Patent Application of

Claremont Speede

for

MOBILE SENDER CONTROLLED DATA ACCESS AND DATA DELETION METHOD AND SYSTEM

CROSS-REFERENCES TO RELATED APPLICATIONS

This application is a non-provisional application of and claims the benefit of U.S. Provisional Application No. 61744332, filed on September 24, 2012 by the present inventor.

Background – Prior Art

The following is a tabulation of some prior art that presently appears relevant:

U.S Patents

Patent Number	Kind Code	Issue Date	App or Patentee
0108621	A1	May 19, 2005	Kim et al.
0165790	A1	Jul. 19, 2007	Rakesh Taori

Existing deletion systems allow for the sender of the data to have control over the storage and access of the data, within the communication network. However, once this data is accessed by the intended receiver, control and ownership of the data by the sender is lost. Knowledge of the data's existence

cannot be determined by its sender. Prior art data deletion systems provide equal control over the access of the stored data, within the communication network, to the sender and the receiver. Existing systems do not make the mobile sender aware of the successful completion of the deletion of the sent data. The life cycle of the mobile sender's data is left to the strength, or weakness of a central system in use, enterprise policy, the receiving end user device, and or the action of data receiver. Existing deletion systems can solely delete short message services type data.

Accordingly, what is desired is a method for enabling data senders, such as a binary or ascii file senders, to have the capability to set, at their own convenience, the time of existence of their sent data, once the remote devices has received the data, or while the data still resides within the network.

FIELD OF THE INVENTION

The present invention generally relates to methods and a data delivery storage system, and more particularly, to methods and a data delivery storage system for remotely deleting binary or ascii formatted data stored on the remote mobile communication device, and within the communication network, by initiating a delete command, or setting a data time of existence during data construction, from a sender mobile communication device.

BACKGROUND OF INVENTION

Concerns about exposure of what was assumed to be confidential exchanges of information, has been the subject of debates aired over the media. It has become obvious that information, once transmitted, may be viewed by third parties along the data communication pathway and by others, the data receiver

may choose to disclose it to. Many forms of data and communication encryption strategies address the communication pathway disclosure issue, but the end user receiver disclosure still exists. In the mobile space, this problem is magnified several times, due to the obvious transient nature of end users. For example, the sender of data has no control or knowledge of the data's existence, after it has been sent. The time of existence of the mobile sender's data is left to the data receiver, the strength, or weakness of system in use, and/or enterprise policy. This scenario adds to the problem of information leakage, which remains an issue even if the line of transmission is secure.

Elaborate security schemes are available to ensure confidentiality is ensured. However, the mobile recipient is not considered to be a member of the group of links, in the security chain, that may pose as a concern. For example, a sender transmits an encrypted data to a mobile receiver, who successfully utilizes it. This discrete data is unusable to everyone except the sender and recipient, thus maintaining confidentiality. However, if the receiver decides, on his own, to execute the data in the presence of a third party, the intended sender receiver confidentiality will be compromised. Also, if data is still in transit, residing on the network, before the receiver device even accesses it, the sender no longer has control over the data, thus leaving the data at the mercy of the rigor of enterprise policy.

Therefore, improvements for a mobile communication and a method for managing sent data, by the data sender, or owner, are needed in the industry to address the aforementioned deficiencies.

BRIEF SUMMARY OF THE INVENTION

Embodiments of the present invention provide techniques that enable

a sender, using a mobile device, to control the access of sent data within a communication network, and to delete, at any time, sent data residing on the receiver's mobile device and network. When a sender attempts to transmit data to a receiver, the data residing within the communication network, that has not been accessed by the receiver, is considered owned by the sender. At this point, the sender may delete the data at will, as the receiver has yet to access the data. Once the data has reached receiver's device, the sender will be notified of the utilization of the remote data. With this notification, the sender may chose to delete the remotely located data. Alternatively, the sender may set a relative time and send data that will automatically get deleted, at the relative amount of time, after it is utilized, or at the relative amount of time after it arrives on the device.

A further understanding of the nature and advantages of the invention herein may be realized by reference of the remaining portions in the specifications and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated herein and form a part of the specification, illustrate embodiments of the present invention and, together with the description, further serve to explain the principles of the invention and to enable a person skilled in the relevant art to make and use the invention.

FIG. 1 illustrates a mobile sender controlled data access and data deletion network, in accordance with an embodiment of the present invention.

FIG. 2 illustrates communication channels in a mobile sender controlled data access and data deletion network, in accordance with an embodiment of the

present invention.

FIG. 3 is a flowchart depicting steps in the operation of a mobile sender controlled data access and data deletion delivery storage system, in accordance with an embodiment of the present invention.

FIG. 4 is a flowchart depicting steps in the operation of the process info process in a mobile sender controlled data access and data deletion delivery storage system, in accordance with an embodiment of the present invention.

FIG. 5 is a flowchart depicting steps in the operation the authentication process residing in a mobile sender controlled data access and data deletion delivery storage system, in accordance with an embodiment of the present invention.

FIG. 6A, FIG.6B and FIG.6C combined, is a flowchart depicting steps of a client service for a mobile sender controlled data access and data deletion delivery storage system, in accordance with an embodiment of the present invention.

FIG. 7 is a flowchart depicting steps of the flagging process of data, of type relative execution time for automatic time of existence, in a client service for a mobile sender controlled data access and data deletion delivery storage system, in accordance with an embodiment of the present invention.

FIG. 8 is a flowchart depicting steps of the deletion background process of a client service for a mobile sender controlled data access and data deletion delivery system, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Patent Application of Claremont Speede for "Mobile Sender Controlled Data Access and Data Deletion Method and System" continued

I. INTRODUCTION

The following detailed description of the present invention refers to the accompanying drawings that illustrate exemplary embodiments consistent with this invention. Other embodiments are possible, and modifications can be made to the embodiments within the spirit and scope of the invention. Therefore, the detailed description is not meant to limit the invention. Rather, the scope of the invention is defined by the appended claims.

It would be apparent to one of skill in the art that the present invention, as described below, can be implemented in many different embodiments of software, hardware, firmware, and/or the entities illustrated in the figures. Any actual software code with the specialized control of hardware to implement the present invention is not limiting of the present invention. Thus, the operational behavior of the present invention will be described with the understanding that modifications and variations of the embodiments are possible, given the level of detail presented herein.

FIG. 1 is a network 100 depicting a mobile sender controlled data access and data deletion/storage network, in accordance with an embodiment of the present invention. The network 100 includes a user device 102, a carrier wireless network 104, and a message delivery storage system 106. As used in this specification, user device 102 will commonly be a cellular telephone having data communication capabilities, although one skilled in the relevant arts will readily appreciate that any communication device, or device having communication capabilities, can be substituted. Similarly, network 104 will commonly be a carrier wireless network throughout this specification, although one skilled in the relevant arts will likewise appreciate that, depending on the

capabilities of user device 102, other network types, to include wired networks of any type, or wireless technology of any type (e.g., Bluetooth, cellular, wi-fi, ad hoc, etc.), can be substituted for wireless network 104.

Data delivery storage system 106 eases the communications between sender and receiver user devices 102, by routing and storing data from sender user device 102 to receiver user device 102, as further disclosed below, in accordance with an embodiment of the present invention. Furthermore, data delivery storage system 106 includes logic for establishing communications with user device 102 over carrier wireless network 104, in accordance with an embodiment of the present invention. Carrier wireless network 104 is, in accordance with an additional embodiment of the present invention, a cellular communications network.

II. NETWORK COMMUNICATIONS

FIG. 2 is a network 200 illustrating communication channels in a mobile sender controlled data access and data deletion network, in accordance with an embodiment of the present invention. As previously disclosed, a user device 102 is operable to connect to a data delivery storage system 106 over carrier wireless network 104 in order to send and receive data. One skilled in the relevant arts will recognize that a user device 102, such as a cellular phone, can communicate using a number of different protocols over a carrier wireless network 104, such as a cellular communications network.

In accordance with an embodiment of the present invention, user device 102 is configured to transmit data of any type over carrier wireless network 104. A carrier gateways 204 are used to receive the data 202 communications from carrier wireless network 104 and

forward the communications to data delivery storage system 106, in accordance with an embodiment of the present invention. In accordance with an additional embodiment of the present invention, gateways 204 is a carrier Gateway GPRS Support Node (GGSN) and an SMS gateway Clickatell provided by Clickatell (Pty) Ltd., of Redwood City, Calif. One skilled in the relevant arts will recognize that the precise configuration of the gateways 204 as shown in FIG. 2 need not exist in every system, where instead other means for forwarding the data 202 communications to data delivery system 106 are implemented.

In accordance with an embodiment of the present invention, user device 102 transmits data 202 to gateways 204 through the use of a special "short code"and Internet protocol address assigned to the data delivery storage system 106, in order to allow gateways 204 to properly route the data 202 to the data delivery system 106.

III. OPERATION OF THE DATA DELIVERY STORAGE SYSTEM

FIG. 3 is a flowchart 300 depicting an operational flow of data delivery storage system 106, in accordance with an embodiment of the present invention. Flowchart 300 method begins at step 301 and proceeds to step 302, where the data delivery storage system 106 receives data 202 from the user device 102. At step 304, the data delivery system 106 performs authentication on the sender user or user device 102, then process proceeds to step 306. If authentication was unsuccessful 306, the method proceeds to step 318 where processing ends. If authentication was successful 306, the method continues to step 308.

At step 308 of flowchart 300, of the data delivery storage system 106, the data 202 is parsed. In the process of parsing the data 202, the intended destination user or user device 102 from some received data 202 is extracted 310. Once

extraction 310 is complete, step 312 of the data delivery storage system 106 performs authentication on the destination user or user device 102, then process proceeds to step 314. If authentication was unsuccessful 314, the method proceeds to step 318 where processing ends. If authentication was successful 314, the method continues to step 316.

At step 316 of flowchart 300, the message delivery storage system 106, the parsed data 202 is then repackaged into a data 202 format, and transmitted to the intended destination user or user device 102, as further disclosed below, in accordance with an embodiment of the present invention. The method ends at step 318, in accordance with an embodiment of the present invention.

With continued reference to flowchart 300 of FIG. 3, the data delivery storage system 106, and network 200 of FIG. 2, an example user interaction with the data delivery storage system 106 is disclosed, in accordance with an embodiment of the present invention. A user creates data (image, video, or any file type), at user device 102 to be delivered to a remote user device 102. In this example, the user creates an image. The user then sends this data to the remote user mobile device 102 by entering a mobile number associated with the remote user mobile device 102. In accordance with an embodiment of the present invention, the data is sent to a short code, such as 45772, that uniquely identifies data delivery storage system 106.

At step 302 of flowchart 300, the data delivery system 106 receives the data 202, and at steps 304 and 312 the data delivery system 106 performs any necessary authentication, as will be fully disclosed herein. If authentications are unsuccessful 306 and 314, the process proceeds to step 318. If authentications are successful 306 and 314, the process continues to step 308 and 316, respectively.

Patent Application of Claremont Speede for "Mobile Sender Controlled Data Access and Data Deletion Method and System" continued

At step 308 of flowchart 300, the data delivery system 106 begins parsing the data to identify a token, or tokens in the aforementioned data, which represents the destination user or user device 102 from some received data 202, in accordance with an embodiment of the present invention. Next, this token is extracted 310 and step 312 of the data delivery storage system 106, performs authentication on the destination user or user device 102. If authentication was unsuccessful 314, the method proceeds to step 318 where processing ends. If authentication was successful 314, the method continues to step 316.

At step 316 of flowchart 300, the data delivery system 106, the data is processed, which is described in more detail in FIG. 4, in accordance with an embodiment of the present invention.

In accordance with an additional embodiment of the present invention, if the authentication of steps 306 and 314 fails, the process flow is terminated. In accordance with a further embodiment of the present invention.

IV. PROCESS INFORMATION

FIG. 4 is a flowchart 400 depicting a process info flow of the data delivery storage system 106, in accordance with an embodiment of the present invention. The method begins at step 401 and proceeds to step 402, where the data delivery storage system 106 processes data 202 received from the user device 102. At step 402, the data delivery storage system 106 determines if the data is abridged meta data. If data is abridged meta data, then process proceeds to step 404. If data is not abridged meta data, the method proceeds to step 414, which is described in more detail below. Meta data is a set of data that describes and gives information about other data. Abridged meta data is information pertaining to what type of data will be sent and an actual fingerprint or unique

marker of the data that will be sent. Non-abridged meta data is the resource or file system information that is linked to the abridged data that includes details such as storage or location information. During the deletion process from the data delivery system, linked meta data, abridged and non-abridged, is automatically removed from the data delivery system. At step 404, the data delivery storage system 106 stores the meta data sent from the sender user device 102. Next, the data delivery storage system 106 allocates network resources for data at step 406. Allocated network resources is the entity which stores the data for example, a hard drive, networked drive, external drive or a cloud system that stores the data. The network resources is a directory of the data. The data delivery storage system 106 then proceeds to step 408. At step 408, the data delivery storage system 106 stores the allocated network resource information. Next, the data delivery system 106 transmits the resource information at step 410 to the sender user device 102. The method then proceeds to step 412 where processing ends.

At step 414, the data delivery storage system 106 determines if the data is a data write success alert. If data is a data write success alert, then process proceeds to step 416. If data is not a data write success alert, the method proceeds to step 420, which is described in more detail below. At step 416, the data delivery storage system 106 selects the stored non-abridged meta data created for the sender user device 102. Next, the data delivery storage system 106 transmits non-abridged meta data to the receiver user device 102 at step 418. The method then proceeds to step 412 where processing ends.

At step 420, the data delivery storage system 106 determines if the data 202 is an alert that the receiver user device 102 was accessed. If data 202 was accessed, then the method proceeds to step 422. If data 202 was not accessed

by the receiver user device 102, then the method proceeds to step 424. At step 422, the data delivery storage system 106 stores the result of the receiver user device's 102 access of the locally stored data 202. The method then proceeds to step 412 where processing ends.

At step 424, the data delivery storage system 106 determines if a delete command was sent by the sender user device 102. If a delete command was sent, then the method proceeds to step 428. If delete command was not sent by the sender user device 102, then the method proceeds to step 426.

At step 428, the data delivery storage system 106 determines if the receiver user device 102 successfully accessed the sent data 202. If data 202 was successfully accessed, then the method proceeds to step 430. If data 202 was not successfully accessed, then the method proceeds to step 436.

At step 426, the data delivery storage system 106 transmits data to the receiver user device 102. The method then proceeds to step 412 where processing ends.

At step 436, the data delivery storage system 106 deletes data 202 from the allocated resources. Next, the data delivery storage system 106 issues a deletion command to the sender user device 102, at step 438. The method then proceeds to step 412 where processing ends.

At step 430, the data delivery storage system 106 determines the number of receiver user devices 102 that successfully accessed data 202. If the number of receiver user devices 102 that accessed the data 202 is greater than one, then the method proceeds to step 432. If only one receiver user device 102 accessed the data 202, then the method proceeds to step 440.

At step 440, the data delivery storage system 106 deletes data 202 from the allocated resources. The method then proceeds to step 442.

At step 442, the delete command is forwarded to the receiver user device 102

that accessed the data 202. The method then proceeds to step 412 where processing ends.

At step 432, the data delivery storage system 106 deletes each of the data 202 allocated resources for each receiver. The method then proceeds to step 434 where a delete command is forwarded to each of the receiver user devices 102 that accessed the data 202. The method then proceeds to step 412 where processing ends.

V. OPERATION OF THE AUTHENTICATION PROCESS

FIG. 5 is a flowchart 500 depicting an operational flow of the authentication process of the data delivery storage system 106, in accordance with an embodiment of the present invention. The method begins at step 501 and proceeds to step 502, where a search is performed in order to determine if the received unique properties can be found. The result is passed to step 504, in accordance with an embodiment of the present invention. At step 504, it is determined if the result is a valid user, by returning success and proceeding to step 506, if indeed the result is a valid user. Step 504 proceeds to step 508, if the result is determined not to be a valid user, in accordance with an embodiment of the present invention. The process then proceeds to step 510, where it ends.

One skilled in the relevant arts will appreciate that additional means for authentication can be used, and the aforementioned means are described by way of example and not limitation.

VI. USER DEVICE CLIENT SERVICE

Patent Application of Claremont Speede for "Mobile Sender Controlled Data Access and Data Deletion Method and System" continued

FIG. 6A, FIG.6B and FIG.6C combined, is a flowchart 600 depicting an operational flow of client service on the user device 102, in accordance with an embodiment of the present invention, of transmitting and receiving data (image, video, or any file type) 202, where by a sender user device 102 can delete a sent data 202, on a remote receiver user device 102. The method begins in FIG. 6A at step 601 and proceeds to step 602, where the user device 102 receives data 202 sent from a sender user device 102. At step 602, the remote receiver user device 102 performs a check to verify if data 202 was received. If no data 202 was received, the method proceeds to step 604. If data 202 was received, the proceeds to step 616, which is described in more detail below, in accordance with an embodiment of the present invention.

At step 604 of flowchart 600, the client service, on the user device 102, verifies if create new data option is selected, in accordance with an embodiment of the present invention. If it was not selected, step 604 continues to step 602. If it was selected, the method proceeds to step 606. At step 606, new data is created, in accordance with an embodiment of the present invention. Once the data is created, the method continues to step 608.

At step 608 of flowchart 600, the client service, on the user device 102, verifies if a manual delete is to be performed on the data 202 when it arrives on the remote user device 102, or on allocated resource within the data delivery storage system 106, in accordance with an embodiment of the present invention. If no manual delete is to be performed, the method continues to step 610 where data time of existence is set, then the method continues to step 611, which packages the meta data, in accordance with an embodiment of the present invention. Once the meta data is created, the method continues to step 612. If manual delete is to be performed, the method continues to step 613 where data

time of existence is set to manual. The method then continues to step 612.

At step 612 of flowchart 600, the client service, on the user device 102, and transmits data 202 to the carrier wireless network 104, in accordance with an embodiment of the present invention. The process then proceeds to step 614, where it ends.

At step 616 of flowchart 600, the client service, on the user device 102, verifies if the received data 202 is an alert that a remote receiver user device 102 has performed an action on a previously sent data 202, in accordance with an embodiment of the present invention. If the received data 202 is an action alert, the process then proceeds to step 618, which is described in more detail below. If the received data 202 is not an alert, the process then proceeds to step 650, which is illustrated and described in more detail in FIG. 6B.

At step 618 of flowchart 600, the client service, on user device 102, extract the execution flag and unique identifier from the alert of the received data 202. One skilled in the relevant arts will recognize that step 618 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. If the flag is determined not to be a set access flag, the process proceeds to step 642, which is described in more detail below. If the flag is determined to be a set open flag, the process proceeds to step 640.

At step 640 of flowchart 600, the client service, on the user device 102, verifies the unique identifier of the manual time of existence data 202 to be deleted on the remote receiver user device 102, in accordance with an embodiment of the present invention. If, the uniquely identified manual time of existence data 202 is to be deleted on the remote receiver user device, the process proceeds to step 620, which is described in more detail below. If, the uniquely identified manual time of existence data 202 is to be not deleted on the

remote receiver user device, the process proceeds to step 614 where processing ends.

At step 620 of flowchart 600, the client service, on the user device 102, sets the delete flag, the unique identifier and an non restrictive time of existence, in accordance with an embodiment of the present invention, and is forwarded to step 612. One skilled in the relevant arts will recognize that step 620 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention.

At step 642 of flowchart 600, the client service, on the user device 102, extracts the deletion complete flag and unique identifier from the alert of the received data 202. One skilled in the relevant arts will recognize that step 642 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. If the flag is determined to be a set deletion complete flag, the process proceeds to step 670, which is described in more detail below. If the flag is determined not to be a set deletion complete flag, the process proceeds to step 646.

At step 670 of flowchart 600, the client service, on the user device 102, determines if all of the receiver devices 202 have deleted their data. One skilled in the relevant arts will recognize that step 670 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. If all of the receiver devices 202 have deleted their data, the process proceeds to step 644, which is described in more detail below. If all of the receiver devices 202 have not deleted their data, the process proceeds to step 614.

At step 646 of flowchart 600, the client service, on the user device 102, extracts the delete flag and unique identifier from the alert of the received data

202. One skilled in the relevant arts will recognize that step 646 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. If the flag is determined to be a set delete flag, the process proceeds to step 648, which is described in more detail below. If the flag is determined not to be a set delete flag, the process proceeds to step 614 where processing ends.

At step 644 of flowchart 600, the client service, on the user device 102, utilizes the unique identifier from the alert of the data 202, and flags the sender's copy of the manual time of existence data 202 for deletion. One skilled in the relevant arts will recognize that step 644 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. Deletion of sender's copy of the manual time of existence data 202, may be performed at any time, of the sender's own choosing. The process proceeds to step 614 where processing ends.

At step 648 of flowchart 600, the client service, on the user device 102, utilizes the unique identifier from the alert of the data 202, and sets a delete flag of the uniquely identified manual time of existence data 202, on the receiver user device 102. One skilled in the relevant arts will recognize that step 648 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. The process proceeds to step 614 where processing ends.

The method continues in FIG. 6B at step 650 of flowchart 600 from step 616, the client service on the user device 102, signals that a data 202 is meta data sent from the sender user device 102, as previously illustrated in FIG. 6A. The process then proceeds to step 652. If data 202 is not meta data, then the process proceeds to 624, as described in more detail below.

Patent Application of Claremont Speede for "Mobile Sender Controlled Data Access and Data Deletion Method and System" continued

At step 652 of flowchart 600, the client service, on the user device 102, the data 202 is accessed and locally stored on the receiver user device. One skilled in the relevant arts will recognize that step 652 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. The process then proceeds to step 630.

At step 630 of flowchart 600, the client service, on the user device 102, determines if the data 202 was successfully accessed and stored locally. One skilled in the relevant arts will recognize that step 630 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. If the data 202 is successfully accessed and stored, the process proceeds to step 632, which is described in more detail below. If the data 202 is not successfully accessed and stored, the process proceeds to step 634.

At step 632 of flowchart 600, the client service, on the user device 102, creates a successful read alert, then the process proceeds to step 612, which is described in more detail above.

At step 634 of flowchart 600, the client service, on the user device 102, creates an unsuccessful read alert, then the process proceeds to step 612, which is described in more detail above.

At step 624 of flowchart 600, the client service, on the user device 102, determines if the data 202 is amended meta data sent from the data delivery storage system 106. If the data 202 is meta data sent from the data delivery storage system 106, the process proceeds to step 626, which is described in more detail below. If the data 202 is not amended meta data sent from the data delivery system 106, the process proceeds to step 622.

At step 622 of flowchart 600, the client service, on the user device 102,

signals that the information has been received and gets stored.

At step 626 of flowchart 600, the client service, on the user device 102, stores the amended meta data 202, then the process proceeds to step 628.

At step 628 of flowchart 600, the client service, on user device 102, accesses allocated resources on the data delivery storage system 106 and stores data 202 (image, video, or any file type). One skilled in the relevant arts will recognize that step 628 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. The process proceeds to step 636.

At step 636 of flowchart 600, the client service, on the user device 102, determines if the data 202 (image, video, or any file type) was successfully accessed and stored locally. One skilled in the relevant arts will recognize that step 636 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. If the data 202 is successfully written, the process proceeds to step 654, which is described in more detail below. If the data 202 is not successfully written, the process proceeds to step 638.

At step 638 of flowchart 600, the client service, on the user device 102, creates a failed write alert, then the process proceeds to step 612, which is described in more detail above.

At step 654 of flowchart 600, the client service, on the user device 102, creates an successful write alert, then the process proceeds to step 612, which is described in more detail above.

The method continues in FIG. 6C at step 622 of flowchart 600, the client service, on the user device 102, signals that data 202 has been received and stores the received data 202, as previously illustrated in FIG. 6B. The

process then proceeds to step 656.

At step 656 of flowchart 600, the client service, on the user device 102, may execute the received manual time of existence data 202 (image, video, or any file type). If the user device 102 will not execute the received manual time of existence data 202, the process proceeds to step 614 where processing ends, as previously illustrated in FIG. 6A and FIG. 6B. If the user device 102 will execute the received manual time of existence data 202, the process proceeds to step 658.

At step 658 of flowchart 600, the client service, on the user device 102, executes the received manual time of existence data 202, thereby run the binary content and flags the manual time of existence data 202 as executed data. One skilled in the relevant arts will recognize that step 658 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. The process then proceeds to step 660.

At step 660 of flowchart 600, the client service, on the user device 102, closes the execution of manual time of existence data 202, then proceeds to step 662, in accordance with an embodiment of the present invention.

At step 662 of flowchart 600, the client service, on the user device 102, verifies if the executed manual time of existence data 202 delete flag was set by the sender user device 102, in accordance with an embodiment of the present invention. If executed manual time of existence data 202 delete flag was set, the process proceeds to step 664, which is described in more detail below. If the executed manual time of existence data 202 delete flag was not set, the process proceeds to step 666.

At step 666 of flowchart 600, the client service on the user device 102 sets a executed flag, a unique identifier and an non restrictive time of existence, for

the executed manual time of existence data 202, in accordance with an embodiment of the present invention, is forwarded to step 612, which is illustrated above in FIG. 6A and FIG 6B.

At step 664 of flowchart 600, the client service, on the user device 102, deletes the executed manual time of existence data 202 (image, video, or any file type) from the user device 102 storage. One skilled in the relevant arts will recognize that step 664 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. The process then proceeds to step 668.

At step 668 of flowchart 600, the client service, on the user device 102, sets a deletion complete flag, a unique identifier and an non restrictive time of existence, for the executed manual time of existence data 202, in accordance with an embodiment of the present invention, is forwarded to step 612, which is illustrated above in FIG. 6A and FIG 6B.

VII. USER DEVICE CLIENT SERVICE AUTOMATIC TIME OF EXISTANCE DATA FLAGGING

FIG. 7 is a flowchart 700 depicting an operational flow of flagging process of automatic time of existence data, of type relative execution time, of the client service on the user device 102, in accordance with an embodiment of the present invention, for the handling of received data 202 (image, video, or any file type) that have an automatic time of existence of type relative execution time, meaning sender user device 102 has preset the time of existence. As previously illustrated in FIG. 6A, FIG. 6B and FIG. 6C, operational flow of the client service on the user device 102, step 622 signals that a data 202 has been received and stores the received data 202. One skilled in the relevant arts will

recognize that step 622 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. The process then proceeds to step 702.

At step 702 of flowchart 700, the flagging process of automatic time of existence data, of type relative execution time, of the client service on the user device 102, may execute the received data 202, which takes the process to step 704, which is described in more detail below, in accordance with an embodiment of the present invention. If the user device 102 will not execute the received data 202, the process proceeds to step 710 where processing ends.

At step 704 of flowchart 700, the flagging process of automatic time of existence data, of type relative execution time, of the client service on the user device 102, executes the stored automatic time of existence data 202, of type relative execution time, and performs its task. The process then proceeds to step 706. In accordance with an additional embodiment of the present invention, received data 202 with automatic time of existence is discussed.

At step 706 of flowchart 700, the flagging process of automatic time of existence data, of type relative execution time, of the client service on the user device 102, flags the automatic time of existence data 202 as executed, then stores the data 202. One skilled in the relevant arts will recognize that step 706 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. The process then proceeds to step 708.

At step 708 of flowchart 700, the flagging process of automatic time of existence data, of type relative execution time, of the client service on the user device 102, closes executed data 202, then proceeds to the end at step 710, in accordance with an embodiment of the present invention.

Patent Application of Claremont Speede for "Mobile Sender Controlled Data Access and Data Deletion Method and System" continued

VIII. USER DEVICE CLIENT SERVICE DELETION BACKGROUND PROCESS

FIG. 8 is a flowchart 800 depicting an operational flow of the deletion background process, of a client service on the user device 102, in accordance with an embodiment of the present invention, of expired automatic time of existence and delete flagged manual time of existence data 202. The method begins at step 801 and proceeds to step 802, where the process 802 selects data from the user device's 102 store, that is the smallest expired automatic time of existence of type relative execution time, smallest manual time of existence that has been flagged as delete, or expired automatic time of existence of type relative arrival time. One skilled in the relevant arts will recognize that step 802 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. The process then proceeds to step 804.

At step 804 of flowchart 800, the deletion background process, of a client service on the user device 102, deletes the selected data from the user device 102. One skilled in the relevant arts will recognize that step 804 can be accomplished by various methods within user device 102, in accordance with an embodiment of the present invention. The process then proceeds to step 806, where the process ends.

IX. ADVANTAGES

From the description above, a number of advantages of some embodiments of my sender controlled data access and deletion method become evident:

(a) The data sender of the data can maintain control over the complete life

cycle of sent data, even after it has been accessed by the intended receiver.

(b) The receiver of the data no longer has equal control over the accessed data, as the sender. The sender has superior, and sometimes sole control over the sent data.

(c) The sender can send data other than text messages, such as pictures, video, etc. Data files of various types may be sent.

(d) The sender has knowledge that data was deleted.

(e) The sender device is the creator and owner of the data, as such, the sender dictates the duration of the data's existence. Not some other entity.

(f) The sender device may delete the same data delivered to multiple receiver devices.

X. CONCLUSION

While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. It will be understood by those skilled in the relevant art(s) that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined in the appended claims. It should be understood that the invention is not limited to these examples. The invention is applicable to any elements operating as described herein. Accordingly, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

Patent Application of Claremont Speede for "Mobile Sender Controlled Data Access and Data Deletion Method and System" continued

CLAIMS: I claim:

1. A method for deleting data initiated by a remote sender user device, the method comprising: creating data and setting its time of expiration on the user device; wherein abridged meta data is provided from the data; sending the meta data from the user device; receiving the meta data on the data delivery storage system; parsing the meta data to obtain a destination user device on the data delivery system; transmitting the appended meta data, with created location information for the data on the network, to the sending user device; receiving the appended meta data on the data sending device; sending the data from the sending device to delivery storage system; transmitting the meta data to the destination user device; receiving meta data on the destination user device; accessing the data on the delivery storage system from the destination user device; storing the data on the delivery storage system onto the destination user device; executing the data on the destination user device; sending a manual delete alert, from the sender user device, to destination user device; receiving delete alert on the delivery storage system; deleting of the data, sent by sender user device on the delivery storage system; forward delete alerts to all receiver devices from the delivery storage system; receiving delete alert on the destination user devices; deleting of the data, sent by sender user device, on the destination user device; deleting copy of the data sent by sender user device on sender user device; background service deleting, on destination user device, executed data with lowest manual time of existence and flag set to delete; background service searching for and deleting, on destination user device, data with lowest expired automatic time of existence and flag set to executed; background service searching for and deleting, on destination user device, data

Patent Application of Claremont Speede for "Mobile Sender Controlled Data Access and Data Deletion Method and System" continued

with lowest expired automatic time of existence of type relative arrival time.

2. The method according to claim 1, wherein the step of receiving the data on the delivery storage system comprises: authenticating the sender user device by comparing a unique properties of the user device to registered values for the unique properties.

3. The method according to claim 2, wherein the user device is a phone, and further wherein the unique properties may comprise of a phone number and various unique phone attributes.

4. The method according to claim 1, wherein the step of parsing the data to obtain a destination user device on the data delivery storage system: authenticating the destination user device by comparing a unique properties of the user device to registered values for the unique properties.

5. The method according to claim 4, wherein the user device is a phone, and further wherein the unique properties may comprise of a phone number and various unique phone attributes.

6. The method according to claim 1, wherein the step of setting the time of existence comprises: selecting from a set of the time of existence levels comprising: manual, automatic relative execution time, and automatic relative arrival time.

7. The method according to claim 1, wherein the step of executing received

data the user device comprises: sending data executed alert, on the destination user device, to the sender user device.

8. The method according to claim 1, wherein the step of sending a manual delete data command, from the sender user device, to destination user device comprises: receiving an executed data alert on the sender user device.

9. The method according to claim 1, wherein the step of deleting of the data, sent by sender user device, on the delivery storage system comprises: receiving delete alert on the delivery storage system; deleting of the stored data, data related meta data of all types, and forwarding delete alert to all receiver devices of the data if data was accessed.

10. The method according to claim 1, wherein the step of deleting of the data, sent by sender user device, on the destination user device comprises: deleting of the stored data and sending deletion complete alert to the sender user device, from the destination user device.

11. The method according to claim 1, wherein the step of deleting copy of the data sent by sender user device on sender user device comprises: receiving deletion complete alerts on the sender user device.

12. The method according to claim 1, wherein the delete command is sent to the number of destination user devices, to data related meta data and associated allocated network resources within the delivery storage

system.

13. The method according to claim 1, wherein the sender receives the non-abridged meta data with location that identifies where the data should be transmitted.

14. A data delivery storage system between a sender user device and a destination user device, the data delivery storage system comprising: a storage facilities to store received data, originally sent from sender user device; a process to delete data stored within storage facilities, delete all data related meta data, and forward delete alerts to all receiver user devices.

15. The method according to claim 14, further comprising determining a number of receiver user devices that accessed the data and deleting the data related non-abridged meta data, abridged meta data and allocated network resources.