



US 20140192968A1

(19) **United States**(12) **Patent Application Publication**
Stroud et al.(10) **Pub. No.: US 2014/0192968 A1**(43) **Pub. Date: Jul. 10, 2014**(54) **SELECTIVE FACSIMILE DENIAL**

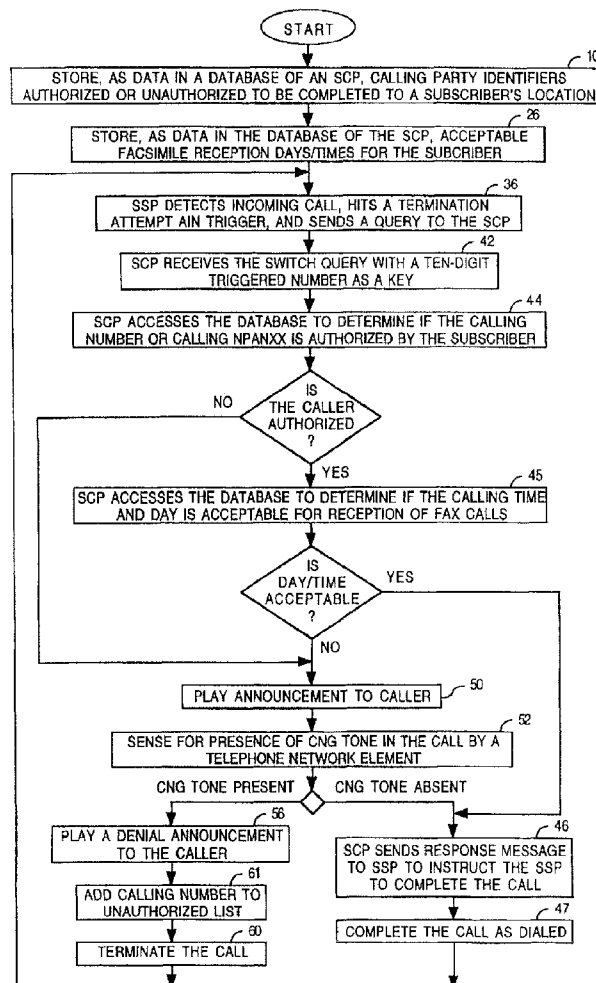
7,653,184, Continuation of application No. 10/967,100, filed on Oct. 15, 2004, now Pat. No. 7,006,612.

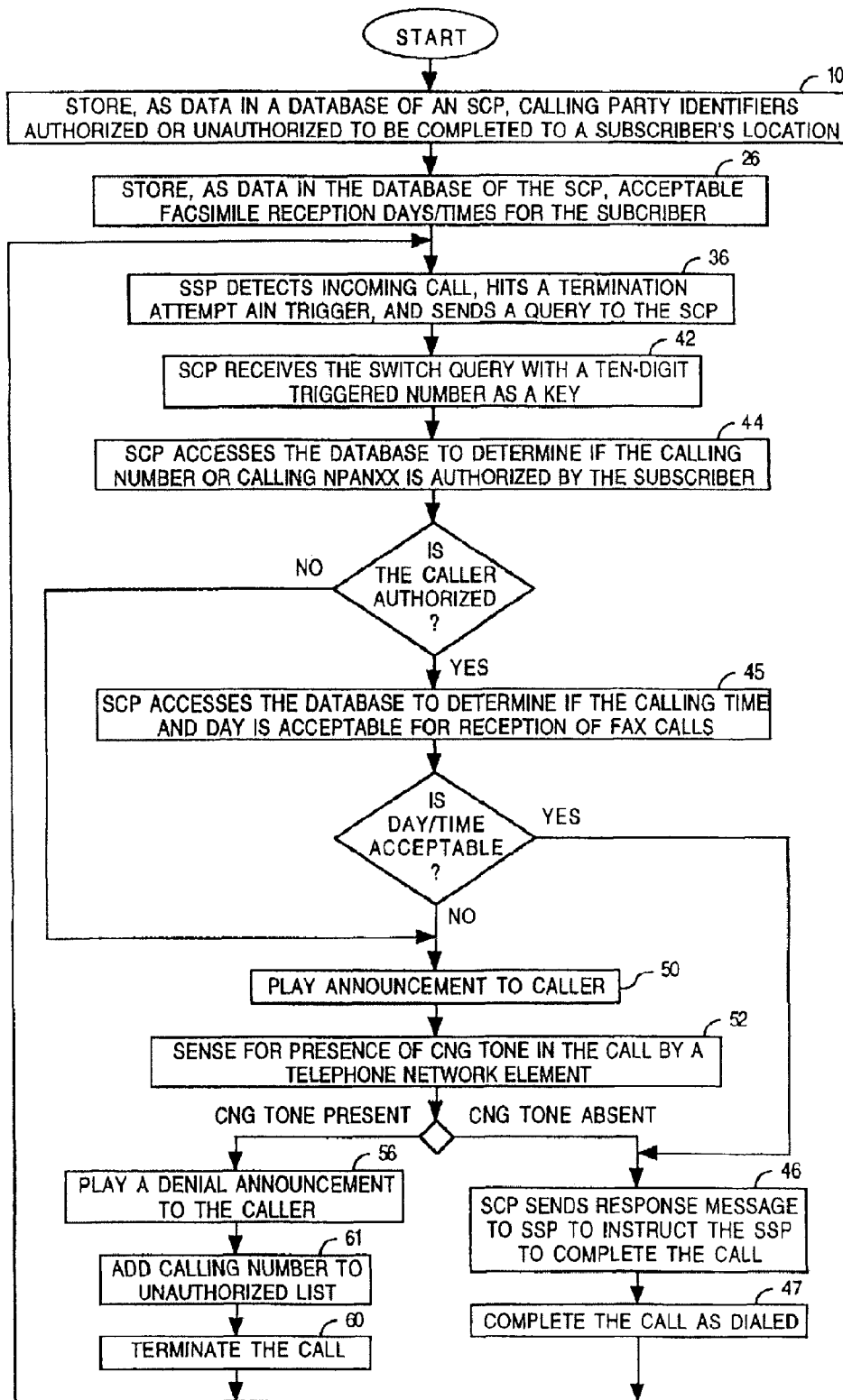
(71) Applicant: **AT&T Intellectual Property I, L.P.**,
Atlanta, GA (US)**Publication Classification**(72) Inventors: **Kenneth Robert Stroud**, Lago Vista,
TX (US); **Paul A. Raccio**, Wallingford,
CT (US)(51) **Int. Cl.**
H04N 1/32 (2006.01)(52) **U.S. Cl.**
CPC **H04N 1/3201** (2013.01)
USPC **379/93.02**(73) Assignees: **SBC KNOWLEDGE VENTURES, L.P.**; **AT&T Intellectual Property I, L.P.**, Atlanta, GA (US)(57) **ABSTRACT**

A method includes determining, at a processor of a computing device, whether an incoming transmission to a first destination is authorized at an electronic device of a communication network. The method includes, in response to determining that the incoming transmission is not authorized, determining whether a particular type of content is communicated via the incoming transmission. The incoming transmission is routed to the first destination when the particular type of content is not communicated via the incoming transmission, and the incoming transmission is not routed to the first destination when the particular type of content is communicated via the incoming transmission.

(21) Appl. No.: **14/206,470**(22) Filed: **Mar. 12, 2014****Related U.S. Application Data**

(63) Continuation of application No. 13/774,085, filed on Feb. 22, 2013, now Pat. No. 8,712,022, Continuation of application No. 12/636,115, filed on Dec. 11, 2009, now Pat. No. 8,406,393, Continuation of application No. 11/274,364, filed on Nov. 15, 2005, now Pat. No.



**FIG. 1**

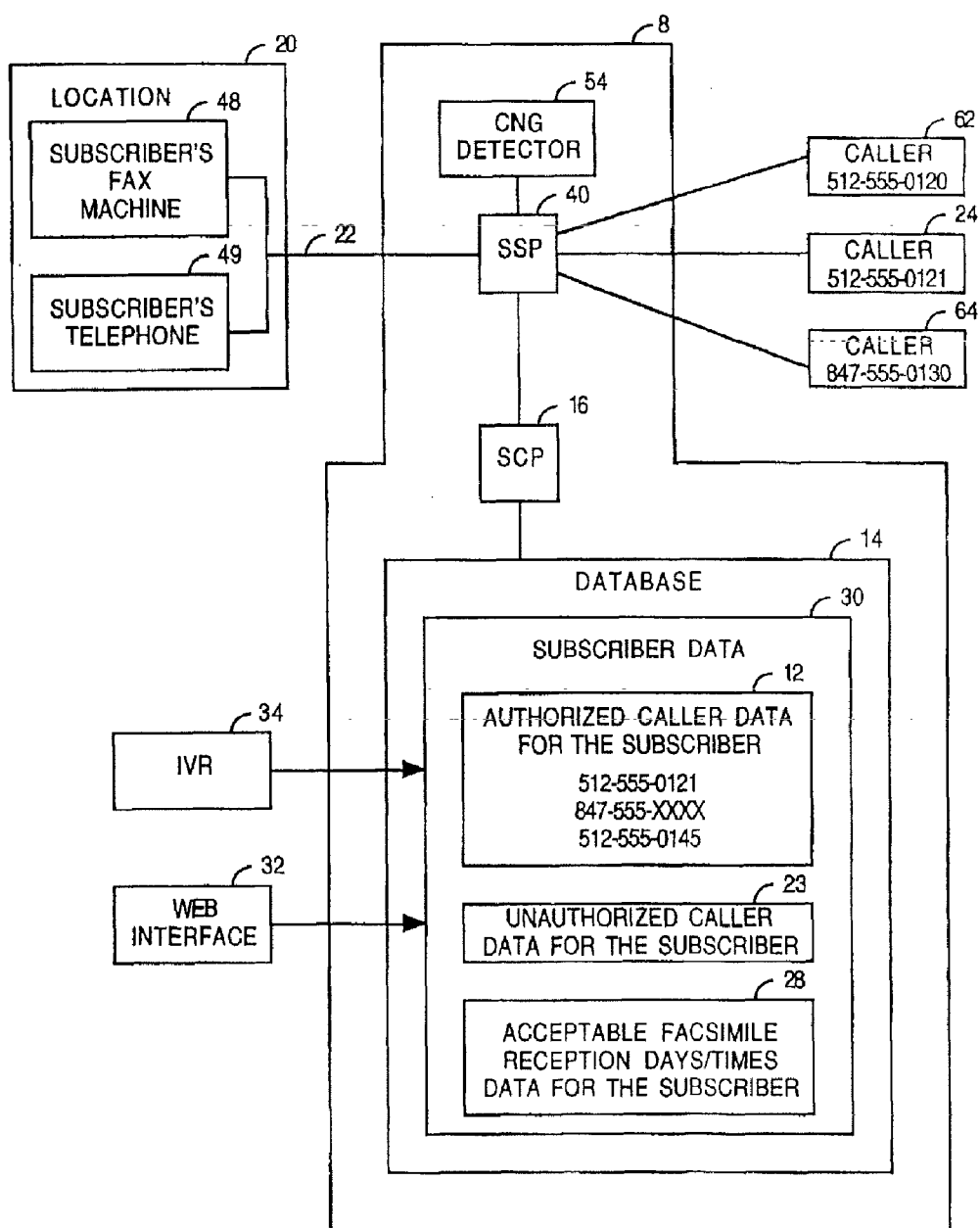


FIG. 2

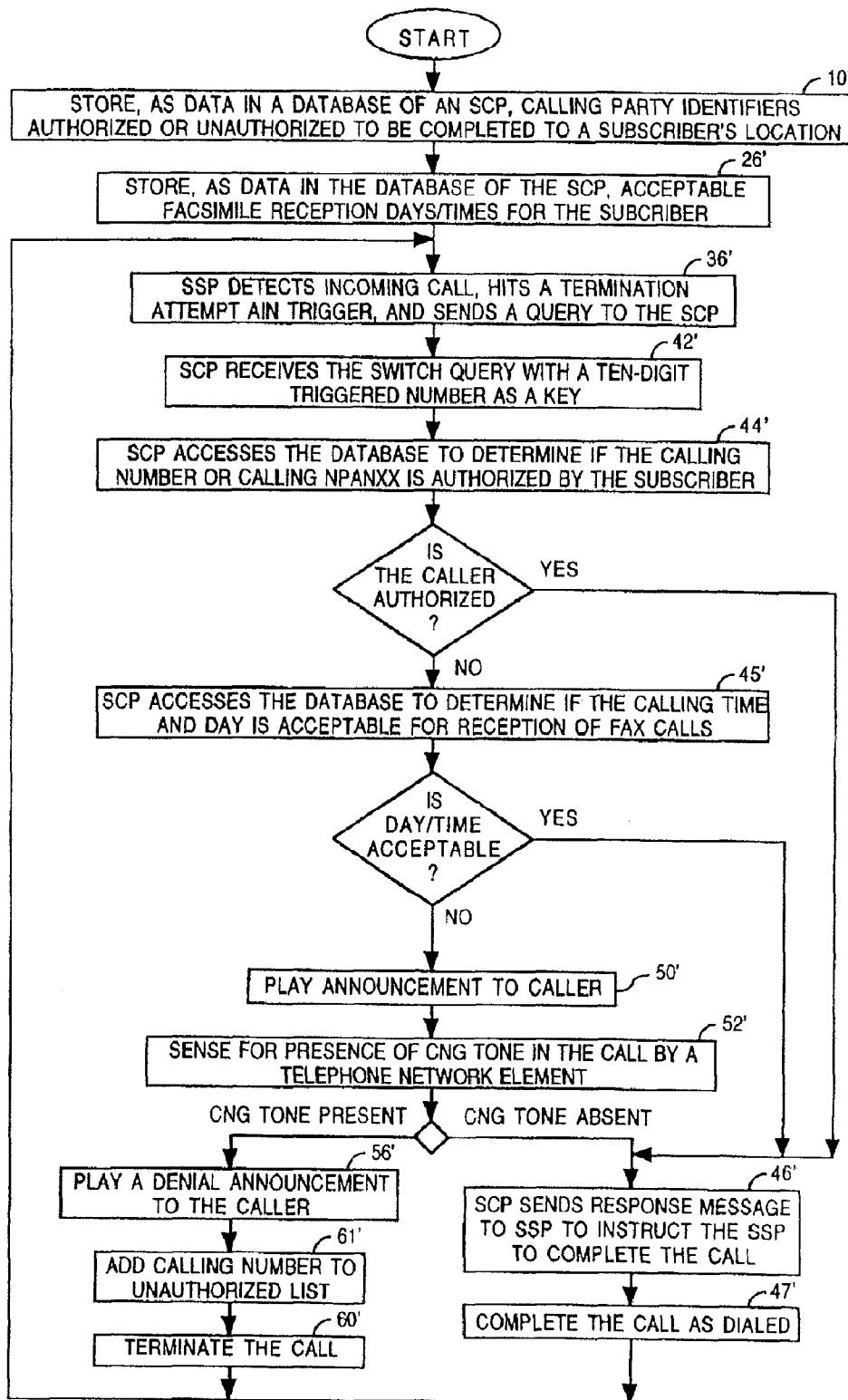


FIG. 3

SELECTIVE FACSIMILE DENIAL

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a continuation of and claims priority from U.S. Patent Application No. 13/774,085, filed on February 22, 2013, which is a continuation of U.S. Patent Application No. 12/636,115, filed December 11, 2009 (now U.S. Patent No. 8,406,393), which is a continuation of U.S. Patent Application No. 11/274,364, filed November 15, 2005 (now U.S. Patent No. 7,653,184), which is a continuation of U.S. Patent Application No. 10/967,100, filed October 15, 2004 (now U.S. Patent No. 7,006,612). Each of the above-referenced applications is incorporated by reference herein in its entirety.

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates to systems for handling incoming facsimile transmissions.

BACKGROUND

[0003] Junk faxes and other unwanted advertisements are often transmitted to business facsimile machines. This results in wasted paper and toner and frustration for the business owner and its employees.

[0004] Many residential owners of facsimile machines use their telephone line for facsimile purposes only on an occasional, outgoing basis. These facsimile machine owners do not wish to have their phone ring during inconvenient hours due to unwanted, incoming faxes, but still wish to receive incoming voice calls.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The present disclosure is pointed out with particularity in the appended claims. However, other features are described in the following detailed description in conjunction with the accompanying drawings in which:

[0006] FIG. 1 is a flow chart of an embodiment of a method of blocking unwanted faxes in a telephone network;

[0007] FIG. 2 is a block diagram of an embodiment of a system for blocking unwanted faxes in the telephone network; and

[0008] FIG. 3 is a flow chart of another embodiment of a method of blocking unwanted faxes in a telephone network.

DETAILED DESCRIPTION

[0009] In a particular embodiment, a system includes a switch and a control module coupled to the switch. The control module is configured to determine whether an incoming telephone call to a telephone line is a facsimile call or a voice call. The control module is also configured to determine, based on a telephone number associated with the incoming telephone call, whether facsimile calls are authorized to be routed to the telephone line. When facsimile calls are authorized, the control module is further configured to instruct the switch to route the incoming telephone call to the telephone line. When facsimile calls are not authorized and the incoming call is a voice call, the control module is configured to instruct the switch to route the incoming telephone call to the telephone line. The control module is also configured to instruct the switch to deny routing of the incoming telephone

call to the telephone line when facsimile calls are not authorized and the incoming call is a facsimile call.

[0010] In another particular embodiment, a method also includes detecting an incoming call at switch of a telephone network. The method includes determining whether facsimile calls are authorized to be routed to a destination. The method further includes routing the incoming call to the destination when facsimile calls are authorized. The method includes determining whether the incoming call includes a facsimile tone when facsimile calls are not authorized. The method also includes routing the incoming call to the destination when the incoming call does not include the facsimile tone. The method further includes denying routing of the incoming call to the destination and routing the incoming call to a second destination when the incoming call includes the facsimile tone.

[0011] In another particular embodiment, a computer-readable storage medium includes instructions, that when executed by a computer, cause the computer to detect an incoming call and determine whether facsimile calls are authorized to be routed to a destination. The instructions also cause the computer to route the incoming call to the destination when facsimile calls are authorized. When facsimile calls are not authorized, the instructions further cause the computer to selectively route the incoming call to the destination based on whether the incoming call includes a facsimile tone.

[0012] Embodiments of the present disclosure block or re-route an unwanted, incoming facsimile transmission call by sensing for a presence of a fax transmission tone within an element of a public telephone network before the telephone network completes the call to a called party. A subscriber-updateable list, table or other data structure that contains authorized calling party identifiers is stored and accessed within the telephone network. The authorized calling party identifiers indicate telephone numbers from which calls are authorized to be completed to the subscriber's location for purposes of fax transmission. The telephone network uses the list to determine whether or not to complete an incoming call as dialed, and whether or not to further analyze the call for the presence of a fax transmission tone, such as a CNG tone. If the telephone network detects the fax tone, the telephone network either blocks or re-routes the incoming call. The telephone network can use an Advanced Intelligent Network (AIN) architecture or alternative architecture to control the handling of calls once the presence or absence of the fax tone is determined.

[0013] Embodiments of the present disclosure are described with reference to FIG. 1, which is a flow chart of an embodiment of a method of blocking unwanted faxes in a telephone network 8, and FIG. 2, which is a block diagram of an embodiment of a system for blocking unwanted faxes in the telephone network 8. The telephone network 8 may be part of a public switched telephone network, a Voice over Internet Protocol (VoIP) telephone network, or a non-traditional phone network.

[0014] As indicated by block 10, the method comprises storing, as data 12 in a database 14 of a service control point (SCP) 16, one or more calling party identifiers from which fax transmission calls are authorized to be completed to a telephone line 22 at a subscriber's location 20. Optionally, the database 14 also stores data 23 indicating one or more other calling party identifiers from which fax transmission calls are explicitly unauthorized to be completed to the telephone line 22 at the subscriber's location 20.

[0015] The calling party identifiers may comprise ten-digit calling numbers and/or portions of ten-digit calling numbers. An example of a portion of a ten-digit calling number is a six-digit NPA-NXX number, where NPA is a three-digit area code and NXX are three digits identifying a specific telephone central office in the area code. When included in the authorized data 12, the NPA-NXX data authorizes completion of fax transmission calls from any telephone number having the NPA-NXX. Use of NPA-NXX combinations in the data 12 is useful where the subscriber has a large number of potential callers within the same NPA-NXX. For example, the subscriber may want to receive faxes from a firm whose headquarters is at a single location and has a large number of potential callers within the same NPA-NXX. In this case, the subscriber would not need to store all of the headquarters' ten-digit numbers in the data 12 of the database 14.

[0016] For purposes of illustration and example, consider the data 12 indicating that the subscriber has authorized reception of fax transmission calls from a first party 24 whose ten-digit number is 512-555-0121, a second party whose ten-digit number is 512-555-0145, and any party whose NPA-NXX is 847-555. Those having ordinary skill will recognize that the data 12 generally can include any number of authorized calling party identifiers.

[0017] Optionally, as indicated by block 26, the method further comprises storing, as data 28 in the database 14 of the SCP 16, days and/or times at which facsimile reception using the telephone line 22 is acceptable or unacceptable to the subscriber. The times may indicate times of day, and the days may indicate specific dates and/or specific days of the week, on which facsimile reception is acceptable or unacceptable. The data 28 is used to provide an additional restriction mechanism for incoming faxes. For example, the subscriber may wish to block all incoming faxes received after business hours.

[0018] Subscriber data 30, which includes the data 12, 23 and 28, can be updated by the subscriber using a Web interface 32 and/or an interactive voice response (IVR) system 34. The subscriber can view a visual display of the calling party identifiers from the data 12 or 23 using the Web interface 32, or can hear an audible display of the calling party identifiers from the data 12 or 23 using the IVR system 34. The subscriber can add or remove calling party identifiers (whether they be full ten-digit numbers or NPA-NXX numbers) from the data 12 or 23 by issuing commands using the Web interface 32 and/or the IVR system 34. Further, the subscriber can add or remove days/times to the data 28, or may choose to turn the fax blocking feature on or off by issuing commands using the Web interface 32 and/or the IVR system 34. The IVR system 34 may be receptive to both voice commands and DTMF commands.

[0019] Optionally, a telephone network element may automatically add to the data 23 a list of one or more unauthorized calling numbers whose calls to the telephone line 22 have been previously blocked by the subscriber.

[0020] As indicated by block 36, a telephone network switch such as a service switching point (SSP) 40 detects an incoming call from a calling party that is intended for the telephone line 22 of the subscriber. Based on detecting the incoming call, the SSP 40 hits a termination attempt advanced intelligent network (AIN) trigger, and sends a query message to the SCP 16 based on the AIN trigger.

[0021] As indicated by block 42, the SCP 16 receives the query message with a ten-digit triggered number of the telephone line 22 as the key.

[0022] As indicated by block 44, the SCP 16 accesses the subscriber data 30 of the database 14 based on the key. The data 12 of the subscriber data 30 is accessed to determine if the subscriber has authorized reception of incoming faxes from the calling number of the calling party. If the data 12 indicates that the subscriber has authorized reception of incoming faxes from the calling party, then optionally the SCP accesses the data 28 of the database to determine if fax reception is acceptable at the current time and/or day, as indicated by block 45.

[0023] If the calling party is authorized based on the data 12 and the time/day is acceptable based on the data 28, then the SCP 16 sends a response message to the SSP 40 to instruct the SSP 40 to complete the call to the telephone line 22, as indicated by block 46. As indicated by block 47, the call is completed to the telephone line 22 as dialed. If the call includes an incoming fax transmission, the subscriber can receive the fax transmission using a fax machine 48 coupled to the telephone line 22. If the call is a voice call, the subscriber can answer the voice call and vocally communicate with the calling party using a telephone 49 coupled to the telephone line 22.

[0024] If the calling party is authorized based on the data 12 but the time/day is unacceptable based on the data 28, or if the calling party is unauthorized based on the data 12 or 23, then an act of playing an announcement to the caller is performed as indicated by block 50. The announcement may comprise an audible phrase such as "please hold while we attempt to complete your call" or a recorded ring. Use of the recorded ring makes the call screening process inconspicuous, or ideally indiscernible, to human callers. Regardless of its audible content, the announcement may be a four-second or other duration AIN switch announcement.

[0025] As indicated by block 52, a telephone network element senses for a presence of a fax transmission tone from the calling party over the duration of the announcement and before the call has been routed to the telephone line 22. The telephone network element may comprise a plain-old telephone system (POTS) network element or a Voice over Internet Protocol (VoIP) network element, for example.

[0026] Sending facsimile machines generate an on-off cadence of fax transmission tones until a receiving facsimile machine generates a response thereto. Thus, the act indicated by block 52 is used by the telephone network to determine whether or not the calling party is sending a fax in the call.

[0027] In one embodiment, the fax transmission tone comprises a CNG tone and the response comprises a CED (Called station iDentification) tone. An ideal CNG tone comprises a 1100-Hz signal for 0.5 seconds followed by no signal for 3 seconds. According to ITU T.30, an acceptable CNG tone is within a frequency tolerance of ± 38 Hz and a timing tolerance of $\pm 15\%$ of the aforementioned ideal CNG tone.

[0028] The telephone network comprises a CNG detector 54 to detect if an acceptable CNG tone has been generated by the calling party during the announcement. The CNG detector 54 waits to collect one digit during the announcement. If a digit has not been collected by the end of the announcement (e.g. by the end of about four seconds) or if a collected digit does not equal 1100 Hz ± 38 Hz, it is assumed that the call is

absent an acceptable CNG tone. If the collected digit is within 1100 Hz $\pm$ 38 Hz, it is assumed that the call has an acceptable CNG tone.

[0029] If a fax transmission tone from the calling party is present in the call (e.g. the CNG detector 54 detects an acceptable CNG tone), then the call is considered to be a fax call either from an unauthorized calling party based on the data 12 or 23, or at an unacceptable day/time based on the data 28. To block these fax calls from being completed to the telephone line 22, flow of the method is directed to block 56 which indicates an act of playing a denial announcement to the calling party, and block 60 which indicates an act of terminating the call. As an alternative to blocking and terminating these unwanted fax calls, an act of re-routing these fax calls to a different fax machine location having a different telephone line may be performed. Either way, the SSP 40 is instructed by the SCP 16 to deny completion of the call to the telephone line 22. Optionally, as indicated by block 61, the calling party identifier (e.g. the telephone number) of the calling party is added to a list of unauthorized calling party identifiers in the data 23. As a result, the database 14 includes a calling party identifier of the calling party to indicate that subsequent facsimile transmission calls from the calling party are unauthorized to be completed to the telephone line 22 of the subscriber.

[0030] If the call is absent a fax transmission tone from the calling party (e.g. the CNG detector 54 does not detect an acceptable CNG tone), then the call is considered not to be a fax call but rather a voice call. Since non-fax calls are allowed to be completed, flow of the method is directed to block 46 which comprises the SCP 16 sending a response message to the SSP 40 to instruct the SSP 40 to complete the call to the telephone line 22. This allows a son/daughter to call his/her parents in the middle of the night even when the telephone network is screening fax calls intended for the parents' telephone line, for example.

[0031] The above acts can be repeated for additional incoming calls intended for the telephone line 22.

[0032] For purposes of illustration and example, consider how the herein-described method and system process the following three hypothetical calls.

[0033] Call 1

[0034] The caller 24, whose telephone number is 512-555-0121, places a call to the telephone line 22. Since the telephone number of the caller 24 is an authorized number in a table in the data 12, and the call has been placed during acceptable hours as indicated by the data 28, the telephone network completes the call as dialed. The subscriber may answer the call using either the fax machine 48 or the telephone 49.

[0035] Call 2

[0036] A caller 62, whose telephone number is 512-555-0120, places a call to the telephone line 22. Since the telephone number of the caller 62 is not in a table of authorized numbers in the data 12, the caller 62 hears an audible announcement such as "please hold while we attempt to complete your call". The call is analyzed, within the telephone network, for a CNG tone. If a CNG tone is present, the call is denied and an audible termination announcement is played to the caller 62. If a CNG tone is not present, the telephone network completes the call as dialed.

[0037] Call 3

[0038] A caller 64, whose telephone number is 847-555-0130, places a call to the telephone line 22. The NPA-NXX

combination of 847-555 of the caller 64 is in a table of authorized numbers in the data 12, however the call is placed after normal business hours as indicated by the data 28. The caller 64 hears an audible announcement such as "please hold while we attempt to complete your call". The call is analyzed, within the telephone network, for a CNG tone. If a CNG tone is present, the call is denied and an audible termination announcement is played to the caller 64 because fax calls are not accepted after normal business hours. If a CNG tone is not present, the telephone network completes the call as dialed.

[0039] The herein-disclosed method and system can be used to block and/or re-route incoming facsimile transmissions for multiple subscribers. The database 14 would include respective subscriber data for each subscriber, such as the subscriber data 30 for the example subscriber described herein. Each subscriber would be able to access and modify his/her subscriber data using the Web interface 32 and/or the IVR 34.

[0040] FIG. 3 is a flow chart of another embodiment of a method of blocking unwanted faxes in a telephone network. This embodiment includes the same acts described with reference to FIG. 1, but with an alternative flow topology. Each act indicated by a primed reference numeral in FIG. 3 corresponds to a respective act having the same, but non-primed reference numeral in FIG. 1.

[0041] The alternative flow topology can be summarized as follows. If the calling party is authorized based on the data 12 or the time/day is acceptable based on the data 28, then the SCP 16 sends a response message to the SSP 40 to instruct the SSP 40 to complete the call to the telephone line 22, as indicated by block 46'. If the calling party is not authorized based on the data 12 or 23 and the time/day is unacceptable based on the data 28, then acts of playing an announcement to the caller and sensing for the presence of a CNG tone are performed as indicated by blocks 50' and 52'.

[0042] The acts performed by each of the herein-disclosed components can be directed by respective computer program code embodied in a computer-readable form on a computer-readable medium. Each of the herein-disclosed components may comprise a respective computer processor responsive to the computer program code to perform the acts.

[0043] It will be apparent to those skilled in the art that the disclosed embodiments may be modified in numerous ways and may assume many embodiments other than the particular forms specifically set out and described herein.

[0044] The above disclosed subject matter is to be considered illustrative, and not restrictive, and the appended claims are intended to cover all such modifications, enhancements, and other embodiments which fall within the scope of the present disclosure. Thus, to the maximum extent allowed by law, the scope of the present disclosure is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.

What is claimed is:

1. A method comprising:

determining, at a processor of a computing device, whether an incoming transmission to a first destination is authorized at an electronic device; and

in response to determining that the incoming transmission is not authorized:

determining whether a particular type of content is communicated via the incoming transmission;

routing the incoming transmission to the first destination when the particular type of content is not communicated via the incoming transmission; and denying routing of the incoming transmission to the first destination when the particular type of content is communicated via the incoming transmission.

2. The method of claim 1, further comprising, in response to determining that the incoming transmission is authorized, routing the incoming transmission to the first destination.

3. The method of claim 1, further comprising routing the incoming transmission to a second destination when the particular type of content is communicated via the incoming transmission.

4. The method of claim 1, wherein determining whether the incoming transmission to the first destination is authorized is based on an identifier of a source of the incoming transmission.

5. The method of claim 4, further comprising determining whether a particular telephone number is included in a list of authorized identifiers.

6. The method of claim 1, wherein determining whether the incoming transmission to the first destination is authorized is based on a date of the incoming transmission, a time of the incoming transmission, or a combination thereof.

7. The method of claim 6, further comprising determining whether the time of the incoming transmission is within an authorized time range.

8. The method of claim 1, further comprising adding an identifier of a source of the incoming transmission to a list of unauthorized identifiers after determining that the particular type of content is communicated via the incoming transmission.

9. The method of claim 1, further comprising providing a message to a source of the incoming transmission after denying routing of the incoming transmission to the first destination.

10. The method of claim 1, wherein determining whether the particular type of content is communicated via the incoming transmission comprises determining whether content of the incoming transmission includes a particular type of audio content.

11. The method of claim 10, wherein the particular type of audio content comprises an identifying tone.

12. The method of claim 11, wherein the identifying tone is within an auditory frequency range.

13. A system comprising:

a processor; and

a memory including instructions that, when executed by the processor, cause the processor to perform operations including:

determining whether an incoming transmission to a destination is authorized;

in response to a determination that the incoming transmission is not authorized:

determining whether a particular type of content is communicated via the incoming transmission;

instructing an electronic device coupled to the processor to route the incoming transmission to the destination when the particular type of content is not communicated via the incoming transmission; and instructing the electronic device to deny routing of the incoming transmission to the destination when the particular type of content is communicated via the incoming transmission.

14. The system of claim 13, wherein the memory is configured to store restriction information including a first list of authorized source identifiers, a second list of unauthorized source identifiers, an authorized time range, an authorized date range, or a combination thereof.

15. The system of claim 14, wherein the restriction information is received via a web interface.

16. The system of claim 14, wherein the restriction information is received via an interactive voice response interface.

17. The system of claim 13, wherein the processor is an element of an internet protocol network.

18. A computer readable storage device including instructions that, when executed by a processor, cause the processor to perform operations including:

determining whether an incoming transmission to a destination is authorized at an electronic device of a communication network; and

in response to determining that the incoming transmission is not authorized:

determining whether a particular type of content is communicated via the incoming transmission;

routing the incoming transmission to the destination when the particular type of content is not communicated via the incoming transmission; and

denying routing of the incoming transmission to the destination when the particular type of content is communicated via the incoming transmission.

19. The computer readable storage device of claim 18, wherein determining whether the incoming transmission to the destination is authorized is based on a identifier of a source of the incoming transmission, a date of the incoming transmission, a time of the incoming transmission, or a combination thereof.

20. The computer readable storage device of claim 18, wherein the operations further include providing a message to a source of the incoming transmission while determining whether the particular type of content is communicated via the incoming transmission.

* * * * *