrates the detainee information 248 as being stored in the memory 246 of the communications server 130, detainee information 248 can be stored in one or more other communications servers (e.g., a different communication server in a separate or same data center). For example, the detainee information 248 can be provided by the communications server 130 to one or many communications servers, for example, as a form of data replication.

[0031] FIG. 3 illustrates an example process 300 for transmitting a dossier of information for a person of interest using the example communications server 130 of FIG. 2. While FIG. 3 is described with reference to FIG. 2, it should be noted that the process steps of FIG. 3 may be performed by other systems or computing devices. The process 300 begins by proceeding from start step 305 when a request is received from a user (e.g., facility staff, investigator, or lawyer on the client computing system 250) to log into the communications server 130. The user may utilize the client computing system 250 to send the request. In one example, the request includes user credentials (e.g., username, password, token, certificate, etc.). In step 310, the process 300 authenticates the user based on the included user credentials in the request.

[0032] In decision step 315, a determination is made whether the user has been successfully authenticated. If the determination of step 315 indicates that the user has not been successfully authenticated, the process 300 ends. If the determination of step 303 indicates that the user has been successfully authentication, the process 300 permits the user to log into the communications server and the process 300 continues to step 320.

[0033] In step 320, the process 300 receives a first input selecting a person of interest. In one example, the selected person of interest is a detainee of a jail or prison. To select the person of interest, the user may provide input (e.g., keyboard, mouse, touch, voice, etc.) in the interface of the web-based application provided by the communications server 130.

[0034] In step 325, the process 300 receives a second input (e.g., keyboard, mouse, touch, voice, etc.) defining one or more filters (including one or more parameters) for restricting information associated with the selected person of interest. In one example, the defined one or more filters may include at least one of a time period, type of data, a second person connected to the selected person of interest, or any person connected to the selected person of interest. The second person connected to the selected person of interest may be a friend of the selected person of interest or family member of the selected person of interest. More specifically, the filters may be defined according to the following examples:

[0035] a. Who is the Person of Interest: Who does the dossier focus on?

[0036] b. What Time Period: What time range is desired? Is it all time, or a specific time range?

[0037] c. Who Else: Does the dossier cover everyone who interacted with the person of interest, or is it just limited to one or a few others?

[0038] d. What Information: The dossier can include all known information, or it may be limited to specific types of information, such as just include financial transactions. Examples of different types of data listed after these steps.

[0039] In step 330, the process 300 determines a set of user restrictions associated with the user. In one example, the set of user restrictions associated with the user include at least one of user privileges, access to data, or download permissions. More specifically, examples of allowed and/or disallowed user rights may include the following:

[0040] a. User privileges: the logged in user's system permissions to access phone recordings, or deposit information, etc.

[0041] b. Access to data: facilities that the user is not attached to (e.g., a facility in a neighboring county where the person of interest may have been incarcerated in the past) may restrict access to data to the user

[0042] c. Download permissions: some user settings prevent users from downloading audio and video files and these permission settings apply to this invention. Changing a user's rights to allow the downloading of recordings would allow downloads to take place.

[0043] In step 335, the process 300 may, optionally, notify the user of any user restrictions determined in step 330. For instance, a notification may be sent to the user to indicate certain types of files are not permitted for downloading based on the user restrictions.

[0044] In step 340, the process 300 retrieves information associated with the selected person of interest based on the defined one or more filters and the determined set of user restrictions. In one example, the retrieved information associated with the selected person of interest includes data pertaining to: an audio file, video file, attempted call, completed call, rejected call, voicemail, message left for customer service, call to customer service representative, call to automated customer service, exchanged text, exchanged photo, exchanged video, video visit scheduled, video visit completed, kiosk deposit, deposit by mail, deposit over the phone, grievance or inmate request attempted, grievance or inmate request submitted, do not contact block via customer service, do not contact block via web site, investigator note, customer service note, visited website, game played, contact searched, video station login, web login by a friend or family, inmate balance check, or inmate balance transfer. Other types of data may be included and still be within the scope of the subject technology.

[0045] By way of example, the following pieces of information are available from a downloaded dossier. Likewise, any of the information below could be filtered out of a dossier, or selected for a dossier.

[0046] Attempted Calls

[0047] Completed Calls

[0048] Rejected Calls

[0049] Voicemails

[0050] Messages left for customer service

[0051] Calls to customer service representative

[0052] Calls to automated customer service

[0053] Exchanged text, photos and video

[0054] Video visits scheduled

[0055] Video visits completed

- [0056] Kiosk deposits
- [0057] Deposits by mail
- [0058] Deposits over the phone
- [0059] Grievances/inmate requests attempted
- [0060] Grievances/inmate requests submitted
- [0061] Do not Contact blocks via customer service
- [0062] Do not Contact blocks via Web site
- [0063] Investigator notes
- [0064] Customer service notes
- [0065] Visited Websites (by inmate)
- [0066] Games played (by inmate)
- [0067] Contacts searched (by inmate)

sum may be stored separately (e.g., on the communications server 130, or in a file) for future verification of the data (e.g., files) included in the dossier.

[0078] In some configurations, each downloaded dossier may include an accompanying text file containing a checksum (e.g., a hash or hashtag) for each recording contained in the dossier (e.g., zip or compressed file). Each checksum may be an MD5 hash of a specific digital file (e.g., audio or video recording, etc.) and may be understood as unique file “fingerprint.” Below is an example of a text file that contains digital fingerprints for two audio recordings:

```
2316183ce2cb10de32a0873cccaca178 01_O_Neil_415-412-9861_07-27-11_1215.wav
e8c6f6c54423185044c82cfd947be9ea 02_O_Neil_210-663-0540_07-27-11_1100.wav
```

- [0068] Video station logins by inmate
- [0069] Web logins by friends & family
- [0070] Inmate balance checks
- [0071] Inmate balance transfers

[0072] In step 345, the process 300 receives a third input selecting a download format for the retrieved information. In one example, the selected download format may be an e-mail including a link to the generated dossier, compressed file, Portable Document Format (PDF) file, MHTML file, or webarchive file. Further, the link to the generated dossier may expire after a predetermined period of time for security considerations. More specifically, the dossier may be:

- [0073] a. Downloaded: downloaded as a compressed file (e.g., zip file) containing both data and recording files, as a single PDF, or as offline web content such as a zipped collection of web files, MHTML file or webarchive format.
- [0074] b. Emailed: a dossier may be emailed to a third party (e.g., defense attorney) by entering that person’s email address. The dossier may be attached as a zip file, or sent as a one-time download link, which can be made more secure for opting for a limited window of availability for the download link.

[0075] In step 350, the process 300 generates a dossier of information including the retrieved information associated with the selected person of interest. In one example, the generated dossier includes one or more checksum values (e.g., hash) for verifying the retrieved information included in the generated dossier. Additionally, the communications server 130 may store such checksum values in the memory 246. In one example, an audio file or video file included in the dossier may be compressed to decrease download times. In one example, all recording files and data are compressed or merged into a single downloadable file. Examples of the single downloadable file may include, but are not limited to, TAR, RAR, SIT, GZIP and ZIP formats.

[0076] In step 355, the process 300 transmits the generated dossier to the user (e.g., the client computing system 250) or an indicated recipient (e.g., when the download format is an e-mail sent to one or more indicated recipients) based on the selected download format. The process 300 then ends.

[0077] In some configurations, at the client computing system 250, the dossier may be verified to ensure that the dossier has not been tampered. For example, the file(s) included in the dossier may be compared with the checksum value(s), which may be a series of characters in an associated text file that act as a digital fingerprint. When a dossier is created, the check-

[0079] In some configurations, the text above would be emailed or otherwise distributed separately from the digital recordings to prevent tampering of the digital recordings. Each digital fingerprint allows a user to verify that the file matches the original at any point in the future. To verify that the files have not been altered, a validation tool or application may be utilized to match each so-called “fingerprint” to each corresponding file. In some configurations, the validation tool may be included in a given operating system.

[0080] In some configurations, the process 300 may be performed when a user (e.g., investigator or attorney) wishes to download a wide variety of data associated with a detainee for offline access (e.g., without Internet or network access). The following description describes example usage scenarios that might occur regarding a detainee that has been in custody for 12 weeks while waiting for a trial:

Investigator

[0081] 1. First, an investigator downloads a dossier of all financial, communications and commissary related records related to the detainee to assist in the search for cohorts in the crime that the detainee is accused of committing.

[0082] 2. The investigator prints a document from the dossier that lists all of the events known to the communications system, which includes calls, deposits, Internet browsing history, games, photos exchanged, grievances filed, and video visits.

[0083] 3. While the records show hundreds of completed calls to a variety of destinations, the investigator notices a number of attempted calls to a single number that were never accepted. The phone number is associated with a person who has previously deposited funds via smartphone to another inmate at another facility that uses Telmate (as its inmate communications provider). Because of this past activity, the dossier download from Telmate includes several clustered geolocation coordinates on a map that are related to previous activity.

[0084] 4. The investigator checks out the geographic coordinates and sees that they cluster around an abandoned building. The abandoned building leads to the arrest of another suspect and the discovery of a methamphetamine lab.

Attorney

- [0085]** 1. The prosecuting attorney requests a download of all data associated with the original arrested detainee and a second download of all records associated with the newly arrested suspect.
- [0086]** 2. The records are shared, through the legal discovery process, with the defense attorneys representing the suspects. Because the records can be downloaded as a single record, or organized batch of records, sharing this information with other attorneys involves just a few clicks.
- [0087]** 3. The documents are discussed between the attorneys and the large amount of evidence that the two suspects are connected (through the records in the downloaded dossier), perhaps combined with other evidence gathered outside this invention, leads the suspects to plead guilty.

Archiving

- [0088]** 1. The downloaded dossier file or files are archived in a manner that matches the County and State's required archiving process ensuring that documents are available five or ten years later when the two detainees are up for parole.
- [0089]** FIG. 4 conceptually illustrates an example graphical user interface (GUI) 400 for setting user restrictions according to some configurations of the subject technology. In some configurations, GUI 400 may be provided by the communications server 130 in an interface of a web-based application (e.g., administrator console).
- [0090]** As illustrated in FIG. 4, the GUI 400 includes one or more graphical elements. A graphical element can include, but is not limited to, a button, check box, radio button, slider, list box, drop-down list, menu, combo box, icon, text box, scroll bar, etc. In the example GUI 400, a graphical display area 410 provides, in different graphical elements, information associated with an individual (e.g., investigator, etc.) such as a display name, login, password, next login option, group, domain, and organization. A user may interact with the graphical elements (e.g., text fields, drop-down menu, etc.) in the graphical display area 410 to modify the information associated with the individual. Further, a graphical display area 420 provides, in different graphical elements, information corresponding to a set of privileges that define a set of user restrictions associated with the individual. A user may interact with the graphical elements (e.g., drop-down menu, etc.) in the graphical display area 420 to modify the set of privileges for different types of data that may be accessed by the individual (e.g., default, deny, read only, read/write). In this fashion, the subject technology provides granularity, on a per-user basis, in defining a set of user restrictions associated with an individual.
- [0091]** FIG. 5 is a block diagram illustrating an example computer system 500 with which the communications terminal 110 and communications server 130 of FIG. 2 can be implemented. In certain aspects, the computer system 500 may be implemented using hardware or a combination of software and hardware, either in a dedicated server, or integrated into another entity, or distributed across multiple entities.
- [0092]** Computer system 500 (e.g., communications terminal 110 and communications server 130) includes a bus 508 or other communication mechanism for communicating

information, and a processor 502 (e.g., processor 212 and 242) coupled with bus 508 for processing information. By way of example, the computer system 500 may be implemented with one or more processors 502. Processor 502 may be a general-purpose microprocessor, a microcontroller, a Digital Signal Processor (DSP), an Application Specific Integrated Circuit (ASIC), a Field Programmable Gate Array (FPGA), a Programmable Logic Device (PLD), a controller, a state machine, gated logic, discrete hardware components, or any other suitable entity that can perform calculations or other manipulations of information.

[0093] Computer system 500 can include, in addition to hardware, code that creates an execution environment for the computer program in question, e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, or a combination of one or more of them stored in an included memory 504 (e.g., memory 204 and 246), such as a Random Access Memory (RAM), a flash memory, a Read Only Memory (ROM), a Programmable Read-Only Memory (PROM), an Erasable PROM (EPROM), registers, a hard disk, a removable disk, a CD-ROM, a DVD, or any other suitable storage device, coupled to bus 508 for storing information and instructions to be executed by processor 502. The processor 502 and the memory 504 can be supplemented by, or incorporated in, special purpose logic circuitry.

[0094] The instructions may be stored in the memory 504 and implemented in one or more computer program products, i.e., one or more modules of computer program instructions encoded on a computer readable medium for execution by, or to control the operation of, the computer system 500, and according to any method well known to those of skill in the art, including, but not limited to, computer languages such as data-oriented languages (e.g., SQL, dBase), system languages (e.g., C, Objective-C, C++, Assembly), architectural languages (e.g., Java, .NET), and application languages (e.g., PHP, Ruby, Perl, Python). Instructions may also be implemented in computer languages such as array languages, aspect-oriented languages, assembly languages, authoring languages, command line interface languages, compiled languages, concurrent languages, curly-bracket languages, data-flow languages, data-structured languages, declarative languages, esoteric languages, extension languages, fourth-generation languages, functional languages, interactive mode languages, interpreted languages, iterative languages, list-based languages, little languages, logic-based languages, machine languages, macro languages, metaprogramming languages, multiparadigm languages, numerical analysis, non-English-based languages, object-oriented class-based languages, object-oriented prototype-based languages, off-side rule languages, procedural languages, reflective languages, rule-based languages, scripting languages, stack-based languages, synchronous languages, syntax handling languages, visual languages, wirth languages, embeddable languages, and xml-based languages. Memory 504 may also be used for storing temporary variable or other intermediate information during execution of instructions to be executed by processor 502.

[0095] A computer program as discussed herein does not necessarily correspond to a file in a file system. A program can be stored in a portion of a file that holds other programs or data (e.g., one or more scripts stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (e.g., files that store one or more

modules, subprograms, or portions of code). A computer program can be deployed to be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network. The processes and logic flows described in this specification can be performed by one or more programmable processors executing one or more computer programs to perform functions by operating on input data and generating output.

[0096] Computer system 500 further includes a data storage device 506 such as a magnetic disk or optical disk, coupled to bus 508 for storing information and instructions. Computer system 500 may be coupled via input/output module 510 to various devices. The input/output module 510 can be any input/output module. Example input/output modules 510 include data ports such as USB ports. The input/output module 510 is configured to connect to a communications module 512. Example communications modules 512 (e.g., communications module 214 and 244) include networking interface cards, such as Ethernet cards and modems. In certain aspects, the input/output module 510 is configured to connect to a plurality of devices, such as an input device (e.g., input device 216) and/or an output device 516 (e.g., display device 218). Example input devices 514 include a keyboard and a pointing device, e.g., a mouse or a trackball, by which a user can provide input to the computer system 500. Other kinds of input devices 514 can be used to provide for interaction with a user as well, such as a tactile input device, visual input device, audio input device, or brain-computer interface device. For example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, tactile, or brain wave input. Example output devices include display devices, such as a LED (light emitting diode), CRT (cathode ray tube), or LCD (liquid crystal display) screen, for displaying information to the user.

[0097] According to one aspect of the present disclosure, the communications terminal 110 and communications server 130 can be implemented using a computer system 500 in response to processor 502 executing one or more sequences of one or more instructions contained in memory 504. Such instructions may be read into memory 504 from another machine-readable medium, such as data storage device 506. Execution of the sequences of instructions contained in main memory 504 causes processor 502 to perform the process steps described herein. One or more processors in a multi-processing arrangement may also be employed to execute the sequences of instructions contained in memory 504. In alternative aspects, hard-wired circuitry may be used in place of or in combination with software instructions to implement various aspects of the present disclosure. Thus, aspects of the present disclosure are not limited to any specific combination of hardware circuitry and software.

[0098] Various aspects of the subject matter described in this specification can be implemented in a computing system that includes a back end component, e.g., as a data server, or that includes a middleware component, e.g., an application server, or that includes a front end component, e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the subject matter described in this specification, or any combination of one or more such back end, middleware, or front end components. The components of the system can be inter-

connected by any form or medium of digital data communication, e.g., a communication network. The communication network (e.g., network 150) can include, for example, any one or more of a PAN, LAN, CAN, MAN, WAN, BBN, the Internet, and the like. Further, the communication network can include, but is not limited to, for example, any one or more of the following network topologies, including a bus network, a star network, a ring network, a mesh network, a star-bus network, tree or hierarchical network, or the like. The communications modules can be, for example, modems or Ethernet cards.

[0099] Computer system 500 can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other. Computer system 500 can be, for example, and without limitation, a desktop computer, laptop computer, or tablet computer. Computer system 500 can also be embedded in another device, for example, and without limitation, a mobile telephone, a personal digital assistant (PDA), a mobile audio player, a Global Positioning System (GPS) receiver, a video game console, and/or a television set top box.

[0100] The term “machine-readable storage medium” or “computer readable medium” as used herein refers to any medium or media that participates in providing instructions or data to processor 502 for execution. Such a medium may take many forms, including, but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media include, for example, optical disks, magnetic disks, or flash memory, such as data storage device 506. Volatile media include dynamic memory, such as memory 504. Transmission media include coaxial cables, copper wire, and fiber optics, including the wires that comprise bus 508. Common forms of machine-readable media include, for example, floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, DVD, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, an EPROM, a FLASH EPROM, any other memory chip or cartridge, or any other medium from which a computer can read. The machine-readable storage medium can be a machine-readable storage device, a machine-readable storage substrate, a memory device, a composition of matter effecting a machine-readable propagated signal, or a combination of one or more of them.

[0101] As used herein, the phrase “at least one of” preceding a series of items, with the terms “and” or “or” to separate any of the items, modifies the list as a whole, rather than each member of the list (i.e., each item). The phrase “at least one of” does not require selection of at least one item; rather, the phrase allows a meaning that includes at least one of any one of the items, and/or at least one of any combination of the items, and/or at least one of each of the items. By way of example, the phrases “at least one of A, B, and C” or “at least one of A, B, or C” each refer to only A, only B, or only C; any combination of A, B, and C; and/or at least one of each of A, B, and C.

[0102] Furthermore, to the extent that the term “include,” “have,” or the like is used in the description, including the claims, such term is intended to be inclusive in a manner similar to the term “comprise” as “comprise” is interpreted when employed as a transitional word in a claim.

[0103] A reference to an element in the singular is not intended to mean “one and only one” unless specifically stated, but rather “one or more.” The term “some” refers to one or more. All structural and functional equivalents to the elements of the various configurations described throughout this disclosure that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and intended to be encompassed by the subject technology. Moreover, nothing disclosed herein is intended to be dedicated to the public regardless of whether such disclosure is explicitly recited in the above description.

[0104] While this specification contains many specifics, these should not be construed as limitations on the scope of what may be claimed, but rather as descriptions of particular implementations of the subject matter. Certain features that are described in this specification in the context of separate embodiments can also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment can also be implemented in multiple embodiments separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a subcombination or variation of a subcombination.

[0105] Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system components in the aspects described above should not be understood as requiring such separation in all aspects, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

[0106] The subject matter of this specification has been described in terms of particular aspects, but other aspects can be implemented and are within the scope of the following claims. For example, the actions recited in the claims can be performed in a different order and still achieve desirable results. As one example, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. These and other implementations are within the scope of the following claims.

What is claimed is:

1. A computer-implemented method, the method comprising:

- receiving a request from a user to log into a communications server, wherein the request includes user credentials;
- authenticating the user based on the included user credentials in the request;
- permitting the user to log into the communications server if the user is successfully authenticated;
- receiving a first input selecting a person of interest;
- retrieving information associated with the selected person of interest;

- generating a dossier of information including the retrieved information associated with the selected person of interest; and

- transmitting the generated dossier to the user or an indicated recipient.

2. The method of claim 1, further comprising:

- receiving a second input defining one or more filters for restricting information associated with the selected person of interest;

- determining a set of user restrictions associated with the user;

- retrieving information associated with the selected person of interest based on the defined one or more filters and the determined set of user restrictions;

- receiving a third input selecting a download format for the retrieved information;

- generating a second dossier of information including the retrieved information associated with the selected person of interest; and

- transmitting the generated second dossier to the user or a respective indicated recipient based on the selected download format.

3. The method of claim 1, wherein the selected person of interest comprises a detainee.

4. The method of claim 2, wherein the defined one or more filters comprise at least one of a time period, type of data, a second person connected to the selected person of interest, or any person connected to the selected person of interest.

5. The method of claim 4, wherein the second person connected to the selected person of interest comprises a friend of the selected person of interest or family member of the selected person of interest.

6. The method of claim 1, wherein the generated dossier includes one or more checksum values for verifying the retrieved information included in the generated dossier.

7. The method of claim 1, wherein the retrieved information associated with the selected person of interest includes data pertaining to at least one of an audio file, video file, attempted call, completed call, rejected call, voicemail, message left for customer service, call to customer service representative, call to automated customer service, exchanged text, exchanged photo, exchanged video, video visit scheduled, video visit completed, kiosk deposit, deposit by mail, deposit over the phone, grievance or inmate request attempted, grievance or inmate request submitted, do not contact block via customer service, do not contact block via web site, investigator note, customer service note, visited website, game played, contact searched, video station login, web login by a friend or family, inmate balance check, or inmate balance transfer.

8. The method of claim 7, wherein all recording files and data are compressed or merged into a single downloadable file.

9. The method of claim 2, wherein the set of user restrictions associated with the user comprise at least one of user privileges, access to data, or download permissions.

10. The method of claim 1, wherein the selected download format comprises one of an e-mail including a link to the generated dossier, compressed file, Portable Document Format (PDF) file, MHTML file, or webarchive file.

11. The method of claim 10, wherein the link to the generated dossier expires after a predetermined period of time.

12. A system, the system comprising:
 a memory comprising instructions; and
 one or more processors configured to execute the instructions to:
 receive a request from a user to log into a communications server, wherein the request include user credentials;
 authenticate the user based on the included user credentials in the request;
 permit the user to log into the communications server if the user is successfully authenticated;
 receive a first input selecting a person of interest;
 receive a second input defining one or more filters for restricting information associated with the selected person of interest;
 determine a set of user restrictions associated with the user;
 retrieve information associated with the selected person of interest based on the defined one or more filters and the determined set of user restrictions;
 receive a third input selecting a download format for the retrieved information;
 generate a dossier of information including the retrieved information associated with the selected person of interest; and
 transmit the generated dossier to the user or an indicated recipient based on the selected download format.

13. The system of claim **12**, wherein the selected person of interest comprises a detainee.

14. The system of claim **12**, wherein the defined one or more filters comprise at least one of a time period, type of data, a second person connected to the selected person of interest, or any person connected to the selected person of interest.

15. The system of claim **14**, wherein the second person connected to the selected person of interest comprises a friend of the selected person of interest or family member of the selected person of interest.

16. The system of claim **12**, wherein the generated dossier includes one or more checksum values for verifying the retrieved information included in the generated dossier.

17. The system of claim **12**, wherein the retrieved information associated with the selected person of interest includes data pertaining to at least one of an audio file, video file, attempted call, completed call, rejected call, voicemail, message left for customer service, call to customer service representative, call to automated customer service, exchanged text, exchanged photo, exchanged video, video visit scheduled, video visit completed, kiosk deposit, deposit by mail, deposit

over the phone, grievance or inmate request attempted, grievance or inmate request submitted, do not contact block via customer service, do not contact block via web site, investigator note, customer service note, visited website, game played, contact searched, video station login, web login by a friend or family, inmate balance check, or inmate balance transfer.

18. The system of claim **17**, wherein all recording files and data are compressed or merged into a single downloadable file.

19. The system of claim **12**, wherein the set of user restrictions associated with the user comprise at least one of user privileges, access to data, or download permissions.

20. The system of claim **12**, wherein the selected download format comprises one of an e-mail including a link to the generated dossier, compressed file, Portable Document Format (PDF) file, MHTML file, or webarchive file.

21. The system of claim **20**, wherein the link to the generated dossier expires after a predetermined period of time.

22. A machine-readable medium comprising instructions stored therein, which when executed by a machine, cause the machine to perform operations comprising:

- receiving a request from a user to log into a communications server, wherein the request includes user credentials;
- authenticating the user based on the included user credentials in the request;
- permitting the user to log into the communications server if the user is successfully authenticated;
- receiving a first input selecting a person of interest;
- receiving a second input defining one or more filters for restricting information associated with the selected person of interest;
- determining a set of user restrictions associated with the user;
- retrieving information associated with the selected person of interest based on the defined one or more filters and the determined set of user restrictions;
- receiving a third input selecting a download format for the retrieved information;
- generating a dossier of information including the retrieved information associated with the selected person of interest; and
- transmitting the generated dossier to the user or an indicated recipient based on the selected download format.

* * * * *



US 20140273929A1

(19) **United States**

(12) **Patent Application Publication**
Torgersrud

(10) **Pub. No.: US 2014/0273929 A1**

(43) **Pub. Date: Sep. 18, 2014**

(54) **METHOD AND SYSTEM FOR FINANCING OF INMATE MOBILE DEVICES**

(52) **U.S. Cl.**
CPC *H04M 15/886* (2013.01); *H04W 4/24* (2013.01)

(71) Applicant: **TELMATE LLC**, San Francisco, CA (US)

USPC **455/406**

(72) Inventor: **Richard Torgersrud**, San Francisco, CA (US)

(57) **ABSTRACT**

(73) Assignee: **TELMATE LLC**, San Francisco, CA (US)

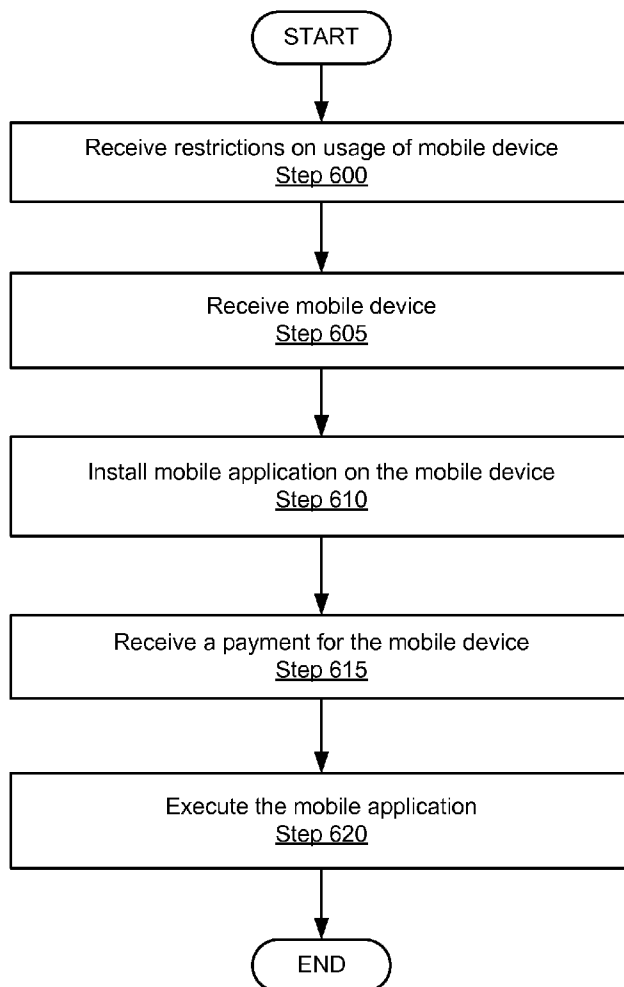
(21) Appl. No.: **13/837,150**

(22) Filed: **Mar. 15, 2013**

A method for financing a mobile device for an inmate involves receiving a plurality of mobile device rules comprising limitations on usage of the mobile device by the inmate within a controlled facility, receiving the mobile device, and installing, on the mobile device, a mobile application, wherein the mobile application conforms the mobile device to the plurality of mobile device rules. The method also involves receiving a payment for the mobile device, and executing, by the mobile device, the mobile application.

Publication Classification

(51) **Int. Cl.**
H04M 15/00 (2006.01)
H04W 4/24 (2006.01)



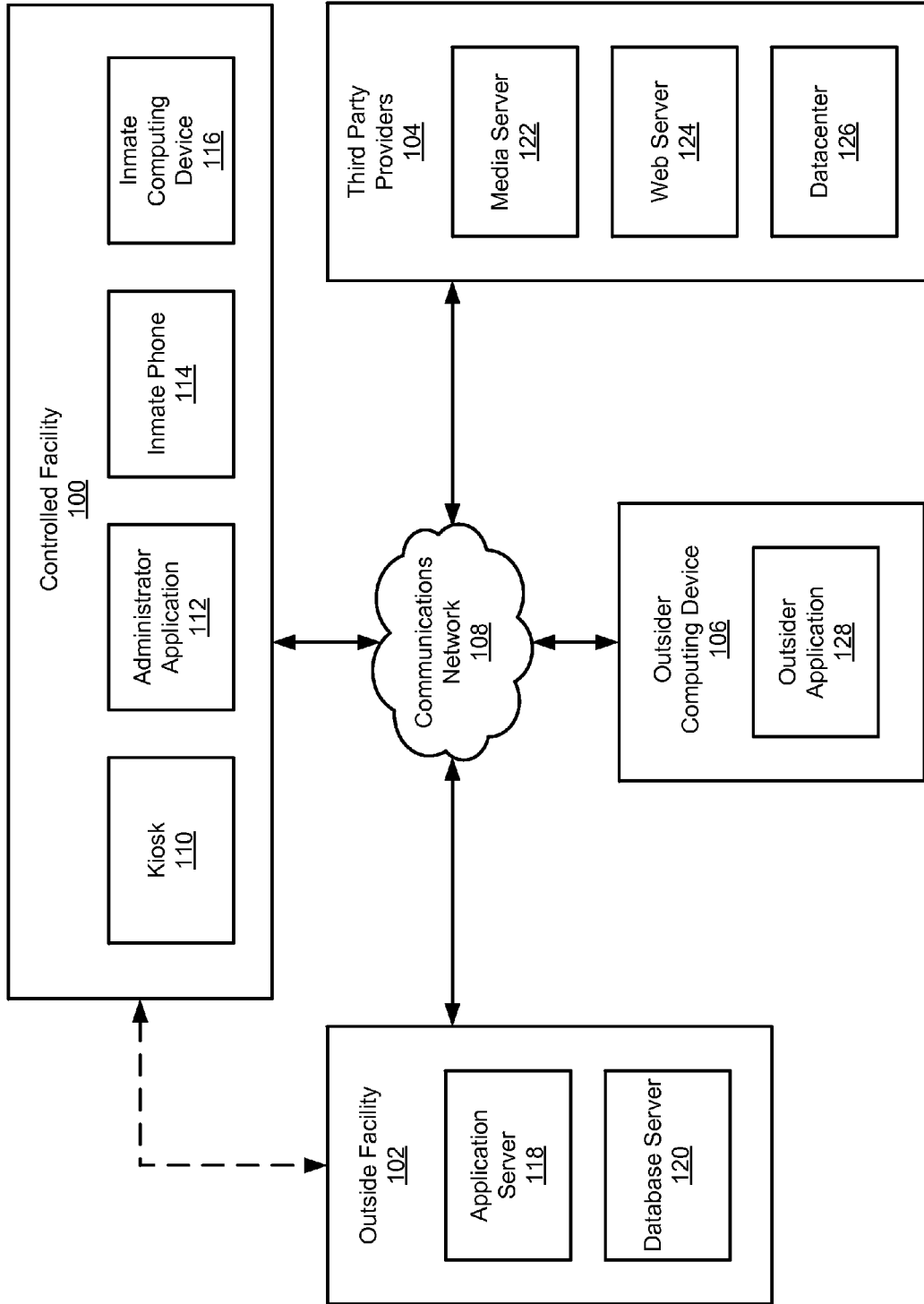


FIG. 1

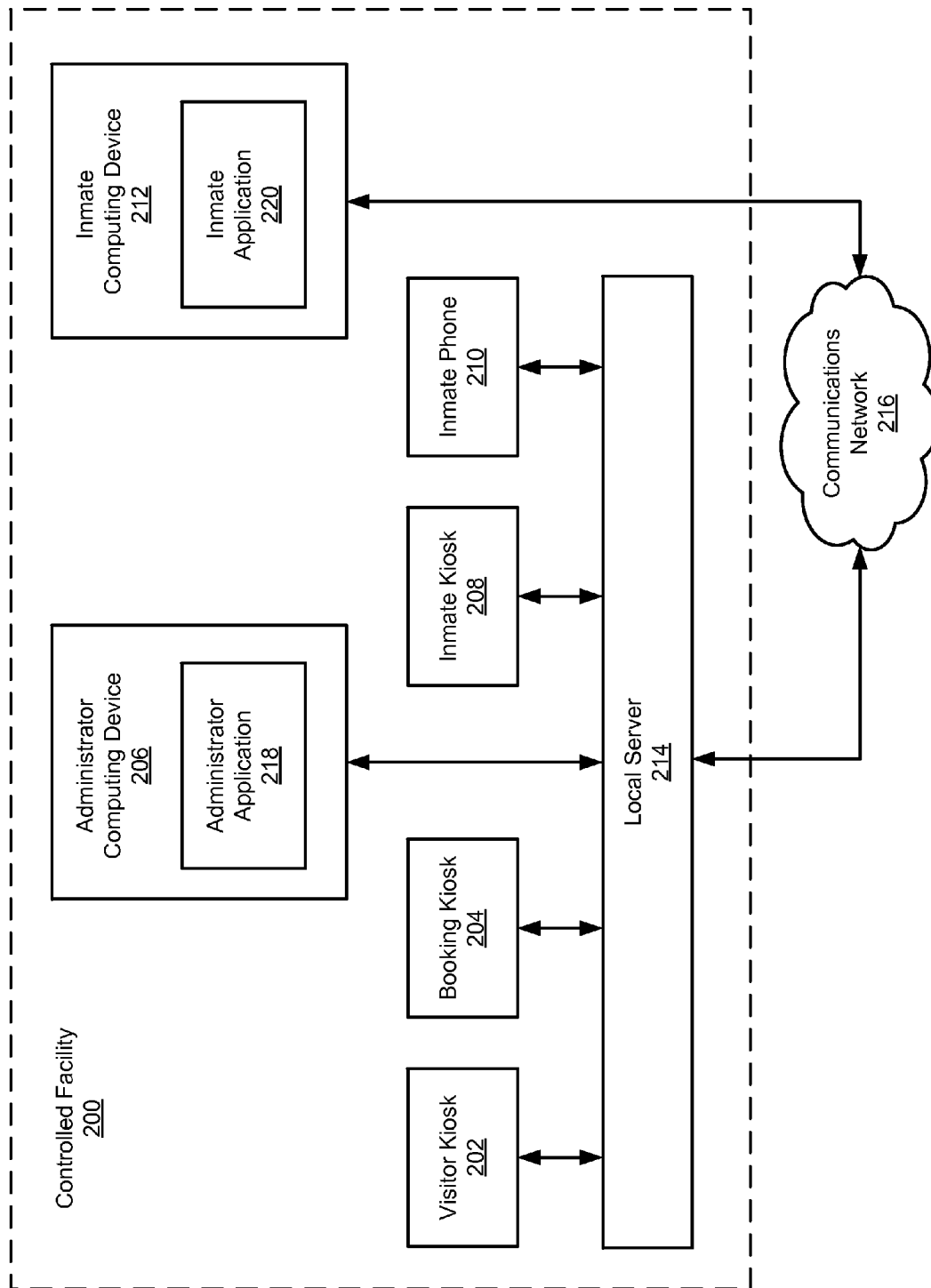


FIG. 2

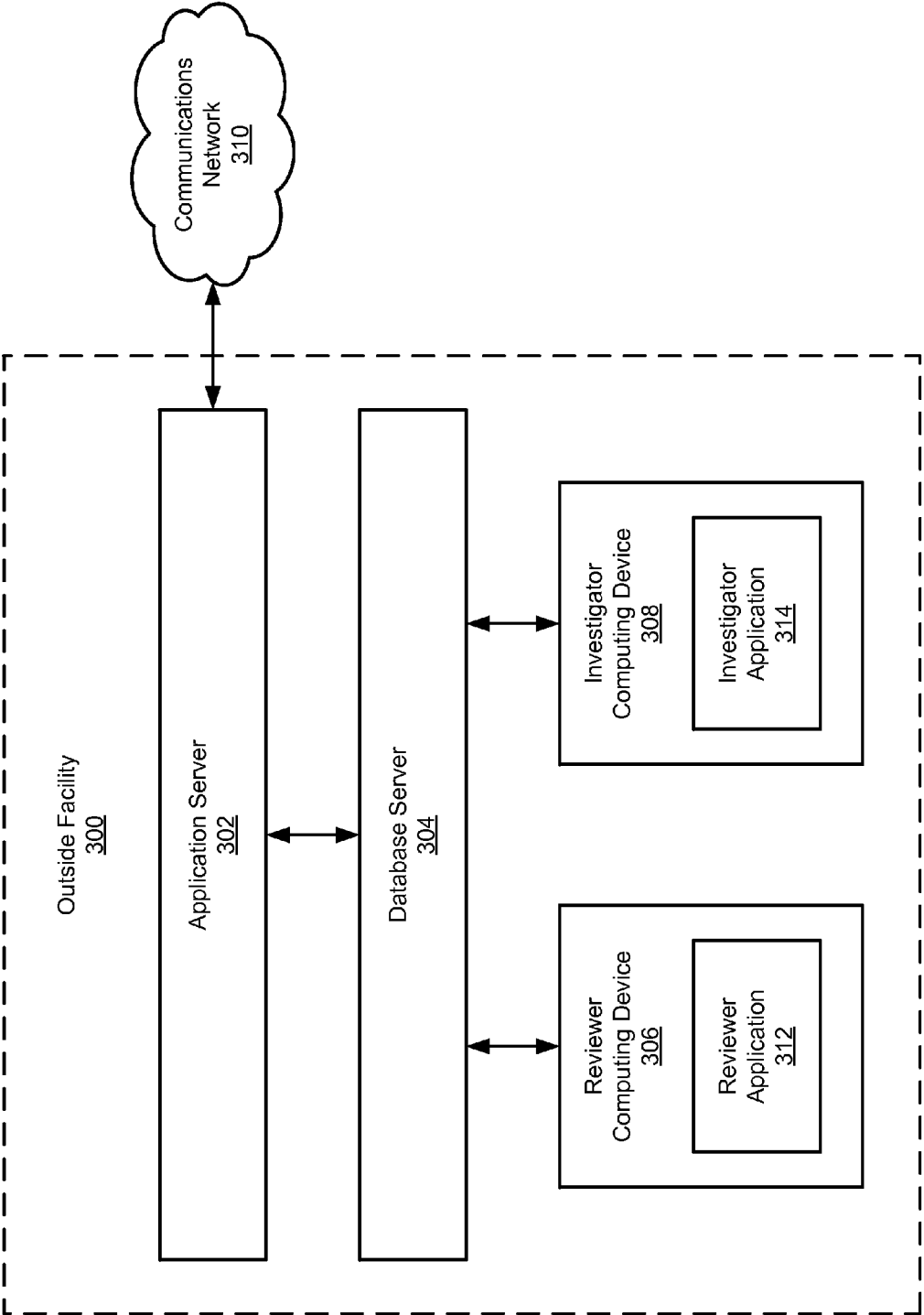


FIG. 3

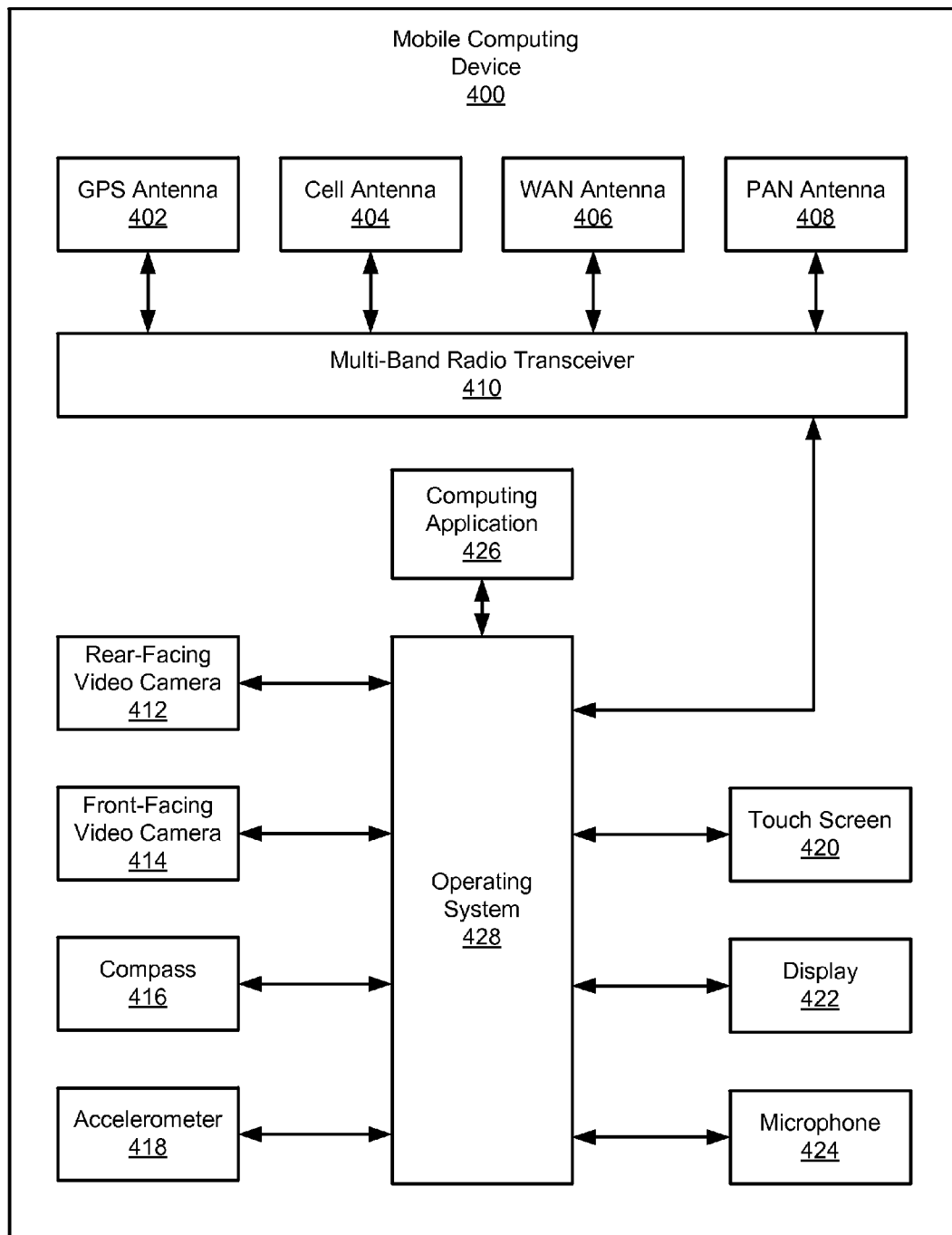


FIG. 4

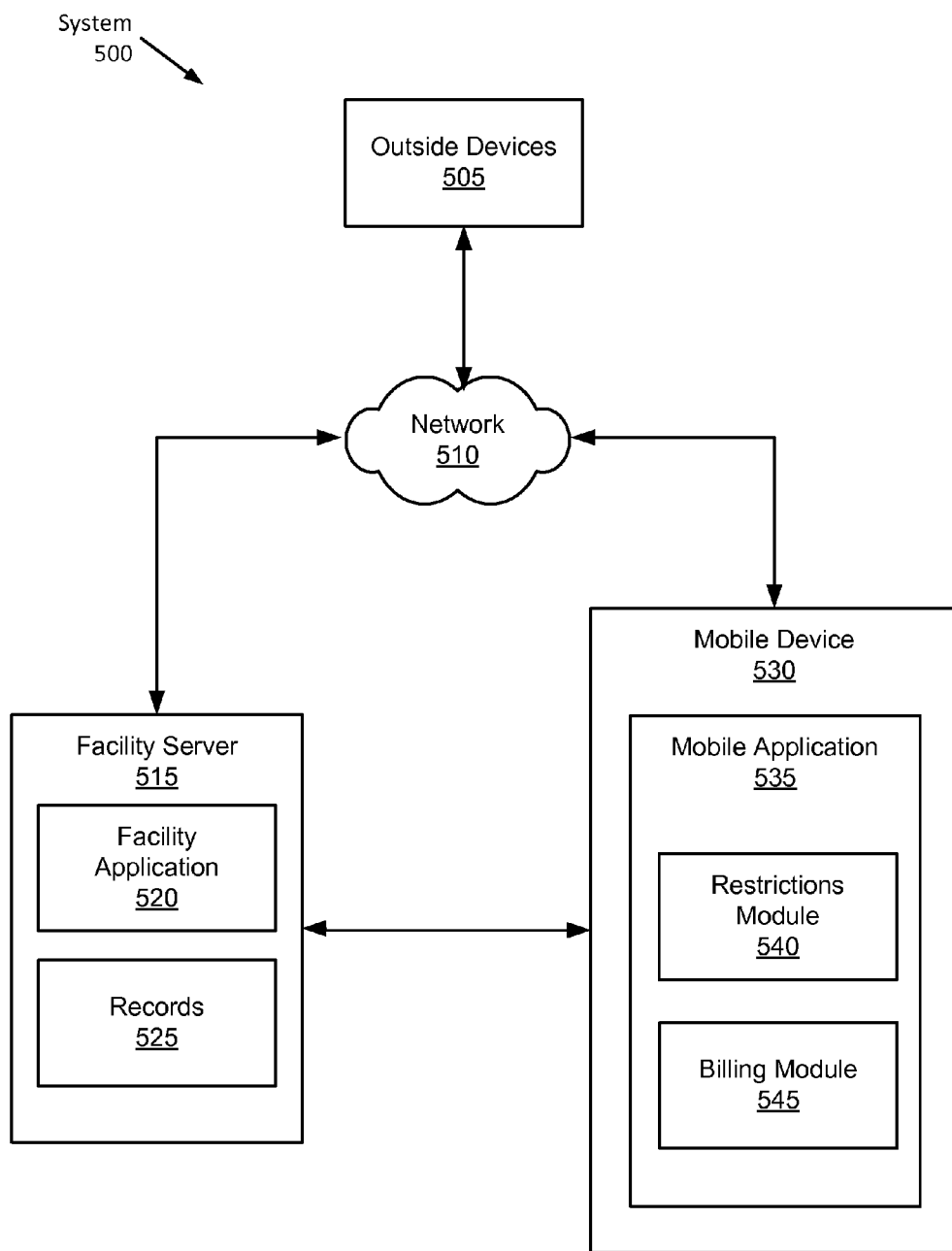


FIG. 5

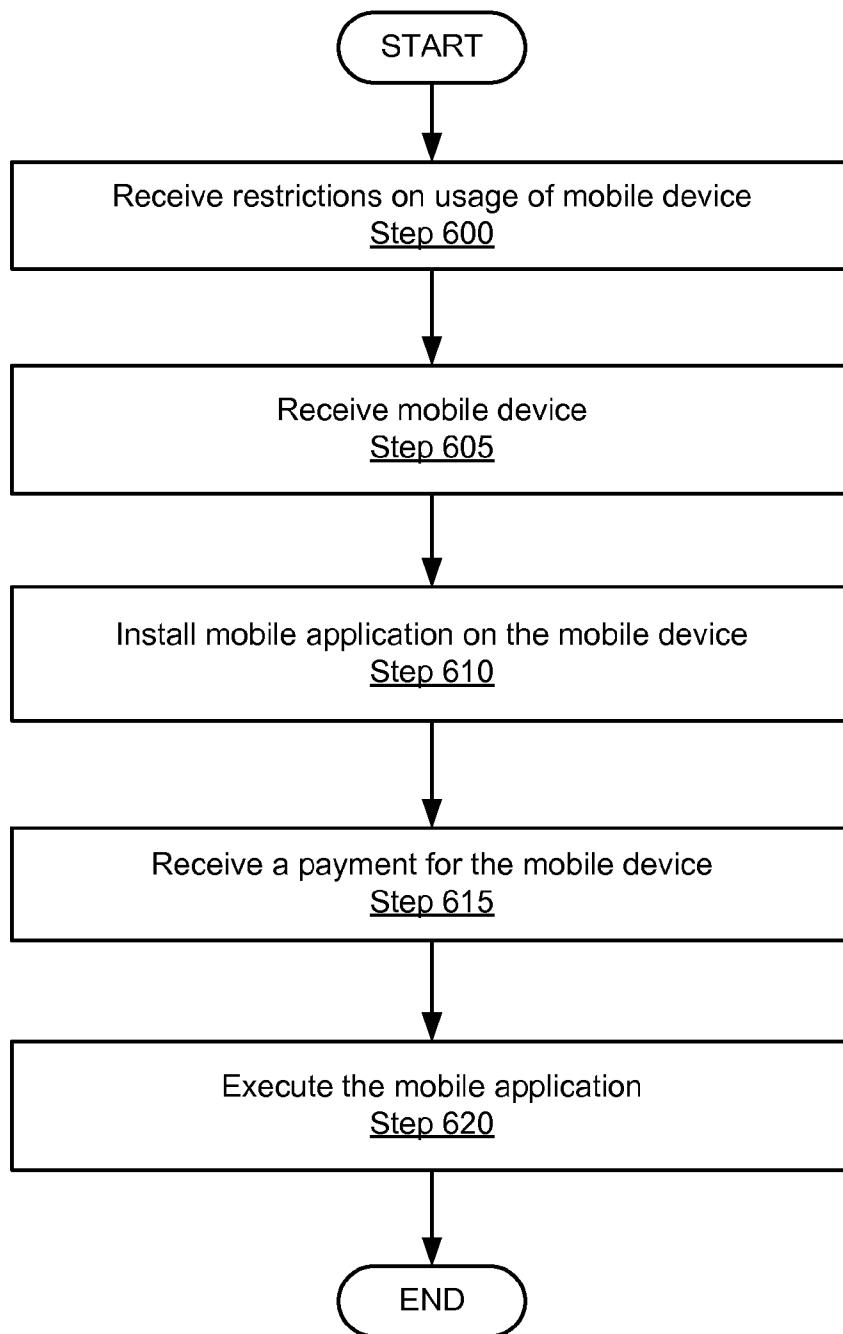


FIG. 6

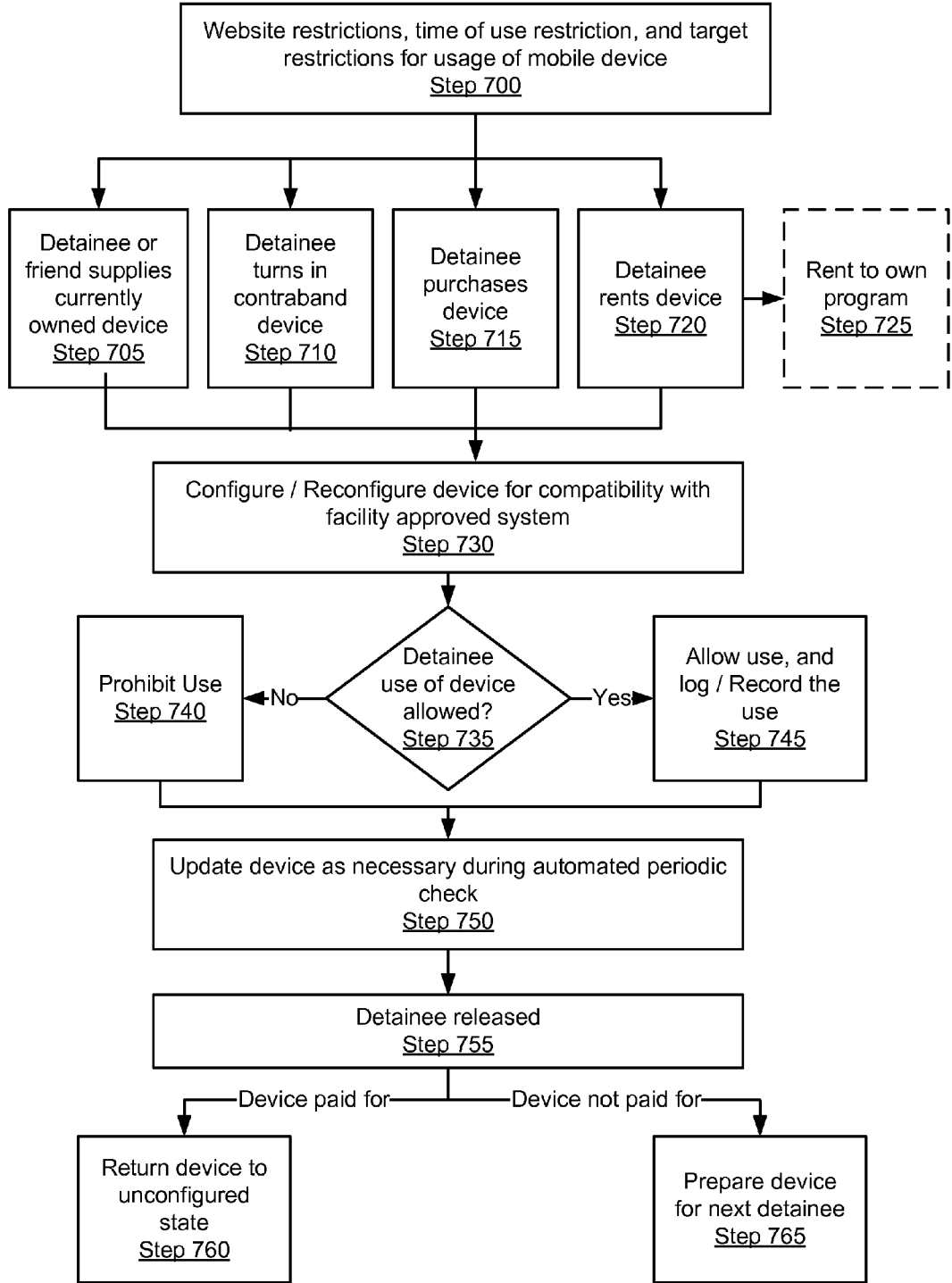


FIG. 7

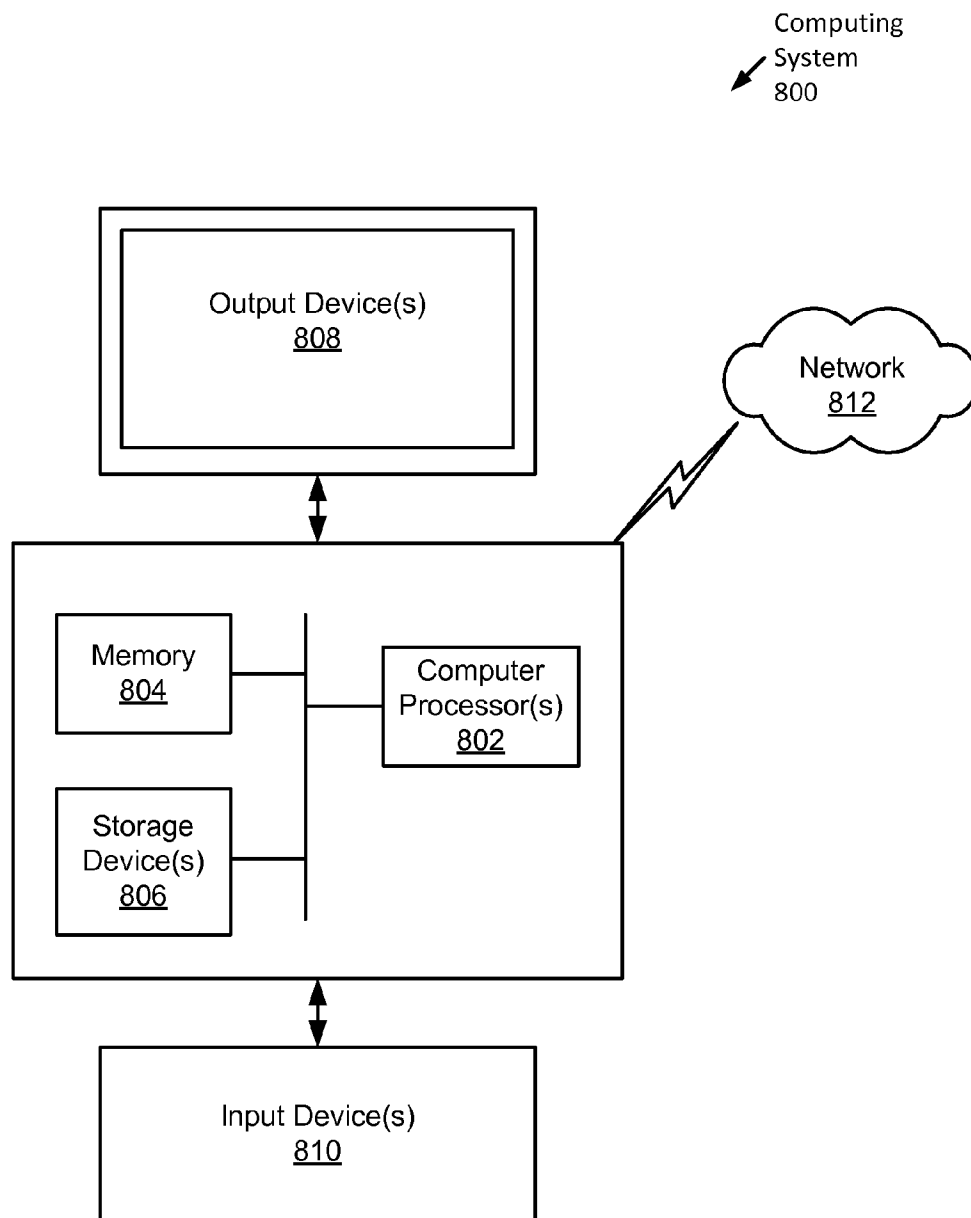


FIG. 8

METHOD AND SYSTEM FOR FINANCING OF INMATE MOBILE DEVICES

BACKGROUND

[0001] Controlled facilities, such as jails, prisons, secure detention environments, detention facilities, secured hospitals, or addiction treatment facilities, house large populations of individuals in confinement, which presents unique administrative challenges. In such detention environments, detained individuals, such as prisoners, offenders, convicts, military personnel, patients, government cleared personnel, or other detainees, frequently desire to communicate with individuals outside the detention environment such as friends or family members.

SUMMARY OF INVENTION

[0002] In general, in one aspect, the invention relates to a method for financing a mobile device for an inmate, comprising: receiving a plurality of mobile device rules comprising limitations on usage of the mobile device by the inmate within a controlled facility; receiving the mobile device; installing, on the mobile device, a mobile application, wherein the mobile application conforms the mobile device to the plurality of mobile device rules; receiving a payment for the mobile device; and executing, by the mobile device, the mobile application.

[0003] In general, in one aspect, the invention relates to a non-transitory computer-readable medium (CRM) storing a plurality of instructions for financing a mobile device for an inmate, the plurality of instructions comprising functionality to: receive a plurality of mobile device rules comprising limitations on usage of the mobile device by the inmate within a controlled facility; receive the mobile device; install, on the mobile device, a mobile application, wherein the mobile application conforms the mobile device to the plurality of mobile device rules; receive a payment for the mobile device; and execute the mobile application.

[0004] In general, in one aspect, the invention relates to a system for financing a mobile device for an inmate, comprising: a server, comprising functionality to: receive a plurality of mobile device rules comprising limitations on usage of the mobile device by the inmate within a controlled facility; receive the mobile device; receive a payment for the mobile device; the mobile device, comprising functionality to: install a mobile application, wherein the mobile application conforms the mobile device to the plurality of mobile device rules; and execute the mobile application.

[0005] Other aspects and advantages of the invention will be apparent from the following description and the appended claims.

BRIEF DESCRIPTION OF DRAWINGS

[0006] FIG. 1 shows a diagram of a system in accordance with one or more embodiments of the invention.

[0007] FIG. 2 shows a diagram of a controlled facility in accordance with one or more embodiments of the invention.

[0008] FIG. 3 shows a diagram of an outside facility in accordance with one or more embodiments of the invention.

[0009] FIG. 4 shows a diagram of a mobile computing device in accordance with one or more embodiments of the invention.

[0010] FIG. 5 shows a diagram of a system in accordance with one or more embodiments of the invention.

[0011] FIG. 6 shows a flowchart of a method in accordance with one or more embodiments of the invention.

[0012] FIG. 7 shows an example in accordance with one or more embodiments of the invention.

[0013] FIG. 8 shows a diagram of a computing system in accordance with one or more embodiments of the invention.

DETAILED DESCRIPTION

[0014] Specific embodiments of the invention will now be described in detail with reference to the accompanying figures. Like elements in the various figures are denoted by like reference numerals for consistency.

[0015] In the following detailed description of embodiments of the invention, numerous specific details are set forth in order to provide a more thorough understanding of the invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these specific details. In other instances, well-known features have not been described in detail to avoid unnecessarily complicating the description.

[0016] In general, embodiments of the invention provide a method and system for financing a mobile device for an inmate. Specifically, after rules governing the use of mobile devices by inmates are received, a mobile device is received, and a mobile application is installed on the mobile device which conforms the mobile device to the rules. A payment is received for the mobile device, and the inmate is able to use the mobile device and/or mobile application.

[0017] Embodiments of the invention may include interactions with a secure social network. In one embodiment of the invention, a secure social network is a network application that facilitates and secures the exchange or transmission of information between two or more parties in which at least one of those parties is subject to special security or law enforcement restrictions or otherwise is subject to the controls of a controlled facility. Exchanged or transmitted information may be member generated, such as a photo or a video message, or it may be member-curated, such as a news headline, a famous quote, or a sports score.

[0018] FIG. 1 shows a diagram of a system in accordance with one or more embodiments of the invention. As shown in FIG. 1, the system includes a controlled facility (100), an outside facility (102), third party providers (104), and an outsider computing device (106) each communicatively coupled to a communications network (108). The controlled facility (100) may include, but is not limited to, a kiosk (110), an administrator application (112), an inmate phone (114), and an inmate computing device (116). The outside facility (102) may include an application server (118) and a database server (120). The third party providers (104) may include a media server (122), a web server (124), and a datacenter (126). The outsider computing device (106) may include an outsider application (128).

[0019] In one or more embodiments of the invention, a controlled facility (100) is an access-restricted location. Examples of controlled facilities (e.g., controlled facility (100)) include, but are not limited to, detention environments (e.g., jails, prisons, etc.), immigration detention centers, military centers, government secure sites, law enforcement holding structures, and psychiatric hospitals.

[0020] In one or more embodiments of the invention, an inmate is a person within a controlled facility (100) who is subject to one or more restrictions, primarily to his or her freedom or rights. Examples of inmates include, but are not

limited to, prisoners, wards of the state, parolees, employees working in a secure office complex, temporary or long-term internees, patients, military personnel, uncharged suspects, and refugees. Inmate restrictions may be part of a court-imposed sentence on an inmate, while others may be specific to the controlled facility (100) exerting control over the inmate. Restrictions may include limitations on an inmate's physical movement (i.e., physical restrictions) and limitations on the inmate's ability to communicate (i.e., communication restrictions). Communication restrictions include inmate use restrictions, inmate target restrictions, and device use restrictions.

[0021] In one or more embodiments of the invention, inmate use restrictions are limitations on an inmate's general ability to communicate with visitors and/or outsiders. Inmate use restrictions may include, for example, periods of time in which an inmate is not allowed to communicate with outsiders or visitors (e.g., between 10 PM and 8 AM, during an imposed one-week punitive period, etc.) and limitations based on lack of funds (e.g., communication account balance to initiate a communication).

[0022] In one or more embodiments of the invention, inmate target restrictions are limitations on the target or source of a communication with the inmate. Inmate target restrictions may be specific outsiders or visitors with whom the inmate is not allowed to communicate (e.g., the victim of a crime perpetrated by the inmate, etc.). Inmate target restrictions may also include types of people with whom the inmate is not allowed contact (e.g., outsiders who are ex-cons, minors under the age of 18, etc.).

[0023] In one or more embodiments of the invention, device use restrictions are restrictions based on the condition or state of the communication device used by the inmate. Device use restrictions include, for example, limitations based on the location of the inmate's mobile device, limitations imposed based on a determination that the device has been tampered with, etc.

[0024] In one or more embodiments of the invention, an outsider is a person outside the controlled facility (100) who may be the source or target of a communication with an inmate. An outsider who enters the controlled facility (100) for the purpose of communicating with an inmate is referred to as a visitor.

[0025] In one or more embodiments of the invention, the kiosk (110) is a computing system with functionality to facilitate communication between an inmate and a visitor or outsider. Such communication facilitation may include creating a system identity data item or secure social networking account, adding or importing contact information for outsiders with whom the inmate wishes to communicate, uploading media (e.g., photos, videos, audio, and text) to, or viewing media from, a secure social network, sending or receiving messages or other media, acting as an endpoint for voice and video communication between an inmate and a visitor or outsider, scheduling a communication, and managing a commissary account.

[0026] In one or more embodiments of the invention, the administrator application (112) is a process or group of processes executing on a computing system with functionality to enable an administrator to create, remove, and/or enforce one or more restrictions on an inmate, device, visitor, and/or outsider. In one embodiment of the invention, an administrator is a person associated with the controlled facility charged with enforcing one or more restrictions. Examples of administra-

tors include, but are not limited to, prison guards, orderlies, wardens, prison staff, jailers, information technology technicians, system administrators, and law enforcement agents. Using the administrator application, an administrator may retrieve or alter the identity data item and/or secure social network account of an inmate, visitor, or outsider. Further detail about the administrator application (112) is provided in FIG. 2.

[0027] In one or more embodiments of the invention, the inmate phone (114) is a device with functionality to send and receive audio communications between an inmate and an outsider or visitor. In one embodiment of the invention, the inmate phone (114) is a stationary (i.e., non-mobile) device. Further, a single inmate phone (114) may be used by more than one inmate. Further detail about the inmate phone (114) is provided in FIG. 2.

[0028] In one or more embodiments of the invention, the inmate computing device (116) is a computing device with functionality to enable an inmate to communicate with a visitor or outsider. Specifically, the inmate computing device (116) may be used to send or receive text messages and/or initiate or receive voice or video calls. In one embodiment of the invention, the inmate computing device (116) also enables an inmate to access a secure social network. Specifically, the inmate computing device (116) may be used to upload media to, or view media from, a secure social network account of the inmate or another secure social network member. In one embodiment of the invention, the inmate computing device (116) is a mobile computing device (e.g., a smartphone, a laptop, a tablet, etc.). Further detail about the inmate computing device (116) is provided in FIG. 2 and FIG. 4.

[0029] In one or more embodiments of the invention, the elements within the controlled facility (100) are communicatively coupled to the communications network (108). In one embodiment of the invention, the communications network (108) is a collection of computing systems and other hardware interconnected by communication channels. The communications network (108) may include networks that are exclusively or primarily used for a single type of communication, such as a telephone network (e.g., Plain Old Telephone System (POTS)), and/or networks used for a wide array of communication types, such as the Internet through Voice over IP (VoIP). Communication channels used by the communications network (108) may include, for example, telephone lines, networking cables, wireless signals, radio waves, etc. Fees charged and payments received by the provider(s) of the communications network (108) may involve multiple parties, including a service provider of the outside facility (102), the management of the controlled facility (100), and provider(s) of the communications network (108). In one or more embodiments of the invention, fees may be split between multiple parties based on the terms of underlying agreements or contracts between the parties. Further, rebates, reimbursements, and/or refunds may be afforded to and paid to the management of the controlled facility (100) based on the terms of underlying agreements or contracts between the parties. For example, the management of the controlled facility (100) may receive a rebate from the service provider of the services provided to inmates based on such factors as the volume of use, the dollar amount, and/or the frequency of use.

[0030] In one or more embodiments of the invention, the outside facility (102) is a group of computing systems located outside of the controlled facility (100). Specifically, the out-

side facility (102) may house system elements with functionality to facilitate communication between inmates and outsiders, access communication data between inmates and outsiders, and enforce one or more restrictions imposed on inmates and inmate communications. In one or more embodiments of the invention, the outside facility (102) is connected directly to the controlled facility (100) bypassing a generally accessible communications network (communications network (108)). One or more of the components within the outside facility (102) may alternatively be located within the controlled facility (100) or within the third party providers (104).

[0031] In one or more embodiments of the invention, the application server (118) is a computing system with functionality to authenticate an inmate, outsider, administrator, reviewer, or investigator for access to system functionality (e.g., initiating voice or video calls, sending text messages, etc.) or data stored on the database server (120) (e.g., inmate identities, communications between inmates and outsiders, etc.). The application server may authenticate inmates, outsiders, administrators, reviewers, and/or investigators using passwords, biometric data, digital access codes, and/or physical access devices. Further detail about the application server (118) is provided in FIG. 3.

[0032] In one or more embodiments of the invention, the database server (120) is a computing system with functionality to store identities used to authenticate inmates, outsiders, administrators, reviewers, and/or investigators. Such identities may include verified data used to compare to verification data provided by the inmate, outsider, administrator, reviewer, or investigator to authenticate the inmate, outsider, administrator, reviewer, or investigator.

[0033] In one or more embodiments of the invention, the database server (120) also stores communication data about communications between an inmate and an outsider or visitor. Such communication data may include, for example, a recording of a video call, the length of a voice call, the frequency of video calls, sent and received text messages, etc. The database server (120) may also store media submitted to a secure social network before, during, and/or after the media has been reviewed. Further detail about the database server (120) is provided in FIG. 3.

[0034] In one or more embodiments of the invention, the third party providers (104) are computing systems that provide network application and data storage services (i.e., cloud computing services). Third party providers (104) may include service providers used directly by inmates and outsiders, such as photo sharing services, general social networking sites, and digital music retailers. Third party providers (104) may include service providers employed by administrators and for use by inmates and outsiders, such as audio and video streaming applications, conferencing applications, and secure social network media storage. One or more of the components within the third party providers (104) may alternatively be located within the controlled facility (100) or the outside facility (102).

[0035] In one or more embodiments of the invention, the media server (122) is a computing system or group of computing system with functionality to provide network application services to facilitate communication between an inmate and an outsider, and to facilitate access to a secure social network. Such services include, but are not limited to, VoIP services, video conferencing services, and media streaming services.

[0036] In one or more embodiments of the invention, the web server (124) is a computing system or group of computing system with functionality to provide an interface to access and interact with webpages and other network application services. In one embodiment of the invention, the web server (124) is a type of media server (122).

[0037] In one or more embodiments of the invention, the datacenter (126) is a computing system or group of computing system with functionality to provide an interface to access and interact with data stored on one or more data servers (not shown). In one embodiment of the invention, the datacenter (126) is a type of media server (122).

[0038] In one or more embodiments of the invention, the outsider computing device (106) is a computing device with functionality to execute the outsider application (128). In one or more embodiments of the invention, the outsider computing device (106) is a mobile computing device (e.g., a smartphone, a laptop, a tablet, etc.). Further detail about the outsider computing device (106) is provided in FIG. 6.

[0039] In one or more embodiments of the invention, the outsider application (128) is a process or group of processes (in software, firmware, hardware, or combination thereof) with functionality to enable communication between an outsider and an inmate. Specifically, the outsider application (128) may be used to send or receive text messages and/or initiate or receive voice or video calls. In one embodiment of the invention, the outsider application (128) also enables an outsider to access a secure social network. Specifically, the outsider application (128) may be used to upload media to, or view media from, a secure social network account of the outsider, an inmate, other secure social network member.

[0040] FIG. 2 shows a controlled facility in accordance with one or more embodiments of the invention. As shown in FIG. 2, the controlled facility (200) may include a visitor kiosk (202), a booking kiosk (204), an administrator computing device (206), an inmate kiosk (208), an inmate phone (210), an inmate computing device (212), and a local server (214). The inmate computing device (212) and the local server (214) are communicatively coupled to the communications network (216). The administrator computing device (206) includes an administrator application (218). The inmate computing device (212) includes an inmate application (220).

[0041] In one or more embodiments of the invention, the visitor kiosk (202) is a computing system with functionality to facilitate communication between an inmate and a visitor. Specifically, the visitor kiosk (202) may be a combination of computing hardware and software used by a visitor to make and receive voice and video calls to/from an inmate residing in the same controlled facility (200) or another controlled facility (not shown). The visitor kiosk (202) may also be used to schedule a voice or video call with an inmate for a future date. Further, the visitor kiosk (202) may also include the functionality to exchange media (e.g., photos, videos, and audio) with an inmate residing in the controlled facility (200). The visitor kiosk (202) may include functionality to generate such media, such as a camera, microphone, keyboard, and software to record or otherwise create media to send to an inmate. Such media may be subject to review before being delivered.

[0042] In one or more embodiments of the invention, a visitor wanting to use a visitor kiosk (202) may be required to participate in an authentication process to verify the identity of the visitor. The authentication process may include creating an identity data item and verified data for storage and later

comparison. The verified data used for authentication may be a username and password combination and/or biometric information about the visitor.

[0043] In one or more embodiments of the invention, the visitor kiosk (202) includes functionality to access a secure social network. Specifically, the visitor kiosk (202) may be used by a visitor to create and manage a secure social network account. The visitor kiosk (202) may also be used by a visitor to upload digital media to the visitor's secure social network account or the account of another secure social network member. The visitor kiosk (202) may further be used to view digital media uploaded to the visitor's social network account or the account of another secure social network member.

[0044] In one or more embodiments of the invention, the visitor kiosk (202) includes functionality to manage a commissary account and/or communication account for one or more inmates. Specifically, a visitor may use a visitor kiosk (202) to add money to the commissary account and/or communication account of an inmate in the controlled facility (200), view a transaction history of the commissary account and/or or communication account, transfer funds between commissary accounts and/or or communication accounts, and/or remove funds from a commissary account and/or or communication account.

[0045] In one or more embodiments of the invention, the booking kiosk (204) is a computing system with functionality to aid administrators in admitting an inmate into a controlled facility (e.g., controlled facility (200)). Specifically, the booking kiosk (204) may include functionality to create or update an inmate identity data item. Specifically, the booking kiosk (204) may be used to obtain verified data (e.g., passwords, biometric data, etc.) and save the verification data in one or more identity data items for the inmate. The verified data may then be used to authenticate the inmate for access to the communications network (216). In one embodiment of the invention, the booking kiosk may also be used to associate one or more restrictions with the inmate via the inmate's identity data item.

[0046] In one or more embodiments of the invention, the booking kiosk (204) includes functionality to input contact information for visitors, outsiders, administrators, or other inmates with whom the inmate wants to communicate. Such contact information may then be associated with the inmate's identity data item, and may be used to initiate a voice or video call, or otherwise transmit media to visitors, outsiders, or other inmates. Further, in one embodiment of the invention, the contact information may be retrieved from an inmate's mobile computing device (e.g., cell phone, smart phone, etc.) or a local or remote data storage device (e.g., a flash drive, a webmail account, etc.). The contact information may be retrieved using a wired or wireless connection between the booking kiosk and the inmate's mobile computing device and/or the data storage device. The contact information may be subject to review before the inmate is permitted to contact the visitor, outsider, administrator, or other inmate.

[0047] In one or more embodiments of the invention, the booking kiosk (204) includes functionality to prepare a mobile computing device for use by the inmate within the controlled facility (200). Specifically, a controlled facility (200) may allow inmates the use of computing devices while residing in or subject to the controlled facility (200). However, use of such inmate computing devices may require that the computing device is instrumented with software restrict-

ing the use of the inmate computing device. The booking kiosk (204) may be used to instrument the inmate computing device as required.

[0048] In one or more embodiments of the invention, the administrator computing device (206) is a computing system or group of computing systems with functionality to execute the administrator application (218). In one embodiment of the invention, the administrator application (218) is a process or group of process with functionality to provide access to communications between inmates at the controlled facility (200) and visitors, outsiders, administrators, and other inmates. The administrator application (218) may also be used to monitor current voice or video calls between an inmate and a visitor, outsider, administrator, or other inmate.

[0049] In one embodiment of the invention, the administrator application (218) is used to manage an identity data item associated with an inmate. Such management may include altering the restrictions (device use restrictions, inmate use restrictions, and inmate target restrictions) applicable to the inmate. In one embodiment of the invention, the administrator application (218) is used to access the secure social network account of an inmate, visitor, or outsider. In one embodiment of the invention, the administrator application (218) may provide heightened access (i.e., a level of access greater than that of the inmate, visitor, or outsider) to data stored in the secure social networking account.

[0050] In one or more embodiments of the invention, the inmate kiosk (208) is a computing system with functionality to facilitate communication between an inmate and a visitor or outsider. Specifically, the inmate kiosk (208) may be a combination of computing hardware and software used by an inmate to make and receive voice and video calls to/from a visitor, outsider, or another inmate residing in another controlled facility (not shown). The inmate kiosk (208) may also be used to schedule a voice or video call with a visitor at a future date. Initiating or scheduling a voice or video call may include determining whether the currently attempted call or the scheduled call are adverse to one or more restrictions (e.g., inmate use restrictions, device use restrictions, and/or inmate target restrictions). Further, the inmate kiosk (208) may also include the functionality to exchange media (e.g., photos, videos, and audio) with a visitor or outsider. The inmate kiosk (208) may include functionality to generate such media, such as a camera, microphone, keyboard, and software to record or otherwise create media to send to a visitor or outsider. Such media may be subject to review before being delivered.

[0051] In one or more embodiments of the invention, an inmate wanting to use an inmate kiosk (208) may be required to participate in an authentication process to verify the identity of the inmate. The authentication process may include providing verification data for comparison to verified data previously obtained from the inmate and stored in the inmate identity data item. The verified data may be a username and password combination and/or biometric information about the inmate.

[0052] In one or more embodiments of the invention, the inmate kiosk (208) includes functionality to access a secure social network. Specifically, the inmate kiosk (208) may be used by an inmate to manage a secure social network account. The inmate kiosk (208) may also be used by an inmate to upload digital media to the inmate's secure social network account or the account of another secure social network member. The inmate kiosk (208) may further be used to view digital media uploaded to the inmate's social network

account or the account of another secure social network member. Uploaded media may be subject to review before posting.

[0053] In one or more embodiments of the invention, the inmate kiosk (208) includes functionality to manage a commissary account for the inmate. Specifically, an inmate may use an inmate kiosk (208) to view a transaction history of the commissary account and/or to apply commissary funds for goods and services consumed or enjoyed by the inmate.

[0054] In one or more embodiments of the invention, the inmate phone (210) is a device with functionality to send and receive audio communications between an inmate and an outsider or visitor. The inmate phone (210) may be implemented as handset connected to a telephone line. In one embodiment of the invention, all or part of the voice call may be conducted over a VoIP connection. In one embodiment of the invention, a single inmate phone (210) is utilized by multiple inmates.

[0055] In one embodiment of the invention, initiating or receiving a voice call using the inmate phone (210) requires a form of authentication (e.g., providing a password, personal identification number, or voice verification). In one embodiment of the invention, voice calls made using the inmate phone (210) are monitored by one or more administrators using the administrator computing device (206), and are recorded and stored in a data storage system within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown). The inmate phone (210) may also be subject to device use restrictions limiting the ability to use the inmate phone (210) at certain times (e.g., between 9 PM and 8 AM) or under certain conditions (e.g., emergency lockdown).

[0056] In one embodiment of the invention, the identity of the visitor or outsider targeted by the inmate or attempting to contact the inmate using the inmate phone (210) is verified against inmate target restrictions imposed on the inmate. Such restrictions may be associated with the inmate's identity data item and may be stored locally within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown). The visitor or outsider identity may be verified by the local server (214) or by another server within the outside facility (not shown), or within a third party provider (not shown).

[0057] In one or more embodiments of the invention, the inmate computing device (212) is a computing system configured to execute the inmate application (202). In one embodiment of the invention, each inmate computing device (212) is utilized exclusively by a single inmate. In one embodiment of the invention, access to the inmate application requires a form of initial authentication. This initial authentication may use verification data stored locally on the inmate computing device (212) (e.g., a code or combination used to unlock the phone, locally stored biometric data, etc.).

[0058] In one or more embodiments of the invention, accessing a communications network (e.g., communications network (216)) using the inmate application (220) may require further network-based authentication. This further authentication may use verification data stored external to the inmate computing device (212) but locally within the controlled facility (200), or remotely within the outside facility (not shown) or within a third party provider (not shown).

[0059] In one or more embodiments of the invention, an authenticated inmate may use the inmate application to initiate or receive voice or video calls, initiate or receive text or media messages, schedule a voice or video call, manage a

commissary account, manage a communication account, and/or post media to a secure social network. In one embodiment of the invention, voice and video calls made using the inmate computing device (212) are monitored by one or more administrators using the administrator computing device (206), and are recorded and stored in a data storage system within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown).

[0060] In one embodiment of the invention, the identity of the visitor or outsider targeted by the inmate or attempting to contact the inmate using the inmate computing device (212) is verified against inmate target restrictions imposed on the inmate. Such restrictions may be associated with the inmate's identity data item and may be stored locally within the controlled facility (200), within the outside facility (not shown), or within a third party provider (not shown). The visitor or outsider identity may be verified by the local server (214) or by another server within the outside facility (not shown), or within a third party provider (not shown).

[0061] In one or more embodiments of the invention, the inmate computing system (212) and/or the inmate application (220) may limit access to the communications network (216) based on one or more restrictions (inmate use restrictions, inmate target restrictions, and device use restrictions). Further, the inmate computing system (212) and/or the inmate application (220) may gather data from input devices of the inmate computing system (212) to determine whether one or more restrictions apply. Such input devices may include, for example, a system clock, a global positioning system antenna, a wide area network antenna, etc.

[0062] In one or more embodiments of the invention, the local server (214) is a computer system or group of computers systems located within the controlled facility (200) that facilitate communication between inmates and visitors, outsiders, and/or other inmates. Specifically, the local server (214) may implement the software necessary to host voice and video calls between and among the visitor kiosk (202), the inmate kiosk (208), the inmate phone (210), and an outsider computing system (not shown). The local server (214) may also include functionality to enforce communication restrictions associated with the inmates using the inmate kiosk (208) or inmate phone (210). Alternatively, the local server (214) may merely provide access to other systems capable of hosting the communication software and data storage (e.g., located within an offsite facility or a third party provider). Further, in one embodiment of the invention, the local server (214) includes functionality to regulate inmate access to a secure social network.

[0063] FIG. 3 shows an outside facility in accordance with one or more embodiments of the invention. As shown in FIG. 3, the outside facility (300) includes an application server (302), a database server (304), a reviewer computing system (306), and an investigator computing system (308). The application server (302) is communicatively coupled to the communications network (310). The reviewer computing device (306) includes a reviewer application (312), and the investigator computing device (308) includes an investigator application (314).

[0064] In one or more embodiments of the invention, the application server (302) is a computing system or group of computing systems configured to authenticate inmates, visitors, outsiders, administrators, reviewers, and/or investigators. Specifically, the application server (302) includes functionality to receive a request to authenticate an inmate, visitor,

outsider, administrator, reviewer, and/or an investigator, retrieve verified data associated with the request, and compare the verified data to verification data submitted in the authentication request. In one or more embodiments of the invention, the application server provides access to identity data items and other data stored in the database server (304).

[0065] In one or more embodiments of the invention, the database server (304) is a computing system or group of computing system configured to store data about inmates, visitors, outsiders, administrators, reviewers, and/or investigators as well as communication data describing communications between and among inmates, visitors, outsiders, administrators, reviewers, and/or investigators. Data stored in the database server may include, but is not limited to, identity data items, verified data, approved communication media, communication media pending review

[0066] In one or more embodiments of the invention, the reviewer computing device (306) is a computing system configured to execute the reviewer application (312). In one embodiment of the invention, a reviewer is a person charged with viewing a media item submitted by an inmate, visitor, or outsider, and determining one or more attributes of the media item. Based on the determined attributes of the media item, the reviewer may then approve the media item for transmission to its target inmate, visitor, or outsider. Alternatively, the reviewer may reject, conditionally approve, or redact the media item, thus preventing or altering the transmission to its target inmate, visitor, administrator, or outsider. In one embodiment of the invention, the reviewer application (312) include functionality to view media items, associate one or more attributes to the media item, and/or mark the media items as approved or rejected.

[0067] In one or more embodiments of the invention, the investigator computing device (308) is a computing system configured to execute the investigator application (314). In one embodiment of the invention, an investigator is a person gathering information about an inmate, visitor, or outsider generally for the purposes of law enforcement. The investigator application (314) includes functionality to provide access to data stored on the database server (304) for investigative purposes.

[0068] FIG. 4 shows the hardware and software elements of a mobile computing device in accordance with one or more embodiments of the invention. Specifically, the mobile computing device (400) is a portable device that provides a user interface. Examples of mobile devices may include, but are not limited to, cellular phones, personal digital assistants, personal communicators, pagers, smart phones, or any other computing device. The hardware and software elements shown in FIG. 4 may be in addition to the elements described in FIG. 8.

[0069] As shown in FIG. 4, the mobile computing device (400) includes a global positioning system (GPS) antenna (402), a cell antenna (404), a wide area network (WAN) antenna (406), and a personal area network (PAN) antenna (408), each connected to a multi-band radio transceiver (410). GPS antenna (402) includes functionality to obtain a location coordinate of the mobile computing device (400). Mobile computing device (400) may be configured to use the GPS antenna (402) to provide latitude and longitude location coordinates. In one or more embodiments of the invention, the network connection (i.e., via antenna (402), cell antenna (404), WAN antenna (406), PAN antenna (408), and/or multi-band radio transceiver (410)) may be facilitated by a wireless

infrastructure (not shown), including one or more transceivers cooperating to facilitate wireless communications to wireless devices. The wireless infrastructure may include one or more routers, switches, microwave links, base stations, optical fibers, or other similar networking hardware or software components. For example, the wireless infrastructure may be a paging network, a cellular network, etc.

[0070] The mobile computing device (400) may also include a rear-facing video camera (412), a front-facing video camera (414), a compass (416), an accelerometer (418), a touch screen (420), a display (422), and a microphone (424), all of which may include any functionality or features now known or later developed. The mobile computing device (400) may also include a computing application (426) executing on an operating system (428).

[0071] FIG. 5 shows a diagram of a system for financing a mobile for an inmate. Specifically, the system (500) includes outside devices (505), a network (510), a facility server (515), a facility application (520), records (525), a mobile device (530), a mobile application (535), a restrictions module (540), and a billing module (545) in accordance with one or more embodiments of the invention. In one or more embodiments of the invention, the outside devices (505) are any devices outside of the prison or controlled facility, with which an inmate desires to communicate. The outside devices (505) may be any suitable device for communication such as outsider computing device (106) in FIG. 1, any smart phone, computer, and/or any other suitable device. It will be apparent to one of ordinary skill in the art that the outside devices (505) may be many different devices and, as such, the invention should not be limited to the above examples.

[0072] In one or more embodiments of the invention, a network (510) is any network, wired or wireless, that may be used for communication. For example, the network (510) may be a Wide Area Network (WAN) such as the Internet, a Local Area Network (LAN), a cell phone network, and/or any other suitable network. It will be apparent to one of ordinary skill in the art that the network (510) may be used for communication amongst the outside devices (505), the facility server (515), and the mobile device (530) and, as such, should not be limited to the above examples.

[0073] In one or more embodiments of the invention, the facility server (515) is any computing device (i.e., a rack, server, desktop computer, laptop computer, etc.) owned, controlled, or used by the prison or controlled facility which houses the inmate(s) using the mobile devices (e.g., the mobile device (530)) of the present invention. For example, the facility server (515) may have the components and/or functionality described with regards to the application server (302) and/or the database server (304) in FIG. 3. In one or more embodiments of the invention, the facility server (515) is owned by a third party, such as a prison telephone system provider. Specifically, the facility server (515) may facilitate the use of mobile devices (e.g., the mobile device (530)) by inmates of the prison or controlled facility. For example, all messages or data sent by the mobile device (530) may be routed through and/or stored on the facility server (515). The facility server (515) executes the facility application (520) and stores records (525). Further, in one or more embodiments of the invention, the facility server (515) receives, manages, and facilitates financial transactions associated with the mobile device (530), and may have any functionality described with respect to the billing module (545), below.

[0074] In one or more embodiments of the invention, the facility application (520) enables the use of mobile devices (e.g., the mobile device (530)) by the inmates of the prison or controlled facility. In one or more embodiments of the invention, the facility application (520) may assist in the installation of the mobile application (535) on the mobile device (530), for example, by sending the necessary data to the mobile device (530). Additionally, the facility application (520) may allow administrators of the prison or controlled facility to establish or alter restrictions on the use of the mobile device (530) by inmates, which may subsequently be distributed to the mobile device (530) in the form of an update. The facility application (520) may also provide software updates to the mobile device (530) for any other reason. In one or more embodiments of the invention, the facility application (520) is able to remotely enable/disable the mobile device (530), using any method now known or later developed. The facility application (520) may receive and/or manage payments from inmates for the use of the mobile device (530). The payments that the facility application (520) may receive or manage are discussed in more detail below, with the billing module (545). In one or more embodiments of the invention, the facility application (520) tracks and records every action taken by the inmate(s) using the mobile device (530), and stores the data as records (525). It will be apparent to one of ordinary skill in the art that the facility application (520) is able to perform any actions necessary for the deployment and administration of an inmate mobile device system and, as such, the invention should not be limited to the above examples.

[0075] In one or more embodiments of the invention, records (525) are records of the usage of the mobile device (530) by the inmates of the prison or controlled facility. Records (525) may store any and all actions take using the mobile device (530). For example, records (525) may store text messages received and sent, record all video calls, log every picture taken, track every game played, and/or any other action taken on the mobile device (530).

[0076] In one or more embodiments of the invention, the mobile device (530) is a smart phone, cell phone, laptop, or other mobile computing device. For example, the mobile device (530) may be similar to the mobile computing device (400) of FIG. 4, and/or the inmate computing device (116) of FIG. 1. The mobile device (530) may have many different components and functionality, some of which are not appropriate for a prison or controlled facility. Thus, the mobile application (535) is installed on and executes on the mobile device (530) to limit the functionality of the mobile device (530). The mobile device (530) may be received from a variety of different sources. For example, the inmate may already own the mobile device (530) when they enter the prison or controlled facility. Alternatively, if the inmate has an illegal mobile device, the inmate may exchange and/or turn in the mobile device (530) via, for example, an amnesty program. As another option, the inmate may purchase the mobile device (530) from the prison or controlled facility, a third party supplier, phone company, or other suitable entity. Further still, the inmate may be able to rent the mobile device (530) from the prison or controlled facility, a prison telephone system provider, or other third party. For example, the inmate may be able to rent the mobile device (530) for any amount of time including but not limited to: hours, days, weeks, months, or years. Further still, a rent to own program, where once the inmate makes a set amount of payments (e.g., 75, 100, etc.)

the inmate owns the mobile device (530), may be provided. The funds for making the payment(s) may come from any source, and are discussed in detail with regards to the billing module (545), below.

[0077] In one or more embodiments of the invention, the mobile application (535) limits the functionality of the mobile device (530), thereby making the mobile device (530) appropriate for a prison or controlled facility. The mobile application (535) may replace, augment, or limit the original operating system of the mobile device (530). Alternatively, the mobile application (535) may be a program that the inmate uses to access services via the mobile device (530). In one or more embodiments of the invention, the mobile application (535) may be periodically updated (e.g., by the facility server (515)) to ensure that the restrictions and software is up to date. The mobile application (535) includes a restrictions module (540) and a billing module (545). It will be apparent to one of ordinary skill in the art that the mobile application (535) contains any functionality necessary to turn the mobile device (530) into a mobile device approved for use by an inmate and, as such, the invention should not be limited to the above examples.

[0078] In one or more embodiments of the invention, the restrictions module (540) includes all of the limitations and/or restrictions for the mobile device (530). The restrictions module (540) may receive the limitations and/or restrictions from any suitable source including, but not limited to: administration of the prison or controlled facility, the facility server (515), etc. The restrictions module (540) may limit any component or functionality of the mobile device (530). For example, the restrictions may include but are not limited to: limiting the hours at which the mobile device may be used (i.e., 6 am to 6 pm, etc), restricting what websites the inmate may access, limitations on the base functionality of the device such as games, phone calls, video, text messaging, camera/pictures, Global Positioning System (GPS) tracking, restrictions on locations where the mobile device may be used, rules for stolen devices (i.e., disabled immediately, actively tracked, etc), rules for transitioning the mobile device to the inmate when the inmate is released, rules governing the archiving and review of all actions taken on the mobile device, rules limiting who the inmate may contact, and/or any other suitable restrictions for a mobile device. It will be apparent to one of ordinary skill in the art that the restrictions may take many different forms and, as such, the restrictions module (540) should not be limited to the above examples.

[0079] In one or more embodiments of the invention, the billing module (545) is responsible for payments made for or using the mobile device (530). Optionally, the functionality associated with the billing module (545) may be located on another component, such as the facility server (515) or other suitable device. The billing module (545) may enable an inmate to make payments from the prisoner's commissary account, or any other account allowed by the prison or controlled facility including, but not limited to: checking accounts, savings account, credit cards, gift cards, online payment accounts, and/or any other account. In one or more embodiments of the invention, family or friends of the inmate may place funds into a special account strictly for payment of fees associated with the mobile device (530), which the inmate may then access via the billing module (545) for payment of any fees associated with the mobile device (530) or the usage of mobile device (530).

[0080] FIG. 6 shows a flowchart of a method for financing a mobile device for an inmate. While the various steps in this flowchart are presented and described sequentially, one of ordinary skill in the art will appreciate that some or all of the steps may be executed in different orders and some or all of the steps may be executed in parallel. Further, in one or more embodiments of the invention, one or more of the steps described below may be omitted, repeated, and/or performed in a different order. Accordingly, the specific arrangement of steps shown in FIG. 6 should not be construed as limiting the scope of the invention.

[0081] In Step 600, restrictions are received on the usage of the mobile device. The restrictions may be received, for example, from the institution whose controls the inmate is subject to, such as a prison, jail, military base, security controlled environment, and or any other controlled area. Alternatively, the restrictions may be received from a third party, such as the organization providing the mobile phones, the government, or any other suitable organization or entity. In one or more embodiments of the invention, the restrictions define how the inmate may interact with the mobile device. As described previously, the restrictions may be an inmate use restriction, inmate target restriction, device restriction, and/or any other restriction. For example, the restrictions may include but are not limited to:

[0082] limiting the hours at which the mobile device may be used (i.e., 9 am to 9 pm, etc), restricting which Uniform Resource Locators (URLs) (i.e., what websites) the inmate may access, limitations on the base functionality of the device such as games, phone calls, video, text messaging, camera/pictures, Global Positioning System (GPS) tracking, restrictions on locations where the mobile device may be used, rules for stolen devices (i.e., disabled immediately, actively tracked, etc), rules for transitioning the mobile device to the inmate when the inmate is released, rules governing the archiving and review of all actions taken on the mobile device, rules limiting who the inmate may contact, and/or any other suitable restrictions for a mobile device. It will be apparent to one of ordinary skill in the art that the restrictions may take many different forms and, as such, the invention should not be limited to the above examples.

[0083] In Step 605, the mobile device is received. The mobile device may be received in a variety of ways. For example, when an inmate first arrives at the detention center, he or she may bring a mobile device with him or her. Alternatively, an illegal mobile device may be confiscated from an inmate, or turned in during an amnesty program, for example. Further still, the mobile device may be a new (or used) device acquired, or rented, from a telephone company and/or other third party. It will be apparent to one of ordinary skill in the art that the mobile device may come from any source and, as such, the invention should not be limited to the above examples.

[0084] In Step 610, a mobile application is installed on the mobile device. The mobile application may, for example, replace the operating system of the mobile device. Alternatively, the mobile application may merely augment or alter the operating system, such as by limiting the functionality of the operating system. Further still, mobile application may merely be an application that executes on top of the operating system of a mobile device. The mobile application may be installed on the mobile device using any method now known or later developed. It will be apparent to one of ordinary skill

in the art that the mobile application converts an open mobile device into a tightly controlled and monitored mobile device that is appropriate for an inmate at a prison or controlled facility and, as such, the invention should not be limited to the above examples.

[0085] In Step 615, a payment is received for the mobile device. The payment may be received in a variety of ways including, but not limited to: from a family member or friend paying using any method now known or later developed, from a commissary account of the inmate (either via a payment module on the mobile device or via a computer associated with the commissary, or any other suitable method), etc. The payment may be for usage of the device, and the amount of the payment may be based on a variety of financial models. For example, there may be a free (to the inmate) model, a subscription model, and an ala carte model. The free model may have friends and family pay for communications with the inmate, while the inmate uses the mobile device for free. The subscription model may have a weekly or monthly charge, and usage limits such as a maximum number of messages or data per day or billing period. Finally, the ala carte model may have payments based on the specific activity performed on the mobile device—some activities may have a fee associated with them (e.g., send a text message for 10 cents, etc.), while others may be free (e.g., reading the news, etc.).

[0086] Additionally, in one or more embodiments of the invention, a rent to own program may be available for the inmate. That is, after the inmate makes a set number of rental payments (e.g., 50 payments, 75 payments, etc.) the inmate will own the mobile device, and will be able to sell it or take it with him or her when they leave the prison or controlled facility. It will be apparent to one of ordinary skill in the art that there are many ways to structure payments for the mobile device and, as such, the invention should not be limited to the above examples.

[0087] In Step 620, the mobile application is executed. The inmate may be required to execute the application to access the mobile device, thereby ensuring that unauthorized use of the mobile device is not possible. While the mobile application is executing, the inmate may perform any allowed action on the mobile device (provided payment has been made, when applicable), and all actions taken may be tracked and stored for later review by administrators of the prison or controlled facility.

[0088] The following section describes various examples of the invention. The examples are included to aid in the understanding of the invention and are not intended to limit the scope of the invention.

[0089] FIG. 7 shows an example in accordance with one or more embodiments of the invention. The steps shown in FIG. 7 may be performed in any order and should not be limited to the arrangement shown in FIG. 7.

[0090] In Step 700, website restrictions, time of use restrictions, and target restrictions for usage of the mobile device are received from the prison. Next a mobile device is received from one of a variety of sources, such from the detainee or a friend supplying a currently owned device (Step 705), a detainee turning in a contraband device (Step 710), a detainee purchasing a device (Step 715), or a detainee renting a device (Step 720). Optionally, when a detainee rents a device (Step 720), the detainee may establish a rent to own program (Step 725) that outlines how many payments the detainee must make before full ownership of the device is transferred to the detainee.

[0091] Regardless of how or from where the mobile device is acquired, the device is configured/reconfigured for compatibility with facility approved system (Step 730) by installing a mobile application. Subsequently, when the detainee uses the mobile device, it is determined if the use is allowed (Step 735). When the use of the device is not allowed, such as when the use violates the rules or there are insufficient funds to pay for the usage, the use is prohibited (Step 740). When the use is allowed and there are sufficient funds, the use is allowed and logged/recorded for later review (Step 745) by administrators, investigators, and other suitable parties.

[0092] At any time, the mobile device may be updated during an automated periodic check (Step 750), to ensure that the device and the mobile application maintain the highest standards of security and the most up to date restrictions. Finally, at some point, the detainee is released. If the device is paid for by, for example, the detainee completing a rent to own program, paying for the device outright, or originally owning the device, then the device is returned to the unconfigured state (Step 760) and the detainee may resume using the device in the outside world. Alternatively, if the device is not paid for, then the device is prepared for the next detainee (Step 765) by removing any personal data.

[0093] FIG. 8 shows a general computing system in accordance with one or more embodiments of the invention. As shown in FIG. 4, the computing system (800) may include one or more computer processor(s) (802), associated memory (804) (e.g., random access memory (RAM), cache memory, flash memory, etc.), one or more storage device(s) (806) (e.g., a hard disk, an optical drive such as a compact disk (CD) drive or digital versatile disk (DVD) drive, a flash memory stick, etc.), and numerous other elements and functionalities. The computer processor(s) (802) may be an integrated circuit for processing instructions. For example, the computer processor(s) may be one or more cores, or micro-cores of a processor. The computing system (800) may also include one or more input device(s) (810), such as a touchscreen, keyboard, mouse, microphone, touchpad, electronic pen, or any other type of input device. Further, the computing system (800) may include one or more output device(s) (808), such as a screen (e.g., a liquid crystal display (LCD), a plasma display, touchscreen, cathode ray tube (CRT) monitor, projector, or other display device), a printer, external storage, or any other output device. One or more of the output device(s) may be the same or different from the input device(s). The computing system (800) may be connected to a network (814) (e.g., a local area network (LAN), a wide area network (WAN) such as the Internet, mobile network, or any other type of network) via a network interface connection (not shown). The input and output device(s) may be locally or remotely (e.g., via the network (812)) connected to the computer processor(s) (802), memory (804), and storage device(s) (806). Many different types of computing systems exist, and the aforementioned input and output device(s) may take other forms.

[0094] Software instructions in the form of computer readable program code to perform embodiments of the invention may be stored, in whole or in part, temporarily or permanently, on a non-transitory computer readable medium such as a CD, DVD, storage device, a diskette, a tape, flash memory, physical memory, or any other computer readable storage medium. Specifically, the software instructions may correspond to computer readable program code that when executed by a processor(s), is configured to perform embodiments of the invention.

[0095] Further, one or more elements of the aforementioned computing system (800) may be located at a remote location and connected to the other elements over a network (814). Further, embodiments of the invention may be implemented on a distributed system having a plurality of nodes, where each portion of the invention may be located on a different node within the distributed system. In one embodiment of the invention, the node corresponds to a distinct computing device. Alternatively, the node may correspond to a computer processor with associated physical memory. The node may alternatively correspond to a computer processor or micro-core of a computer processor with shared memory and/or resources.

[0096] While the invention has been described with respect to a limited number of embodiments, those skilled in the art, having benefit of this disclosure, will appreciate that other embodiments can be devised which do not depart from the scope of the invention as disclosed herein. Accordingly, the scope of the invention should be limited only by the attached claims.

What is claimed is:

1. A method for financing a mobile device for an inmate, comprising:
 - receiving a plurality of mobile device rules comprising limitations on usage of the mobile device by the inmate within a controlled facility;
 - receiving the mobile device;
 - installing, on the mobile device, a mobile application, wherein the mobile application conforms the mobile device to the plurality of mobile device rules;
 - receiving a payment for the mobile device; and
 - executing, by the mobile device, the mobile application.
2. The method of claim 1, wherein the payment comprises a periodic rent payment.
3. The method of claim 2, wherein the periodic rent payment is part of a rent-to-own program.
4. The method of claim 1, wherein the mobile device is a contraband device received from the inmate.
5. The method of claim 1, wherein the payment is received from a third-party.
6. The method of claim 1, further comprising:
 - removing, by the mobile device, the mobile application, wherein removing the mobile application returns the mobile device to an initial state.
7. The method of claim 1, wherein the payment comprises a fee for sending a message.
8. The method of claim 1, wherein the mobile device is provided to the inmate upon or after release in a state that is not limited by the plurality of mobile device rules.
9. The method of claim 1, wherein the mobile device is returned to an administrator and all personal information is removed from the device.
10. A non-transitory computer-readable medium (CRM) storing a plurality of instructions for financing a mobile device for an inmate, the plurality of instructions comprising functionality to:
 - receive a plurality of mobile device rules comprising limitations on usage of the mobile device by the inmate within a controlled facility;
 - receive the mobile device;
 - install, on the mobile device, a mobile application, wherein the mobile application conforms the mobile device to the plurality of mobile device rules;

receive a payment for the mobile device; and execute the mobile application.

11. The non-transitory CRM of claim **10**, wherein the payment comprises a periodic rent payment.

12. The non-transitory CRM of claim **11**, wherein the periodic rent payment is part of a rent-to-own program.

13. The non-transitory CRM of claim **10**, wherein the mobile device is a contraband device received from the inmate.

14. The non-transitory CRM of claim **10**, wherein the payment is received from a third-party.

15. The non-transitory CRM of claim **10**, the instructions further comprising functionality to:

remove the mobile application, wherein removing the mobile application returns the mobile device to an initial state.

16. The non-transitory CRM of claim **10**, wherein the payment comprises a fee for sending a message.

17. A computer system, comprising:

a computer processor;

a mobile device comprising functionality to:

install a mobile application, wherein the mobile application conforms the mobile device to a plurality of mobile device rules, and

execute the mobile application; and a facility server, comprising the computer processor and having functionality to:

receive the plurality of mobile device rules comprising limitations on usage of the mobile device by an inmate within a controlled facility, and receive a payment for the mobile device.

18. The computer system of claim **17**, wherein the payment comprises a periodic rent payment.

19. The computer system of claim **18**, wherein the periodic rent payment is part of a rent-to-own program.

20. The computer system of claim **17**, wherein the mobile device is a contraband device received from the inmate.

21. The computer system of claim **17**, wherein the payment is received from a third-party.

22. The computer system of claim **17**, wherein the mobile device further comprises functionality to: remove the mobile application, wherein removing the mobile application returns the mobile device to an initial state.

23. The computer system of claim **17**, wherein the mobile device is provided to the inmate upon or after release in a state that is not limited by the plurality of mobile device rules.

24. The computer system of claim **17**, wherein the mobile device is returned to an administrator and all personal information is removed from the device.

* * * * *