US 20130018963A1

(19) **United States**

(12) **Patent Application Publication**

Brauff et al.

(10) **Pub. No.: US 2013/0018963 A1**

(43) **Pub. Date: Jan. 17, 2013**

(54) **JOURNALING, ANALYSIS, AND ARCHIVING OF ELECTRONIC COMMUNICATIONS**

(75) Inventors: **Craig A. Brauff**, Bellevue, WA (US); **Calvin R. Cochran**, Tacoma, WA (US); **Justin D. Perkins**, Renton, WA (US)

(73) Assignee: **CM2.COM, INC.**, Renton, WA (US)

(21) Appl. No.: **13/179,700**

(22) Filed: **Jul. 11, 2011**

Publication Classification

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **709/206**

(57) **ABSTRACT**

Disclosed is a communication journaling and archival system which obtains content from social networks, handles re-authentication requirements which occur with respect to monitored users and social networks, includes content obtained from social networks in a journal and archiving system compatible with email journaling and archiving, and can be configured to send a journaled communication to multiple journal destinations and journal formats.

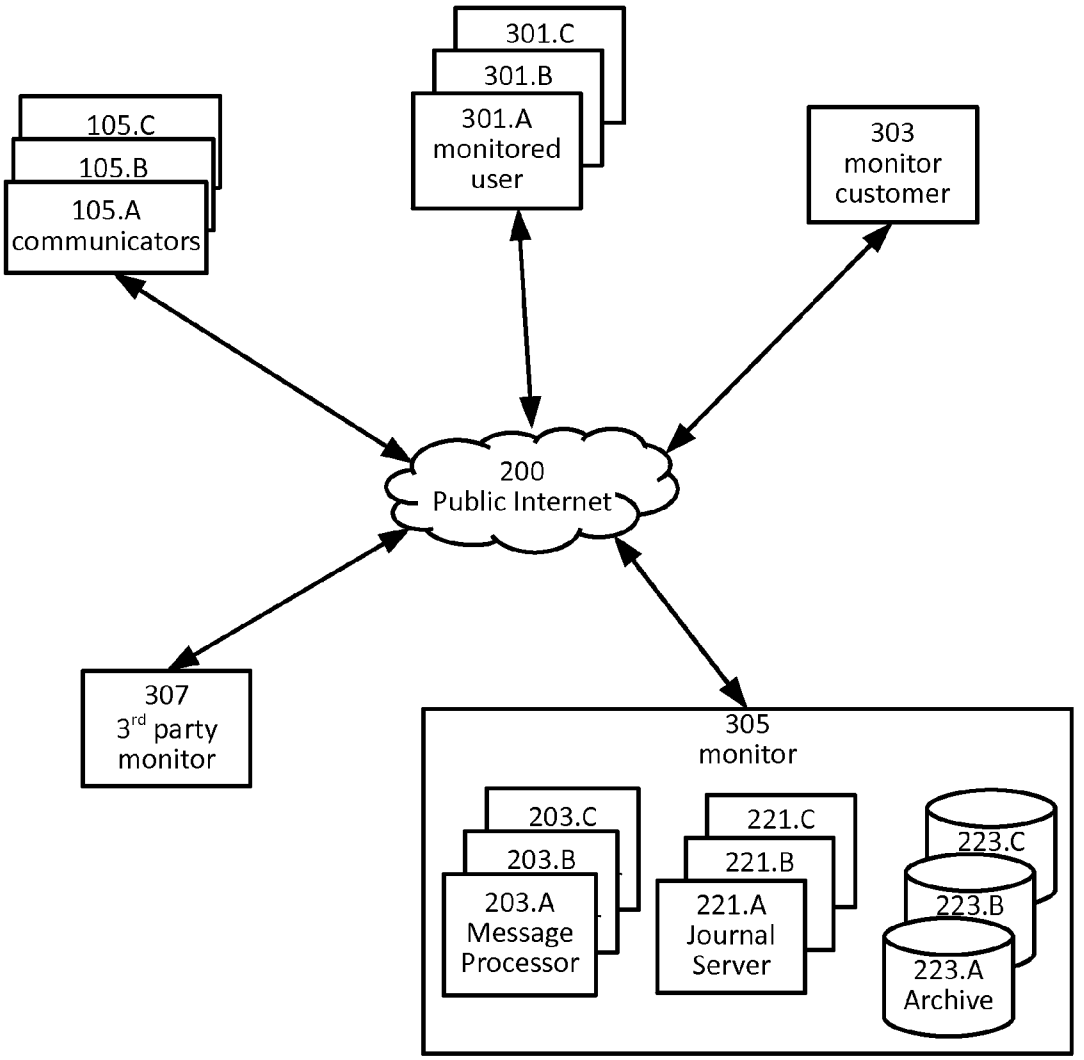
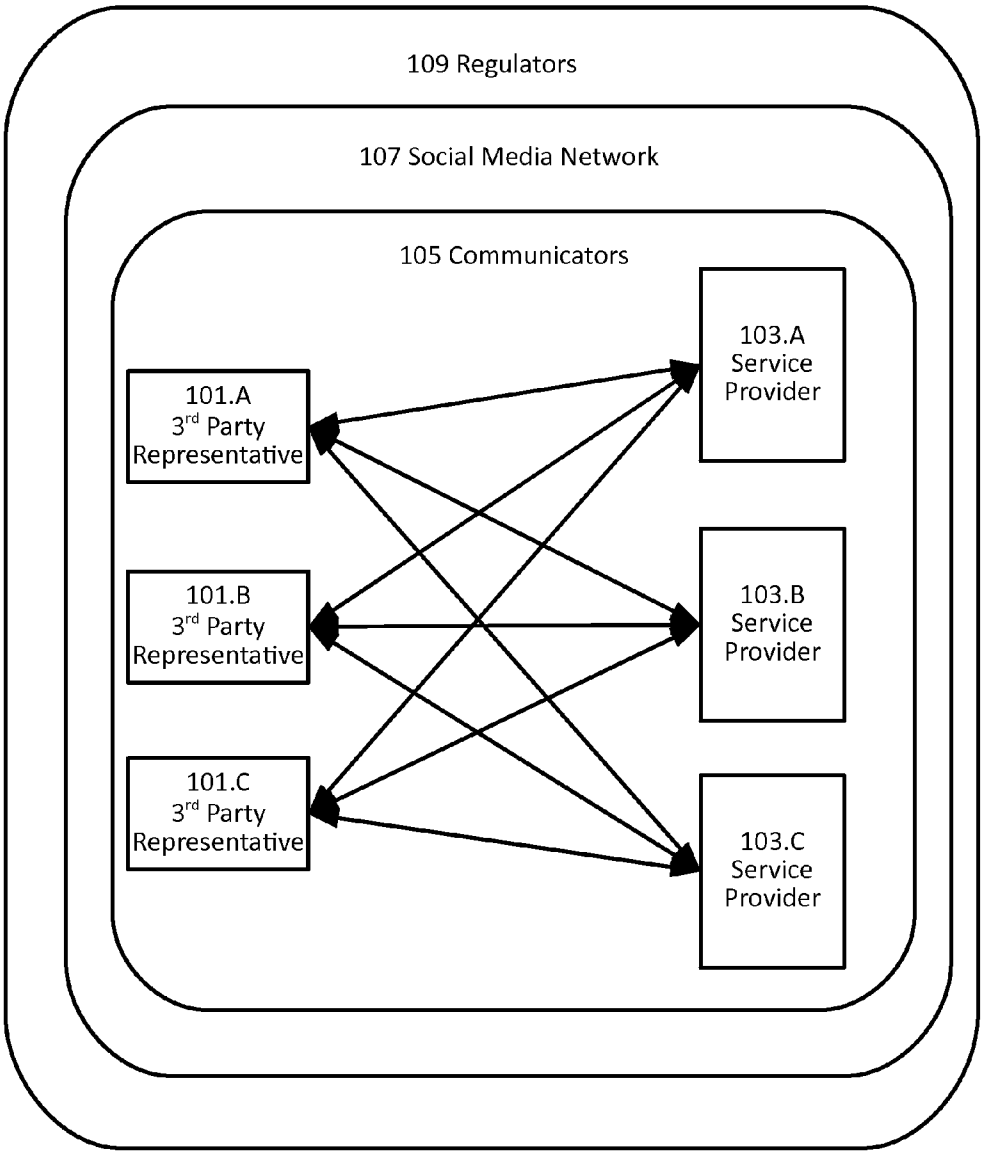


Figure 1


109 Regulators
107 Social Media Network
105 Communicators
101.A 3rd Party Representative
101.B 3rd Party Representative
101.C 3rd Party Representative
103.A Service Provider
103.B Service Provider
103.C Service Provider

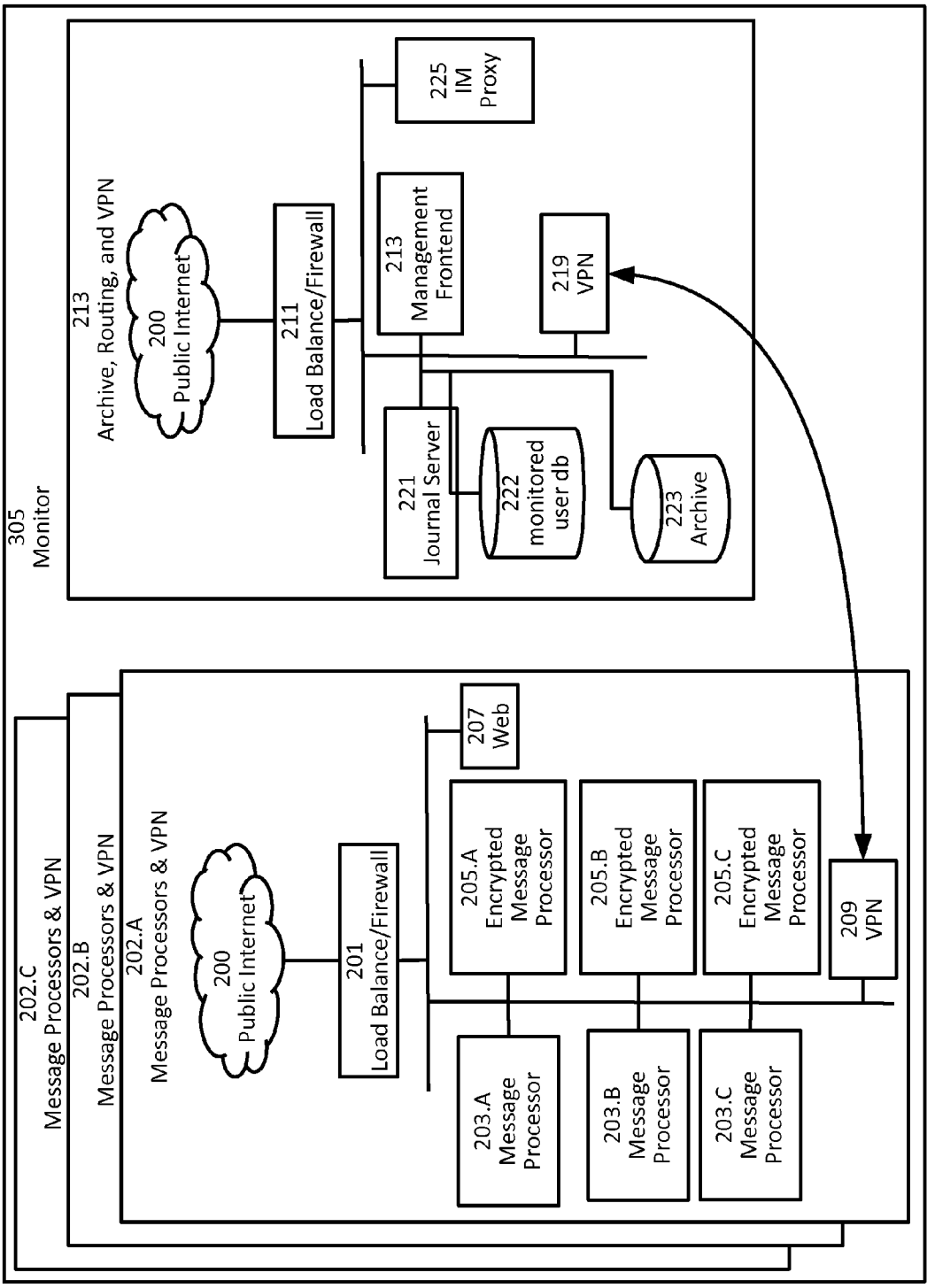

305
Monitor
213
Archive, Routing, and VPN
200
Public Internet
211
Load Balance/Firewall
213
Management
Frontend
225
IM
Proxy
219
VPN
221
Journal Server
222
monitored
user db
223
Archive
202.C
Message Processors & VPN
202.B
Message Processors & VPN
202.A
Message Processors & VPN
200
Public Internet
201
Load Balance/Firewall
207
Web
205.A
Encrypted
Message
Processor
205.B
Encrypted
Message
Processor
205.C
Encrypted
Message
Processor
209
VPN
203.A
Message
Processor
203.B
Message
Processor
203.C
Message
Processor

Figure 2

Figure 3

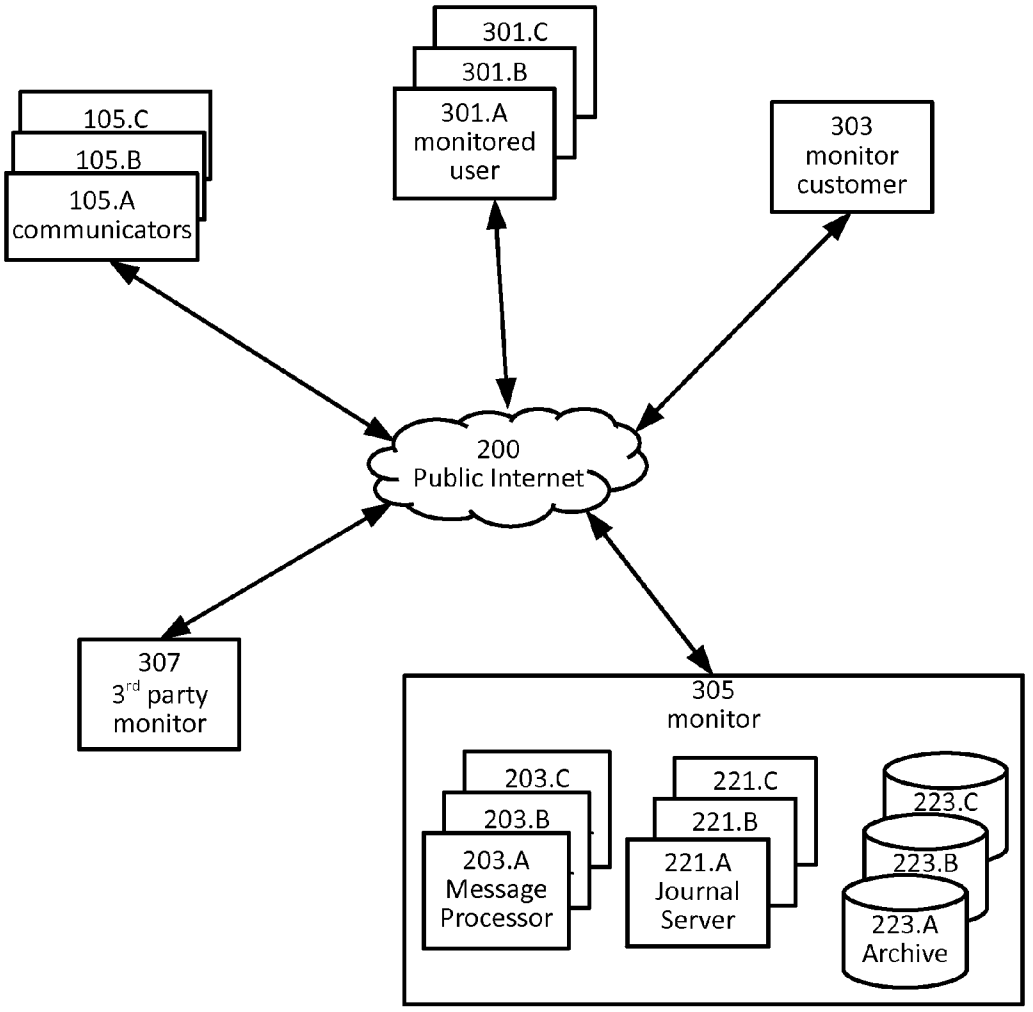

301.C
301.B
301.A
monitored
user
105.C
105.B
105.A
communicators
303
monitor
customer
200
Public Internet
307
3rd party
monitor
305
monitor
203.C
203.B
203.A
Message
Processor
221.C
221.B
221.A
Journal
Server
223.C
223.B
223.A
Archive

Figure 4

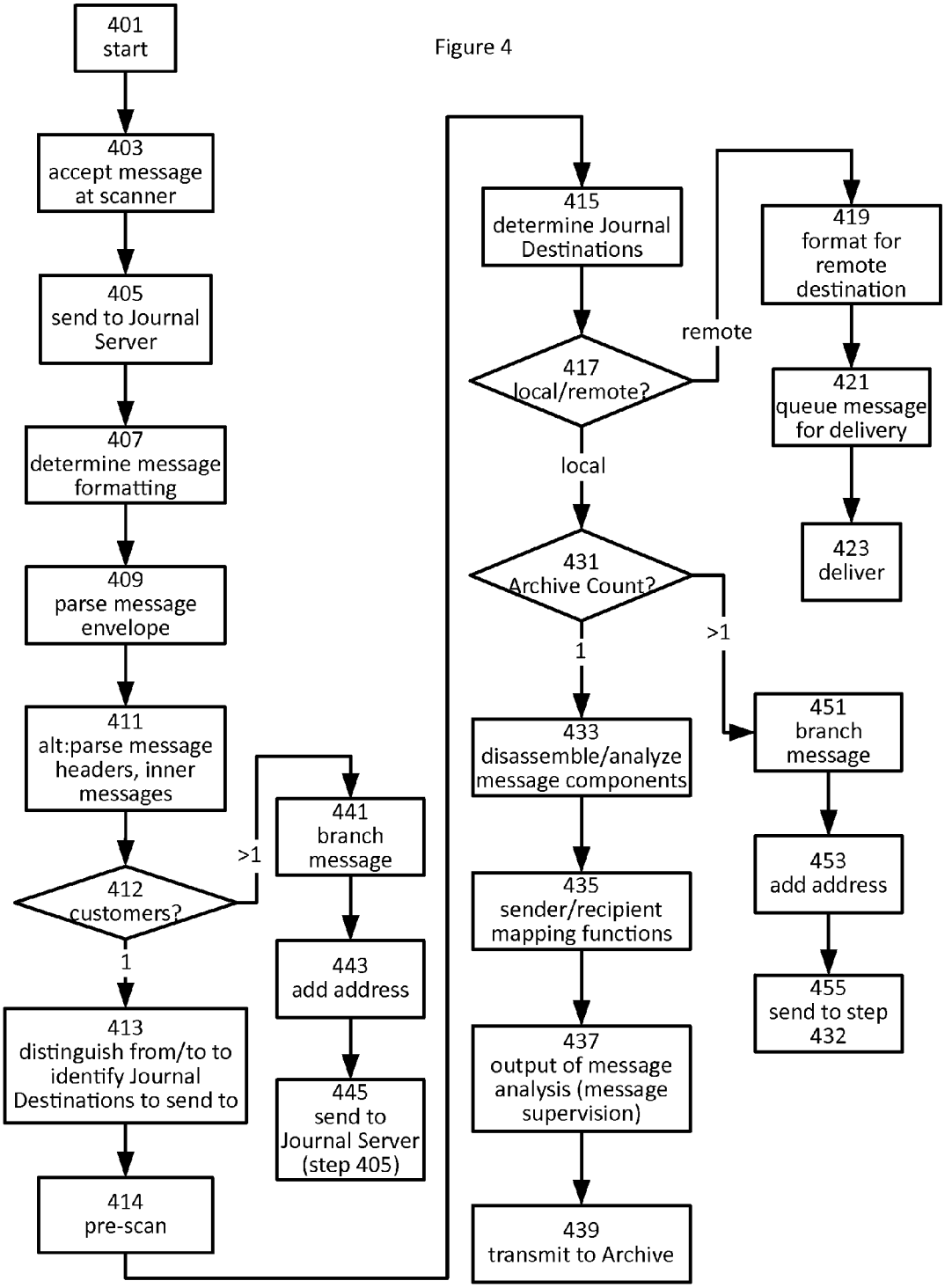

401
start
403
accept message at scanner
405
send to Journal Server
407
determine message formatting
409
parse message envelope
411
alt:parse message headers, inner messages
412
customers?
>1
441
branch message
443
add address
445
send to Journal Server (step 405)
1
413
distinguish from/to to identify Journal Destinations to send to
414
pre-scan
415
determine Journal Destinations
417
local/remote?
remote
419
format for remote destination
421
queue message for delivery
423
deliver
local
431
Archive Count?
>1
451
branch message
453
add address
455
send to step 432
1
433
disassemble/analyze message components
435
sender/recipient mapping functions
437
output of message analysis (message supervision)
439
transmit to Archive

Figure 5

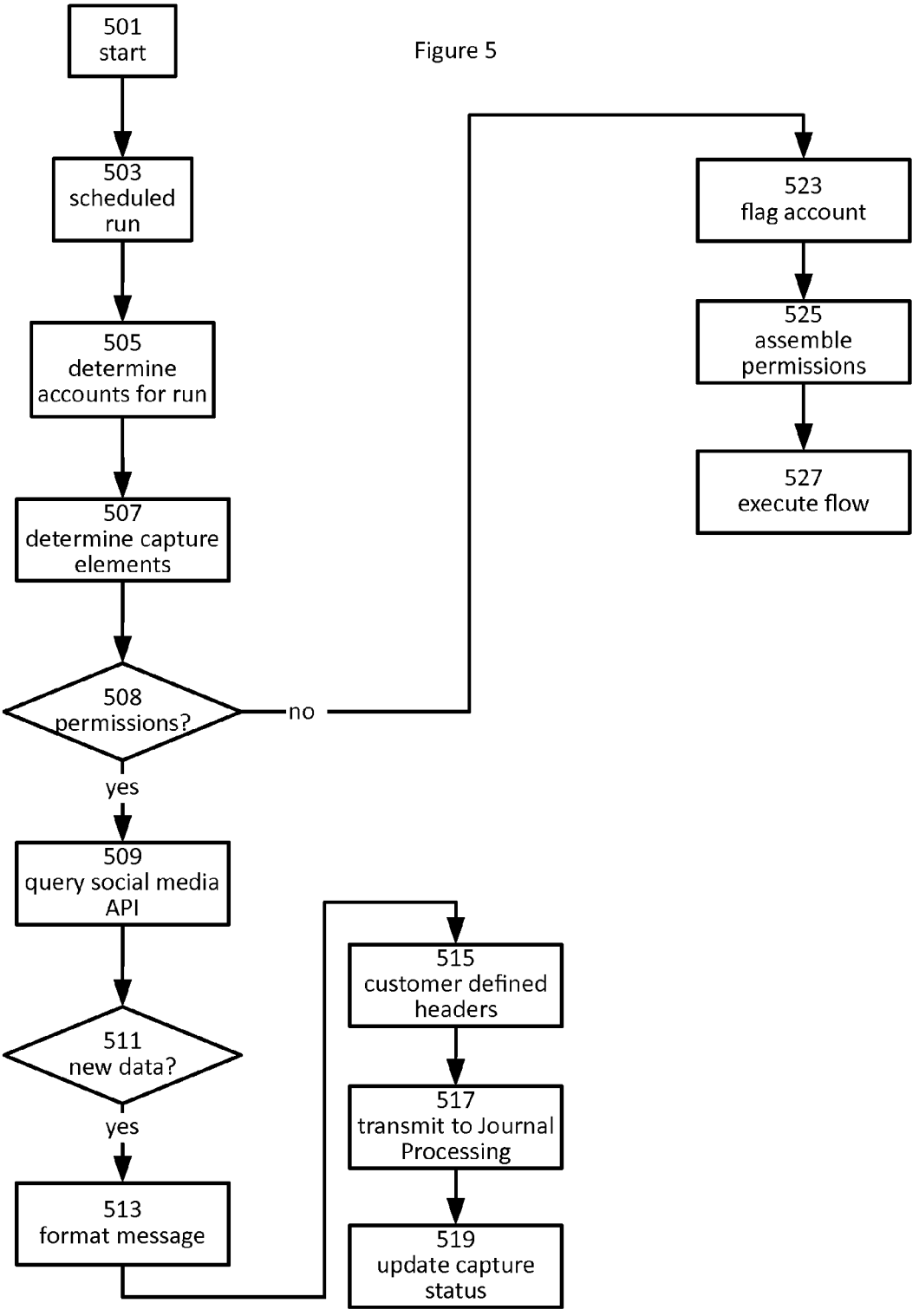
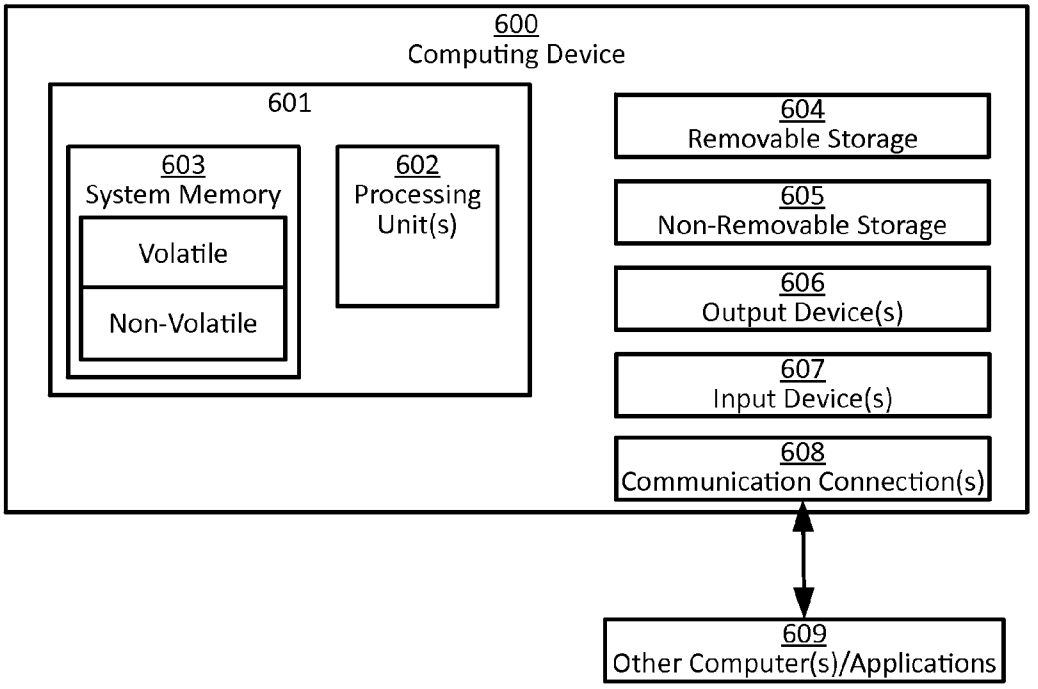

501
start
503
scheduled
run
505
determine
accounts for run
507
determine capture
elements
508
permissions?
no
yes
509
query social media
API
511
new data?
yes
513
format message
515
customer defined
headers
517
transmit to Journal
Processing
519
update capture
status
523
flag account
525
assemble
permissions
527
execute flow

Figure 6


600
Computing Device
601
603
System Memory
Volatile
Non-Volatile
602
Processing
Unit(s)
604
Removable Storage
605
Non-Removable Storage
606
Output Device(s)
607
Input Device(s)
608
Communication Connection(s)
609
Other Computer(s)/Applications

JOURNALING, ANALYSIS, AND ARCHIVING OF ELECTRONIC COMMUNICATIONS

SUMMARY OF THE INVENTION WITH BACKGROUND INFORMATION

[0001] Governmental regulatory bodies, courts, and laws required that certain communications be preserved and require that organizations and individuals respond to certain communications in prescribed manners. For example, an insurance company may be required to log (and potentially respond to) all instances in which a litigation threat is made to an insurance broker in relation to a policy written by the insurance company, even if the broker is not employed directly by the insurance company, but is an independent contractor representing multiple insurance companies. In another example, a company involved in litigation may be required to produce all communications to or from a particular employee or type of employee. In another example, a company may be required to handle credit card information in ways prescribed by contract and/or law, such as that credit card information be encrypted and/or that it not be held for longer than a specified period of time. In the United States, Sarbanes Oxley, HIPAA, the Data Protection Act, the Patriot Act, and other laws require that certain communications be preserved, sometimes in different ways (such as with different security levels) and/or responded to in different ways. Hereinafter, the term "monitored user" will refer to a party whose communications need to be journaled and archived; the monitored user may be a party such as the broker discussed above, an employee of a company, or similar.

[0002] Various service providers and software companies have begun to address the need to journal and archive electronic communications, such as email, and one-to-one or one-to-many instant messaging. However, many such solutions require that the email and/or instant messaging take place on computers under the control of the company with the journaling need and/or under the control of a journaling service provider. For example Microsoft, Inc., released an email journalling feature in service packs for Exchange™ dating back to 2000, 2003, and 2004. As is typical, the feature requires that rules be set to determine which emails should be journaled, rules based on a sender or recipient. Journaling and archiving systems commonly operate at the email server by copying a journaled message to a new email (often as an attachment), preserving the journaled message's original headers in the message body of the new email (if an email is merely forwarded by an email client, the original headers are often discarded or modified), optionally utilizing different protocols to record bcc recipients, recipients from distribution groups, and recipients who result from forwarding rules, and sending the new journal email to a journaling server and/or archive server. These systems represent a problem relative to the example provided in the preceding paragraph with respect to the insurance company broker who, as an independent contractor, may be using an email service not controlled by the insurance company. Steps may be taken to forward the email from the broker's site to the insurance company or a journaling/archiving service provider, though these steps assume that the broker controls the broker's email server, which may not be the case, and/or such an approach may result in forwarding too many emails to the journaling/archiving service provider, such as forwarding all of the broker's email and/or email from others at the broker's location which may meet the forwarding criteria. In addition, existing journaling and archiving systems do not address communications which take place in social media. Social media present a different set of problems in terms of identifying which and how communications are to be journaled/archived, accessing the social media providers, and maintaining access to the social media providers in a way which is not taxing to the monitored user.

[0003] In addition, a journaling/archiving service provider may find that an email to be journaled and archived needs to be sent to multiple journal and archive destinations, such as if the monitored user represents a company with multiple journaling and archiving destinations or if the monitored user represents more than one company, each of which may have multiple journaling and archiving destinations. For example, FIG. **3** (not showing prior art) presents a diagram of a monitor **305**. The monitor **305** may be engaged by one or more monitor customers **303** to monitor the communications sent and received by the monitored users **301**.A through **301**.C from communicators **105**.A through **105**.C (who may be anyone the monitored users **301** communicate with, including the monitor customer **303** and others). The monitor **305** may maintain its own journal servers **221** and archives **223** to journal and archive monitored communications; the monitor customer **303** may also require that communications be sent to a 3rd party monitor **307**, separate from the monitor **305**; the 3rd party monitor may maintain journal servers and archives (not shown) or may perform other operations with respect to monitored communications, such as (for example) indexing content to improve a search algorithm. The multiple archives **223**.A through **223**.C and archives and/or other processors of the 3rd party monitor **307** may utilize different formats, may have different security requirements, or generally have different structures. In this case, the multiple journaling and archiving destinations may accept the message to be journaled in different formats.

[0004] In existing approaches, multiple journaling and archiving systems must be setup separately to address the monitored users **301**. In addition, the monitor **305** would not handle social media. In addition, different journaling and archiving systems maintained by monitor **305** and 3rd party monitor **307** do not work together. **0005** In the context of email, emails generally have a structure comprising an envelope, one or more headers, a message body (or simply "body"), and attached messages. Email format is generally described in Request for Comments ("RFC") 5322, published by the Network Working Group of the Internet Engineering Task Force ("IETF"), with additional information in RFC 5321, Simple Mail Transfer Protocol ("SMTP"). The envelope generally contains addressing information which is used by email servers to route the email, generally the "to" address and a "from" or "on behalf of" address. The header generally contains addressing and additional information (such as subject and date/time), though the header information is not necessarily used by email servers to route the email. The message body generally contains text in ASCII format. Email attachments are generally in a Multipurpose Internet Mail Extensions ("MIME") format, which makes possible text in character sets other than ASCII (including for use in supporting non-ASCII header information), non-text data attachments, message bodies with multiple parts, and as otherwise specified in the following RFCs: 2045, 2046, 2047, 4288, 4289, and 2049. As used herein, emails are discussed as comprising an outer message comprising an envelope, header, body, and attachments (if any), as well as potentially

comprising an inner message. The inner message may comprise the same parts (envelope, header, body, and attachments), though the envelope of the inner message is not generally used to route the inner message. The inner message is carried in the message body of the outer message or as an attachment to the outer message. The inner message is not routed separately from the outer message (which is routed). The inner message is an email message which is attached to or made part of (the body of) the outer message

[0005] An email journal message or journal message is an outer email message which includes an inner message comprising content from a new email message. The journal message (including both outer and inner parts) may be journaled, analyzed and archived, while the new message (just the inner part of the email journal message) is sent (separately from the email journal message) to the intended recipient. In addition to the inner message comprising content from the new email message, the journal message may contain metadata related to the new message, such as times, dates, names/physical location of/identifiers for individuals involved in the communication, and/or a class or category assigned to the message by a person or by rules executed by a software program. The journal message generally follows an email transport format, such as SMTP, and is sent as an email to an email journal server. The journal message may be encrypted and/or may not be accessible to the end-user who generated the new email message which was journaled. The journal message may be handled as an email by existing communication infrastructure.

[0006] Archiving generally refers to backing up a communication, often to an off-site location or to files not actively used by an end user's email client. A journaling system may be used as an interface to an archival system.

[0007] Recently, social media (such as Facebook, Twitter, and similar) have become widely used as communication forums. Social media present many challenges in the context of journaling and archiving communications, including that authorization is required from the social media forum to perceive the communication, that social media authentication and authorization systems change frequently, that the presentation of communications to users within a social media context may depend on a host of factors (there is not necessarily a "sender" and a "recipient"), and that a wide range of communication modes are possible, including video, photographs, text exchanges taking place across short or long time frames, communications composed of content from multiple contributors selected by the social media operator and advertisers, and communications directed algorithmically at groups, rather than from one individual to another or through broadcasts.

[0008] Needed is a communication journaling and archiving system which i) obtains specified content from a social media network, re-authenticates with the social media network as necessary, ii) stores email, instant message, and content from social media networks in a system compatible with email journaling and archiving systems, and iii) can be configured to send a journaled communication to multiple journal destinations and journal formats.

SUMMARY

[0009] Disclosed is a communication journaling and archival system which obtains content from social networks, handles re-authentication requirements which occur with respect to monitored users and social networks, includes content obtained from social networks in a journal and archiving system compatible with email journaling and archiving, and can be configured to send a journaled communication to multiple journal destinations and journal formats.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. **1** depicts parties, devices, and certain communication paths in a functional block diagram.

[0011] FIG. **2** depicts devices and certain communication paths of a monitor in a functional block diagram.

[0012] FIG. **3** is a functional block diagram depicting an example of devices and certain communication paths.

[0013] FIG. **4** is a flow chart of a process described in these papers.

[0014] FIG. **5** is a flow chart of a process described in these papers.

[0015] FIG. **6** is a functional block diagram of an exemplary computing device and some data structures and/or components thereof.

DETAILED DESCRIPTION

[0016] FIG. **1** diagrams parties involved in a set of communications used as an example in these papers. Components **101**.A through **101**.C depict example representatives of service providers, service providers depicted by components **103**.A through **103**.C; these parties may be, for example, stock/bond brokers, dealers, banks, insurance companies, or other product or service providers. The representatives **101**.A-**101**.C are labeled as "3rd party Representatives," though they may be employees of one or more of the service providers **103**.A-**103**.C. A line is drawn between each of the representatives **101**.A-**101**.C and the service providers **103**.A-**103**.C, each line representing a one-to-one or one-to-many communication connection, such as may be provided by email or instant messaging. Communication lines (not shown) may also exist between the representatives as well as between service providers. The representatives **101** and service providers **103** are also referred to herein as "monitored users" and are also depicted in FIG. **3** as monitored users **301**.A through **301**.C. 3rd party Representatives **101** (or monitored users **301**) as well as others (such as service providers **103**.A-**103**.C) may also be customers of a journaling and archiving service (also referred to as a monitor **305**), in which case they are referred to herein as "monitor customers **303**."

[0017] Surrounding the representatives **101** and the service providers **103** are communicators **105**. The communicators **105** may be customers of the representatives **101**, the service providers **103**, or both. The communicators **105** may also be those who are not customers, but who may nonetheless have legally significant communications with the representatives **101** and/or the service providers **103**, which communications need to be preserved. The communicators may communicate with one another and the other parties shown in FIG. **1** via email, instant messaging, through social media networks **107**, through phone, videophone, physical mail, and in-person.

[0018] Around the representatives **101**, service providers **103**, and communicators **105** in FIG. **1** is depicted a social media network **107**. More than one social media network **107** may exist. The social media network **107** may, for example, provide an Internet based forum for exchanging identity information, text, pictures, audio, video (collectively referred to herein as "content"), and computer applications (referred

to herein as "apps") between users of the social media network **107**. The users of the social media network **107** may (without limitation) include the representatives **101**, the service providers **103**, the communicators **105**, and the regulators **109**. A user of the social media network, such as a communicator **105**, may have a "home," "wall," "landing page" or similar within the user interface of the social media network where the social media network user can post and manage content, interact with apps, identify other users with whom the user is associated (referred to herein as "friends"), and search the social media network **107** and/or the Internet. The social media network **107** may provide users with a set of permissions defining whether and how various of the user's content may be accessed by others, including other users, advertisers, app developers, and users of the Internet in general. The permissions may be set with respect to particular content items (such as a photograph, a video, the user's name, address, or similar) or groups of items (such as all photos, all videos, folders, etc.) and may specify how far the permission may propagate, such as to a friend, a friend-of-a-friend, app providers, etc. Permissions may last indefinitely or may time out. Permissions in social media networks **107** may be changed by users as well as by the operator of the social media network **107**.

[0019] Permissions may be managed, for example, through the use of an OpenID identifier or OAUTH credential or token (referred to herein as an "OAUTH credential"). Instead of providing the user's credentials (typically a username and password), the monitored user **301** (or a social media network acting on behalf of the user) may provide an OAUTH credential which provides access to some or all of a user's content in the social media network **107** for a period of time (ranging from indefinite to for a specified period). The user may provide the OAUTH credential by interacting with, for example, a "flow" supported by the social media network **107**, such as a user-agent flow, a web server flow, a device flow, or others.

[0020] In a typical flow, the monitor **305** has an account with the social media network; the monitor **305** uses the account to configure authorization requests which the monitor **305** expects to generate in relation to monitored users **301**. The monitor **305** then generates a hypertext link containing output from a hash algorithm, such as an MD5 or cryptographic algorithm, performed on an identifier for the monitored user and/or on an identifier for the monitor **305** or performed on content from the social media network associated with the monitored user, which link is sent or otherwise presented to a monitored user. When the monitored user clicks on or otherwise activates the link, the link directs the monitored user to a webserver operated by the monitor which may then redirect the monitored user to a webpage or similar generated by the social media network. The hash output identifies the monitored user **301** and the monitor **305** to the social media network. The social media network's webpage provides the monitored user **301** with an opportunity to grant permissions to the monitor **305**. If the monitored user approves the grant of permissions, then the social media network typically issues an OAUTH credential to the monitor **305**. Other flows may be used.

[0021] Turning back to FIG. **1**, regulators **109** are depicted around the other parties. The regulators **109** may include governmental regulatory bodies, courts, laws, trade group policies, contractual terms and similar which require that certain communications be preserved for prescribed times and require that organizations and individuals respond to certain communications in prescribed manners. For example, an insurance company may be required to log (and potentially respond to) all instances in which a litigation threat is made to an insurance broker in relation to a policy written by (or under) the insurance company, even if the broker is not employed directly by the insurance company, but is an independent contractor representing multiple insurance companies. In another example, a company involved in litigation may be required to produce all communications to or from a particular employee or type of employee. The regulatory requirements may be imposed on all the parties depicted in FIG. **1**. In order to preserve and potentially respond to communications as required by the regulators **109**, one or more of the service providers **103**.A-**103**.C may obtain message journaling and archiving services, such as from the monitor **305** depicted in FIGS. **2** and **3**.

[0022] FIG. **2** depicts a single monitor **305** with a system comprising multiple components. Within these components, box **202**.A depicts a message processor and VPN (virtual private network); additional boxes **202**.B and **202**.C signify that there may be more than one set of these items (still within one message journaling and archiving service provider). Box **213** depicts components used for archiving, routing, and VPN. The components in boxes **202** and **213** may be physically located together or apart (as shown). Within box **202**, there is a component for a public Internet connection **200**, which is connected to a load balancing and firewall component **201**. The load balancing and firewall **201** may then be connected to an internal network (such as, without limitation, an ethernet network) connected to one or more message processing components **203**, one or more encrypted message processing components **205**, a web server **207**, and a VPN server **209**. The message processors **203** may receive, for example, messages such as emails, instant messages, and similar. Messages may be sent, for example, by a representative **101**, a service provider **103**, or another monitored user **301**. As discussed above, the monitored user **301** may configure the monitored user's email server to send a copy or branch of all inbound and outbound email messages to the monitor **305**, which branch maintains the original message envelope. The monitored user may configure the monitored user's instant messaging client(s) to use the IM proxy **225** of the monitor **305**. The message processors **203** may also be used to transmit email out of the monitor **305**. The outbound message processors **205** may be used if outbound communications require encryption not typically offered by the message processors **203**.

[0023] The VPN server **209** at the message processor **202** is connected to a VPN server **219** at the archive, routing, and VPN component **213**. The archive, routing, and VPN component **213** is also depicted as comprising a public Internet connection **200**, a load balancing and/or firewall component **211**, which is connected to an internal network (such as, without limitation, an ethernet network) connected to components for a journal server **221**, a monitored user database **222**, an archive **223** (which may be one or more databases, one or more flat files, etc.), a management frontend **213** (which may provide a web or other interface for monitor customers **303** and the monitor **305**), and an IM proxy **225**. The journal server **221** routes messages to other journal servers (**221**.A through **221**.C in FIG. **3** and potentially 3rd party monitor **307** in FIG. **3**) and archives (**223**.A through **223**.C in FIG. **3** and potentially 3rd party monitor **307** in FIG. **3**), according to the method discussed below. The monitored user

database **222** may be one or more databases, flat files, or similar containing records associated with monitored users, such as identifiers associated with monitored users, social media provider identifiers associated with monitored users, email addresses, phone numbers, instant message identifiers and similar associated with monitored users, the output of hash algorithms performed on content associated with monitored users, the output of hash algorithms performed on identifiers associated with monitored users, time/date stamps, and similar.

[0024] FIG. **4** depicts a flow chart of steps in a process wherein messages are received, journaled, and archived. The messages may include email such as may be received at a message processor **203** and/or instant messages received or sent by an instant message client utilizing the IM proxy **225**. The messages may include email comprising content from a social media network, as discussed further below in relation to FIG. **5**.

[0025] Step **403** depicts accepting a message at a scanner, which scanner may be a message processor **203**. The scanner may provide geographic redundancy and may verify that the message is a properly formatted email. The message is then sent, for example using the VPN **209**, as a journal message to the journal server **221**. The message is sent as an inner message attached to or part of an outer message. After being accepted (not shown) at the journal server **221**, the message formatting is determined **407**. If the outer message was sent by the message processor **203**, the format may be a known first format utilized by the message processor **203**. If the message is from a third party and does not conform to the first message format, the journal server **221** may determine if the format conforms to another message format, such as the message journal format used by Microsoft, Inc. or another format. The message format is determined so that in step **409** the outer message envelope may be parsed to identify what address the outer message was sent to and what address the outer message was sent from. Determining the message format may also be used to identify headers, body, and attachments, which body and attachments may further comprise one or more inner email messages. If step **409** was not successful, then step **411** may be performed to obtain address data from the outer message headers or, in further alternatives, from inner message envelopes, headers, bodies, or attachments.

[0026] At step **412**, the number of monitor customers **303** associated with the addressing is determined (referred to in the claims as a "monitor customer container count"). The number of monitor customers **303** may be based on domain names and/or other email address portions obtained at step **409** (or **411**). Specific email addresses may be assigned to specific monitor customers and/or strings or coded strings in the envelope addresses, in headers, body, or attachments may identify or be associated with monitor customers **303**. If more than one monitor customer is determined, then the process moves to step **441**. At step **441** the message is branched. Branching may mean that both the inner and outer messages are included as inner messages in a new outer message or it may mean that only the inner message is included in a new outer message. As an example, at step **443** at least one address from or associated with the monitored customers which caused the monitored customer count to exceed one is used as an address in the envelope for the outer message of the message branch. At step **445** the message branch is processed by the journal server, similar to step **405**. The message may be branched once at step **441** and the process of steps **407** to **445** iterated to address multiple customers, with one of the addresses which caused the customer count to exceed one being used, removed, or flagged on each iteration (such as by using a specified variation on the address in the envelope for the branch); alternatively, at step **441** a branch of the message may be made for each customer exceeding one, executing steps **441** through **445** in a batch process for the set of customers exceeding one.

[0027] At step **413** records associated with the monitored users associated with the monitored customers are checked to determine if one or more of the monitor customers have requested multiple journal destinations and/or multiple journal sub-destinations based on the monitor customer and the sender/recipient in the addressing. For example, a monitor customer may have requested that any email sent to/from <example@sample.com> be sent to both one or more remote journaling service and one or more local journaling service (s). At step **414** a pre-scan may be performed. The pres-scan may analyze one or more of inner and/or outer envelopes, headers, bodies, and/or attachments to identify if the message contains content associated with a subset of the journal destinations identified in step **413**. The pre-scan step **414** may be performed before or in conjunction with step **413**.

[0028] At step **417** a decision is made regarding whether the message is to be routed to a local or a remote journal destination. If the journal destination is remote (for example, a journal not controlled by the monitor **305** and/or the party executing the process outlined in FIG. **4**), then at step **419** the format for the remote destination may be applied. As examples, the following formats may be utilized: an email format (delivered, for example, using SMTP); a text format (up/downloaded via FTP or secure FTP); an XML format (up/downloaded via FTP or secure FTP); an SQL format (delivered via SQL insert); and/or in a Lotus Notes format. At step **421** the message is queued and delivered at step **423**. If an email format was used, then delivery will typically use SMTP; if a text format was used, then the text file will typically be up/downloaded via FTP or secure FTP; if an XML format was used, the XML file will typically be up/downloaded via FTP or secure FTP; if an SQL format was used, then delivery will typically be via an SQL insert. Delivery of the message may be from a VPN component, such as **219** and/or **209**, and/or may follow additional criteria, such as that delivery will be not be done if it cannot be done via VPN or through another secure channel or only that best efforts will be made to deliver the message (securely or otherwise).

[0029] If the journal destination is local, a determination may be made at step **431** regarding whether there is one or more than one archive to which the message is to be sent. If there is more than one archive (more than one place to sent the message to for each customer associated with a message, such as with a domain name in a message address), then at step **451** a branch of the message is made for each destination, an address is created for the message branch at step **453**, and the message branch is sent to the archive (via the address) at step **455**. To avoid a looping condition, a flag may be set and/or the address created for the message branch may be a specified address format which indicates that the message branch address is derived from an address in the message and that the created address in the message should not be used again. These are examples, other ways may be used to avoid looping conditions and/or to otherwise reduce processing of the branch.

[0030] At step **433** the message components are disassembled, decoded, and analyzed, such as to obtain ASCII text, to perform optical character recognition ("OCR"), to perform lexical analysis on the text, and/or to perform image recognition or similar. At step **435** the message's sender/recipient address may be mapped to alternatives, such as an address of <user1@example.com> mapping to <user1@2ndexample.com>. The alternative address(es) may be stored in the envelope, header, or body of an outer message which contains the (now inner) message. The alternatives may be obtained, for example, from the monitored user database **222**. At step **437** the output of step **433** and/or **435** are acted on according to rules set up by the monitor customer, such as that lexical analysis at step **433** found the word "lawsuit" the output of which may cause the message to be flagged or to have the word included in message's index.

[0031] FIG. **5** depicts a flow chart of steps in a process wherein content obtained from a social media network is journaled and archived. At step **501** the process starts and then proceeds, such as at step **503**, by executing the process on a schedule, such as once per minute/hour/day/week/month or similar. At step **505**, if not already performed, the social media network accounts associated with monitored users are identified, individual monitored users potentially being associated with more than one social media network account on one or more social media networks. At step **507** the capture elements are determined, such as whether a monitor customer wants to journal and archive all content, whether the monitor customer wants to exclude audio, video, or other non-static content, or similar.

[0032] At step **508** a determination may be made regarding whether the monitor **305** has sufficient permissions to proceed with accessing the social media network to obtain the monitored user's content. Not shown, this step may involve accessing a database for permissions associated with the account, determining if any permissions have been granted, if granted permissions have timed out (if this can be determined from, for example, an OAUTH credential or similar), if permission requirements at the social media network **107** have changed, or similar. This step may be combined with or be part of step **509** or may be seen in a result of step **509**. As discussed above, permission to access content posted to the social media network **107** may have been memorialized through issuance of an OAUTH credential in a flow, by providing access credentials, or similar. If permissions are not sufficient, then the process may go to step **523** where the account is flagged, the permissions assembled in step **525**, and the appropriate flow executed at step **527**, during which the account holder will be requested to authorize the issuance of a new OAUTH credential or other permission token. **0034** If permissions were sufficient at step **508**, then at step **509** an API or similar for the social media network **107** may be used to query the social media network **107** or to otherwise obtain content posted to the social media network **107** by or in association with the account. If the social media network does not provide a way to obtain only new data compared to the last time that data was obtained, then at step **511** a determination may be made regarding whether the obtained content is new compared to the data which has previously been obtained. This determination may be performed by executing an MD5 message digest algorithm or similar hash function on the obtained data and comparing the obtained value to a value derived from previously obtained data. If new data is not found (not shown), then the process may proceed to step **519** (discussed below). If new data is found, then at step **513** one or more new messages, such as email messages, may be formatted to contain the new data. Email is a useful carrier for the new data because email is already used in message journaling and archival systems, the email bearing the content can be sent to a third-party message journaling and archival system, the MIME format is commonly used in both email and web-based content transmission and rendering systems, and the content can generally be formatted to be human-readable in an email.

[0033] At step **515** the message containing the data is customized per instructions set by the operator of the process and/or by monitor customers. In the context of email messages, examples of this include pre-/post-pending a string into the message subject line or body, including custom formating in the message body to distinguish different instances of content posted to the social media network **107** in different parts and sub-parts of the message body, to call out the time/date (or a range of time/dates across which)the content was captured at step **509** and the time/date or range of times/dates across which the content was posted (if provided by the social media network **107**), and mapping contact or identity information obtained from the social media network **107** to contact or identity information known to the operator of the process (obtained, for example, from the monitored user database **222**), which mapped contact or identity information may be used in the addressing for the email message.

[0034] At step **517** the message may be transmitted to, for example, a journal processing server, such as **221**, where the message may be processed, if it is an email message according to FIG. **4**. Alternatively, the message may be transmitted to a journal, archive, or other repository as an XML, text, or Lotus Notes file or into a database through an SQL insert or similar. One message may be sent for each new content instance or for each time content (which may comprise more than one content instance) is obtained or a message may contain more than one content instance or content obtained across a range of times.

[0035] At step **519** the capture status for the account relative to the social media network **107** may be updated. The capture status may be recorded through use of a time-stamped identifier, through use of output of an MD5 or similar algorithm performed on content associated with the account profile, or similar.

[0036] FIG. **6** is a functional block diagram of an exemplary computing device **600** that may be used to implement one or more computers described above. The computing device **600**, in one basic configuration, comprises at least a processor **602** and memory **603**. Depending on the exact configuration and type of computing device, memory **603** may be volatile (such as RAM), non-volatile (such as ROM, flash memory, etc.) or some combination of the two. Processing units and system memory may be combined, such as in a memory-resistor unit.

[0037] Computing device **600** includes one or more communication connections **608** that allow computing device **600** to communicate with one or more computers and/or applications **609**. Device **600** may also have input device(s) **607** such as a keyboard, mouse, digitizer or other touch-input device, voice input device, etc. Output device(s) **606** such as a monitor, speakers, printer, PDA, mobile phone, and other types of digital display devices may also be included.

[0038] Additionally, device **600** may also have other features and functionality. For example, device **600** may also

include additional storage (removable **604** and/or non-removable **605**) including, but not limited to, solid-state media, magnetic or optical disks or tape. 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. Memory **603**, removable storage **604**, non-removable storage **605**, and smart cards **610** are all examples of computer storage media. 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 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 accessed by device **600**. Any such computer storage media may be part of device **600**.

[0039] Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise," "comprising," and the like are to be construed in an inclusive sense, as opposed to an exclusive or exhaustive sense; that is to say, in the sense of "including, but not limited to." As used herein, the term "connected," "coupled," or any variant thereof means any connection or coupling, either direct or indirect, between two or more elements; the coupling of connection between the elements can be physical, logical, or a combination thereof. Additionally, the words "herein," "above," "below," and words of similar import, when used in this application, shall refer to this application as a whole and not to any particular portions of this application. Where the context permits, words in the above Detailed Description using the singular or plural number may also include the plural or singular number, respectively. The word "or," in reference to a list of two or more items, covers all of the following interpretations of the word: any of the items in the list, all of the items in the list, and any combination of the items in the list.

[0040] The above Detailed Description of embodiments of the system is not intended to be exhaustive or to limit the system to the precise form disclosed above. While specific embodiments of, and examples for, the system are described above for illustrative purposes, various equivalent modifications are possible within the scope of the system, as those skilled in the relevant art will recognize. For example, while processes or blocks are presented in a given order, alternative embodiments may perform routines having operations, or employ systems having blocks, in a different order, and some processes or blocks may be deleted, moved, added, subdivided, combined, and/or modified to provide alternative or subcombinations. Each of these processes or blocks may be implemented in a variety of different ways. Also, while processes or blocks are at times shown as being performed in series, these processes or blocks may instead be performed in parallel, or may be performed at different times. Further, any specific numbers noted herein are only examples: alternative implementations may employ differing values or ranges.

1. A first computer configured to journal and archive email messages, which first computing device executes a method comprising the following steps:

receiving a message, which message contains an inner message which had been sent to or from a monitored user;

determining a format of the received message and/or of the inner message;

identifying addresses of senders and/or recipients in the received message;

determining a monitor customer container count;

if the monitor customer container count is greater than one, then branching the message and/or inner message for each monitor customer container count greater than one;

performing a pre-scan of the message and/or inner message, and analyzing the pre-scan result to identify if the pre-scan result is associated with a journal destination;

analyzing message and/or inner message components;

determining if analysis of message components is associated with a journal destination;

delivering the message and/or inner messages thereof to at least one journal and/or archive.

2. The method according to claim **1** wherein identifying addresses of senders and/or recipients in the received message further comprises identifying addresses in at least one inner message.

3. The method according to claim **1** wherein identifying addresses of senders and/or recipients in the received message further comprises parsing the message headers to determine if the received message was addressed to a sender and/or recipient not in the received message envelope.

4. The method according to claim **1** further comprising mapping sender and/or recipient addresses to alternatives.

5. The method according to claim **4** further comprising including the alternatives in the message envelope.

6. The method according to claim **1** further comprising delivering the message to more than one journal when a result of message and/or inner message component analysis is associated with more than one journal.

7. The method according to claim **1** where a monitor customer container count is determined by a domain name found in a message sender and/or recipient address.

8. The method according to claim **7** further comprising adding a recipient address associated with the domain name which caused the customer container count to exceed one to the message envelope of the branched message and iterating the method of claim **1** with the branched message.

9. The method according to claim **8** wherein the added recipient address is pre-determined and indicates that the customer container count for the branched message is one.

10. The method according to claim **1** where a monitor customer container count is determined by comparing senders and/or recipients from the message and/or inner message to records associated with monitor customers to determine one or more customer containers associated with senders and/or recipients associated with monitor customers.

11. The method according to claim **1** wherein analyzing message and/or inner message components further comprises at least one of performing lexical analysis on text, performing optical character recognition on a graphic, performing speech-to-text, and performing image recognition on a graphic.

12. The method according to claim **1** further comprising determining if the message or any branches thereof are to be delivered to a remote destination, and, if so, determining a format for delivering the message and any branches thereof and delivering the message and any branches thereof to the remote destination in the determined format.

13. The method according to claim **12** wherein the format for delivering the message is selected from at least one of an email format, a text format, an SQL format, a Lotus Notes format, and an XML format.

14. The method according to claim **1** further comprising a second computing device which receives the message and sends the message to the first computing device.

15. A first computer configured to obtain content associated with a first party from a social media provider, which first computing device executes a method comprising the following steps:

querying a social media provider for content associated with the first party;

obtaining from the social media provider content associated with the first party;

formatting a message to contain at least of the of the selected obtained content;

mapping the obtained content to the message format;

transmitting the message to a second computer configured as a journal processor;

updating a record associated with the first party to indicate that the content associated with the first party from the social media provider has been obtained.

16. The method according to claim **15** wherein the message is an email message.

17. The method according to claim **15** further comprising customizing the message according to instructions received from a second party, prior to transmitting the message to the computer configured as a journal processor.

18. The method according to claim **15** further comprising providing a user interface to allow a second party to select what of the obtained content to journal and/or archive.

19. The method according to claim **15** wherein selecting obtained content to journal and/or archive comprises selecting at least one of all content obtained from the social media provider, non-video content obtained from the social media provider, and non-graphic content obtained from the social media provider.

20. The method according to claim **15** wherein the first computer and the computer configured as a journal processor are the same computer.

21. The method according to claim **15** wherein updating a record associated with the first party to indicate that the content associated with the first party from the social media provider has been obtained comprises associating an identifier associated with the first party with a timestamp associated with when the content associated with the first party was either obtained from the social media provider or posted to the social media provider by the first party.

22. The method according to claim **15** wherein updating a record associated with the first party to indicate that the content associated with the first party from the social media provider has been obtained comprises performing a hash on content associated with the first party obtained from the social media provider and storing the hash value in association with the first party.

23. The method according to claim **22** wherein the hash is an MD5 hash.

24. A first computer configured to obtain content associated with a first party from a social media provider and to journal and archive the obtained content, which first computing device executes a method comprising the following steps:

determining from the social media provider that a permission granted to access content posted to the social media provider and associated with the first party is invalid;

determining the permissions required to access the social media provider;

creating a first message to the first party requesting the determined permissions;

transmitting the first message to the first party;

obtaining the requested permission from the first party via data received from social media provider; then utilizing the obtained permission to obtain content associated with the first party from the social media service;

creating a second message containing the obtained content;

journaling the second message.

25. The method according to claim **24** wherein creating the first message to the first party requesting the determined permissions further comprises generating a link associated with the first party, which link points to a webpage hosted by the first or a second computer, and including the generated link in the first message.

26. The method according to claim **25** further comprising performing a hash algorithm on at least one of an identifier associated with the first party and content associated with the first party, output from which hash algorithm is associated with the first user in a database accessible to the first computer, and including output from the hash algorithm in the generated link.

27. The method according to claim **24** wherein creating the second message containing the obtained content comprises formatting the second message to contain at least of the of the obtained content and mapping the obtained content to the second message format.

28. The method according to claim **24** wherein the data comprises an OAUTH credential.

29. The method according to claim **24** wherein the second message is an email message.

* * * * *